Nortel Communication Server 1000

Signaling Server Installation and Commissioning

NN43001-312

Document status: Standard
Document version: 01.02
Document date: 30 May 2007

Sourced in Canada

Revision history

May 2007
Standard 01.02. This document is up-issued to support technical changes in Communication Server 1000 Release 5.0.

May 2007
Standard 01.01. This document is issued to support Communication Server 1000 Release 5.0. This document contains information previously contained in the following legacy document, now retired: *Signaling Server Installation and Configuration (553-3001-212)*.

March 2007
Standard 10.00. This document is up-issued to reflect changes in content.

CR Q01468373(2):

- updated the gkbackup.tar file content list in the “Backing up the H.323 Gatekeeper database” procedure in the “H.323 Gatekeeper database

December 2006
Standard 9.00. This document is up-issued to reflect changes in content.

CR Q01439642:

- added a new procedure (“Verifying the presence of an NRS”) to the “Upgrading from CS 1000 release 4.0” section of the “Software upgrade and reconfiguration” chapter

CR Q01468373(1):

- changed the name of the Gatekeeper database backup file in the “Backing up the H.323 Gatekeeper database” procedure and the “Copying the backed up H.323 database to the upgraded server” procedure, from “nrsback.tar” to “gkbackup.tar” in the “H.323 Gatekeeper database migration” chapter

November 2006
Standard 8.00. This document is up-issued to reflect changes in content.

CR Q014694590:

- addition of verbiage at the beginning of the “Installing the software” section in the “Software installation” chapter to indicate that 768 MB of RAM are required if the Signaling Server must support more than 382 H.323 virtual trunks
- addition of verbiage at the beginning of the “Upgrading the Signaling Server software” procedure in the “Software upgrade” chapter to indicate that 768 MB of RAM are required if the Signaling Server must support more than 382 H.323 virtual trunks

October 2006

Standard 7.00. This document is up-issued to reflect changes in content.

CR Q01413666:

- addition of appropriate instructions to establish FTP connections to the source and target Signaling Servers in the “Uploading the database” procedure in the “H.323 Gatekeeper database migration” section

CR Q014694590:

- addition of verbiage at the beginning of the “Installing the software” section in the “Software installation” chapter to indicate that 768 MB of RAM are required if the Signaling Server must support more than 382 H.323 virtual trunks
- addition of verbiage at the beginning of the “Upgrading the Signaling Server software” procedure in the “Software upgrade” chapter to indicate that 768 MB of RAM are required if the Signaling Server must support more than 382 H.323 virtual trunks

July 2006

Standard 6.00. This document is up-issued to reflect changes in content.

CR Q01382679:

- addition of missing system messages and procedure steps in the “Upgrading Signaling Server software” procedure found in the “Software upgrade and re-configuration” section
- repair of all “textual” procedure step references that were adversely affected by the addition of new procedure steps in the “Upgrading Signaling Server software” procedure found in the “Software upgrade and reconfiguration” section

CR Q01283452:

- addition of “rdsconvert” command to the “rdtools commands” table found in the “Command Line Interface (CLI) commands” section

April 2006
Standard 5.00. This document is up-issued to reflect changes in content.

CR Q01273279

- correct default logon credentials for the Signaling Server in Procedure 22 "Logging on to the Signaling Server" (page 147).

January 2006
Standard 4.00. This document is up-issued to reflect changes in content.

CR Q01190789:

- information on backing up the Gatekeeper database and storing it locally during a software upgrade

August 2005
Standard 3.00. This document is up-issued to support Communication Server 1000 Release 4.5.

September 2004
Standard 2.00. This document is up-issued for Communication Server 1000 Release 4.0.

October 2003
Standard 1.00. This document is a new NTP for Succession 3.0. It was created to support a restructuring of the Documentation Library, resulting in the merging of multiple legacy NTPs. This new document consolidates information previously contained in the following documents:

- *Branch Office (553-3001-214)*
- *IP Line: Description, Installation, and Operation (553-3001-365)*
- *Large System: Planning and Engineering (553-3021-120)*
- *Succession 1000 System: Overview (553-3031-010)*
- *Succession 1000 System: Planning and Engineering (553-3031-120)*
- *Succession 1000 System: Installation and Configuration (553-3031-210)*
- *Succession 1000 System: Upgrade Procedures (553-3031-258)*

Contents

Procedures

New in this release

The following section details new content in the *Signaling Server Installation and Configuration (553-3001-212)* for CS 1000 Release 5.0.

Features

See the following sections for information about feature changes:

- "Nortel Common Processor Pentium Mobile server" (page 13)
- "International Business Machines X306m 1U server" (page 13)
- "Hewlett Packard DL320-G4 1U server" (page 13)

Nortel Common Processor Pentium Mobile server

CS 1000 Release 5.0 introduces the Nortel Common Processor Pentium Mobile (CP PM) server. This server is circuit card-based, rather than PC-based. Nortel designed two models of this server: one for use in CS 1000E systems, and the other for use in CS 1000M SG and CS 1000M MG systems.

For more information about the Nortel CP PM server, refer to "Nortel CP PM server" (page 24).

International Business Machines X306m 1U server

CS 1000 Release 5.0 introduces the International Business Machines (IBM) X306m 1U commercial off-the-shelf (COTS) server. This server is a rack-mounted, PC-based, industry-standard server.

For more information about the IBM X306m server, refer to "IBM X306m server" (page 28).

Hewlett Packard DL320-G4 1U server

CS 1000 Release 5.0 introduces the Hewlett Packard (HP) DL320-G4 1U commercial off-the-shelf (COTS) server. This server is a rack-mounted, PC-based, industry-standard server.

For more information about the HP DL320-G4 server, refer to "HP DL320-G4 server" (page 33).

How to get help

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

How to get help from the Nortel web site

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

www.nortel.com/support

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

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

Getting help over the telephone from a Nortel Solutions Center

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

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

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

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

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

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Introduction

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

Subject

This document describes the Signaling Server and provides the information necessary to install and configure it in a Communication Server 1000 system. This document contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 5.0 software. For information on legacy products and releases, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following CS 1000 systems:

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

Intended audience

This document is intended for individuals who install, configure and maintain Signaling Servers in a Communication Server 1000 environment.

Only qualified personnel are to install a Signaling Server. To use this document, you must have a working knowledge of CS 1000E and CS 1000M equipment and operation. Contact Nortel Training Centers for information on installation courses.

Complete all system engineering and planning activities before using this guide to install a Signaling Server.

Related information

The following NTPs are referenced in this document:

- *IP Peer Networking Installation and Commissioning (NN43001-313)*
- *Branch Office: Installation and Commissioning (NN43001-314)*
- *Element Manager: System Administration (NN43001-632)*
- *IP Line Fundamentals (NN43001-500)*
- *Software Input/Output: Maintenance (NN43001-711)*
- *CS 1000 to MCS 5100 Converged Desktop Type 2: Configuration Guide (NN43001-321)*
- *Communication Server 1000M and Meridian 1: Large System Planning and Engineering (NN43021-220)*
- *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning (NN43021-310)*
- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures (NN43021-458)*
- *Communication Server 1000E: Planning and Engineering (NN43041-220)*
- *Communication Server 1000E Installation and Commissioning (NN43041-310)*
- *Communication Server 1000E: Upgrade Procedures (NN43041-458)*
- *Security Management (NN43001-604)*
- *Network Routing Service Installation and Commissioning NN43001-564)*

The following third party documents are referenced in this NTP:

- *IBM xSeries 306m Types 8848 and 8491 User Guide*
- *HP ProLiant DL320 Generation 4 Server User Guide*

Documentation

To access Nortel documentation online, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

To obtain Nortel documentation on CD-ROM, contact your Nortel customer representative.

Overview

Contents

This section contains information on the following topics:

Description

The Signaling Server provides a central processor to drive Session Initiation Protocol (SIP) and H.323 signaling, IP Phone signaling, and IP Peer Networking in CS 1000E and CS 1000M systems.

The Signaling Server provides signaling interfaces to the IP network using the following software components that run on the VxWorks™ real-time operating system:

- IP Phone Terminal Proxy Server
- SIP and H.323 signaling gateway (Virtual Trunk)
- Network Routing Service (NRS)
- CS 1000 Element Manager Web server

- Application Server for the Personal Directory, Callers List, and Redial List features

Like Media Cards, the Signaling Server has both an ELAN and a TLAN network interface. The Signaling Server communicates with the Call Server through the ELAN subnet.

You can install Signaling Servers in a load-sharing redundant configuration for higher scalability and reliability.

Software applications

This section briefly describes the software components that run on the Signaling Server.

IP Phone Terminal Proxy Server

The Terminal Proxy Server (TPS) provides the signaling interface for IP Phones. The TPS supports a maximum of 5000 IP Phones on each Signaling Server. In conjunction with the Call Server, the TPS delivers a full suite of telephone features.

The Unified Network IP Stimulus protocol (UNIStim) is the single point of contact between the various server components and the IP Phone. UNIStim is the stimulus-based protocol used for communication between an IP Phone and a TPS on the Voice Gateway Media Card.

IP Peer Networking supports the following IP Phones:

- Nortel IP Phone 2001
- Nortel IP Phone 2002
- Nortel IP Phone 2004
- IP Phone 2007
- IP Audio Conference Phone 2033
- Nortel IP Softphone 2050
- Nortel IP Phone 1110
- Nortel IP Phone 1120E
- Nortel IP Phone 1140E
- Nortel IP Phone 1150E

You can configure each IP Phone through the Dynamic Host Configuration Protocol (DHCP) to register with a Call Server for feature control.

The TPS on the Signaling Server also manages the firmware for all connected IP Phones. For more information on IP Phone firmware management, see *IP Line Fundamentals (NN43001-500)* and *Branch Office: Installation and Commissioning (NN43001-314)*.

SIP and H.323 signaling gateway (Virtual Trunk)

Session Initiation Protocol trunking

Session Initiation Protocol (SIP) is a signaling protocol for creating, modifying, and terminating sessions with one or more participants. These sessions can include IP Phone calls, multimedia distribution, and multimedia conferences. Basic SIP connectivity, referred to as SIP trunking, provides a direct media path between users in the CS 1000/Meridian 1 domain and users in the SIP domain.

The SIP trunking software functions as:

- SIP User Agent
- signaling gateway for all IP Phones

For more information about SIP trunking, see *IP Peer Networking Installation and Commissioning (NN43001-313)* and *Network Routing Service Installation and Commissioning NN43001-564)*.

H.323 trunking

H.323 is a standard that specifies the components, protocols, and procedures that provide multimedia communication services over packet networks.

The H.323 signaling software (Virtual Trunk) provides the industry-standard H.323 signaling interface to H.323 gateways. It supports both en bloc and overlap signaling. This software uses an H.323 Gatekeeper to resolve addressing for systems at different sites.

> ***Note:*** For overlap signaling to provide the maximum benefit, Nortel highly recommends that all Signaling Servers in the network be overlap-enabled. Failure to do so results in call-completion delays caused by converting between overlap and en bloc.

The H.323 gateway supports direct, end-to-end voice paths using Virtual Trunks with the following benefits:

- elimination of multiple IP Telephony to circuit-switched conversions
- improved voice quality
- simplified troubleshooting
- inter-operability

For more information about H.323 signaling, refer to *IP Peer Networking Installation and Commissioning (NN43001-313)* and *Network Routing Service Installation and Commissioning NN43001-564)*.

Network Routing Service

The IP Peer Networking feature provides a Network Routing Service (NRS) to which all systems in the network are registered. There are two flavors of NRS in CS 1000 Release 5.0:

- an NRS that runs as an application on a Signaling Server
- an NRS that runs as a standalone application on a dedicated server

This document describes the NRS that runs as an application on a Signaling Server. For more information about the standalone NRS running on a dedicated server, see *Network Routing Service Installation and Commissioning NN43001-564)*.

The NRS application on a Signaling Server has three components:

- Session Initiation Protocol (SIP) Redirect Server
- H.323 Gatekeeper
- Network Connection Service (NCS)

A network requires only one NRS. NRS redundancy is supported and is highly recommended.

SIP Redirect Server

The IP Peer Networking feature also provides a SIP Redirect Server that logically routes (directly or indirectly) SIP requests to the proper destination.

The SIP Redirect Server software provides telephone-number-to-IP address resolution. The software uses a Gateway Location Service to match a fully qualified telephone number with a range of telephone numbers and a SIP gateway that provides access to that range of DNs.

For more information about the SIP Redirect Server, refer to *IP Peer Networking Installation and Commissioning (NN43001-313)* and *Network Routing Service Installation and Commissioning NN43001-564)*.

H.323 Gatekeeper

The IP Peer Networking feature provides an H.323 Gatekeeper on the Signaling Server, where all systems in the network are registered.

The H.323 Gatekeeper software provides telephone-number-to-IP address resolution. Because all systems in the network are registered to the H.323 Gatekeeper, the need for manual configuration of IP addresses and numbering plan information at every site is eliminated. As a result, the

H.323 Gatekeeper software also eliminates the duplication of numbering plan information among sites. However, support is still available for static registration and manual configuration.

For more information about the H.323 Gatekeeper, refer to *IP Peer Networking Installation and Commissioning (NN43001-313)* and *Network Routing Service Installation and Commissioning NN43001-564)*.

Network Connection Service

The Network Connection Service (NCS) provides an interface to the TPS that enables the TPS to query the NRS using the UNIStim protocol. The NCS is required to support the Branch Office, Virtual Office, and Geographic Redundancy features.

CS 1000 Element Manager web server

The CS 1000 Element Manager web server resides on the Signaling Server and is directly accessible through a web browser or Telephony Manager (TM). Element Manager is a simple and user-friendly web-based interface that supports a broad range of system management tasks. Element Manager has many features to help administrators manage systems with maximum efficiency.

For more information on Element Manager, refer to "Element Manager configuration" (page 239) and *Element Manager: System Administration (NN43001-632)*.

Application Server for the Personal Directory, Callers List, and Redial List feature

The Application Server for the Personal Directory, Callers List, and Redial List features (IP Phones Application Server) runs on the Signaling Server. Only one database can exist in the network; redundancy is not supported. The IP Phones Application Server database can coexist with the other software applications on a Signaling Server. However, if you have more than 1000 users, Nortel recommends that you store the database on a dedicated Signaling Server (preferably a Follower). The IP Phones Application Server cannot be run on a Signaling Server at a branch office.

For more information on the IP Phones Application Server (Personal Directory, Callers List, and Redial List), refer to *IP Line Fundamentals (NN43001-500)*.

Hardware description

CS 1000 Release 5.0 introduces three new servers that can host a CS 1000 Release 5.0 Signaling Serverr:

- the Nortel CP PM (Common Processor Pentium Mobile) server

- the IBM X306m server
- the HP DL320-G4 server

The Nortel CP PM server is installed in a Media Gateway chassis or cabinet in a CS 1000E system (model NTDW61BAE5), or in a Universal Equipment Module (UEM) in a CS 1000M SG or CS 1000M MG system (model NTDW66AAE5).

The IBM X306m and HP DL320-G4 servers are commercial, off-the-shelf (COTS) 1U servers.

The legacy Nortel ISP1100 server can still be used in a CS 1000 Release 5.0 system, but may require a RAM upgrade.

This section describes the physical components of each server.

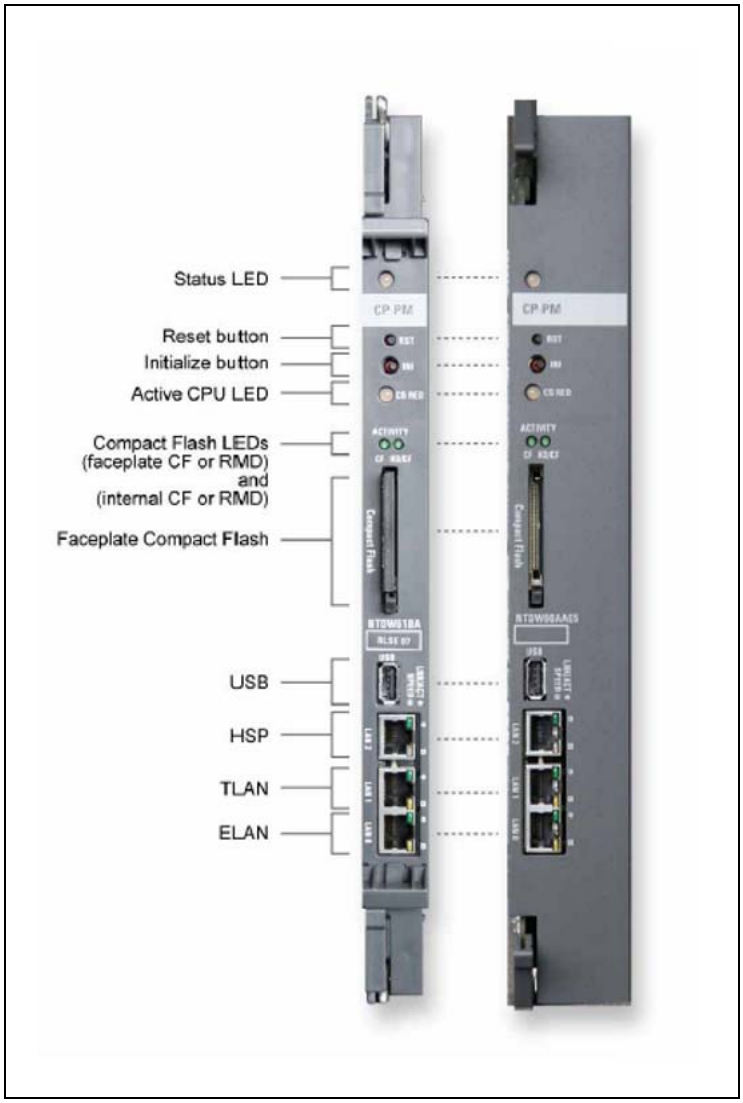
Nortel CP PM server

The Nortel CP PM server is a high performance server that can be used as both a Call server or Signaling Server in a CS 1000 Release 5.0 system. Configured as a Signaling Server, it delivers capacity improvement by providing flexible scaling from 0 to 22,500 IP Phones and represents a 70% increase in power for Signaling Server applications. The increased application power and capacity, coupled with the reduction in foot print and power consumption, means a lower cost of ownership.

The Nortel CP PM server has two models. The NTDW61BAE5 model can be configured as either a Call Server or a Signaling Server in CS 1000E systems. The NTDW66AAE5 model is used as a Signaling Server in CS 1000M systems.

The following figure shows the faceplates of the NTDW61BAE5 (left) and the NTDW66AAE5 (right) models of the server.

Figure 1
Faceplates of the Nortel CP PM server



Product Code

The Nortel CP PM server comes in two models and thus has two product codes:

- NTDW61BAE5 (CS 1000E system)
- NTDW66AAE5 (CS 1000M system)

Features

The Nortel CP PM server provides the following features:

- Intel Pentium M processor (1.4 Ghz)
- Fixed Media Device (FMD)

  - an internal hard drive (NTDW6102E5)
  - hosts all 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
  - 1 Gb of SDRAM is configured when delivered

- One 1 Gb/s Ethernet port (HSP)
  - not used when configured as a Signaling Server

- Two 100BaseT Ethernet ports
  - TLAN port is to connect the server to a TLAN Layer 2 Ethernet switch port
  - ELAN port is to connect the server to an ELAN Layer 2 Ethernet switch port

- Nortel NTDU0606E6 cabling kit
  - ships only with the CS 1000E model (NTDW61BAE5)
  - short length CAT5 cables used to connect the Signaling Server to the TLAN/ELAN ports on a Media Gateway Card (MGC)
  - if the TLAN and ELAN Ethernet ports on the MGC are occupied, longer CAT5 cables are required (not supplied) to connect the Signaling Server directly to the TLAN and ELAN Ethernet switches

- Two serial ports
  - used to connect a maintenance terminal to the server

- Nortel NTAK19EC cabling kit
  - used 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 DTE-DTE null modem cable (not supplied) is needed to connect the 25-pin DB connector to a serial port on a maintenance terminal

- One USB port
  - reserved for future use

- A **RST** (Reset) button
  - used to cold-reboot the server
- An **INI** (Initialize) button
  - to warm-reboot the server

LEDs

Refer to Figure 1 "Faceplates of the Nortel CP PM server" (page 25) when reviewing the following LED descriptions:

- The Status LED is the top-most LED, is unlabeled, and indicates the following:
  - steady RED indicates that the BIOS self-test is running
  - flashing RED indicates that bootrom and Operating System are being loaded
  - steady YELLOW indicates that applications are being loaded
  - flashing YELLOW indicates that applications loaded successfully
  - steady GREEN indicates that the PBX link is up
  - flashing GREEN indicates that the PBX link is down
  - OFF indicates no power to the server
- The Active CPU LED is below the **INI** button, is labeled as CS Red, and is not used on the CP PM server when configured as a Signaling Server.
- Compact Flash LEDs
  - The Compact Flash LED for the faceplate CF drive is labeled as CF and flashing green indicates read/write activities.
  - The Compact Flash LED for the internal CF drive is labeled as HD/CF and flashing green indicates read/write activities.
- The LEDs above the HSP Ethernet port relate to HSP port activity. The HSP port is not used on the Nortel CP PM server when configured as a Signaling Server.
- The LEDs above the TLAN Ethernet port relate to TLAN port activity.
  - The GREEN LED above and to the left of the port has the following indications:
    - steady GREEN indicates that the port is operational
    - flashing GREEN indicates that the port is active
  - The YELLOW LED above and to the right of the port has the following indications:

- steady YELLOW indicates that the port is operating at 100 Mb/s
- OFF indicates that the port is operating at 10 Mb/s

- The LEDs above the ELAN Ethernet port relate to ELAN port activity.
  - The GREEN LED above and to the left of the port has the following indications:
    - steady GREEN indicates that the port is operational
    - flashing GREEN indicates that the port is active
  - The YELLOW LED above and to the right of the port has the following indications:
    - steady YELLOW indicates that the port is operating at 100 Mb/s
    - OFF indicates that the port is operating at 10 Mb/s

Power

Power is supplied to the CP PM server through the backplane of the Media Gateway (CS 1000E) or Universal Equipment Model (CS 1000M SG and CS 1000M MG).

IBM X306m server

The IBM X306m server is a rack-mountable, Pentium 4, PC-based, commercial off-the-shelf (COTS) 1U server. Please refer to the *IBM xSeries 306m Types 8848 and 8491 User Guide* shipped with the server for a more detailed description.

The following figures show photos of the front and back of an IBM X306m server.

Figure 2
Front of the IBM X306m server - photo

Figure 3
Back of the IBM X306m server - photo

Product Code

The product code for the IBM X306m Signaling Server is NTDU99AAE5.

Feature summary

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

Power

The power cord connector is on the left-rear corner of the IBM X306m server. The Power On/Off switch is on the left side of the front faceplate. When the GREEN power LED on the left side of the front faceplate is illuminated, the power is on. The power supply is factory installed and is not customer replaceable.

Cooling

The IBM X306m server has forced-air cooling. The fan runs whenever the unit is operating. The air flow is front-to-back.

Card slots

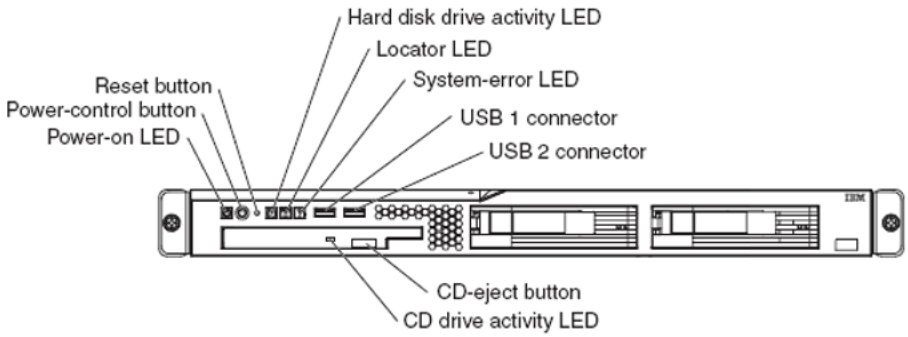
The IBM X306m server has a PCI card slot, but it is not used.

Front panel buttons, connectors and LEDs

This section describes the buttons, connectors and LEDs found on the front panel of the IBM X306m server.

The following figure shows the front panel of an IBM X306m server with labeling for all buttons, connectors and LEDs.

Figure 4
Front panel of the IBM X306m server - buttons, connectors and LEDs



The following list describes each of the front panel buttons, connectors and LEDs for the IBM X306m server:

- Power-on 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.

    Note: If this LED is off, it does not mean that there is no electrical power in the server. The LED might be burned out. To remove all electrical power from the server, you must disconnect the power cord from the electrical outlet.

- Power-control button
  - Press this button to turn the server on and off manually. A power-control-button shield comes installed around the button to prevent the server from being turned off accidentally. You can remove this disk-shaped shield if you prefer.

- Reset button
  - Press this button to reset the server and run the power-on self-test (POST). You might have to use a pen or the end of a straightened paper clip to press the button.
  - cold-reboots the Signaling Server

- Hard disk drive activity LED
  - When this LED is flashing, 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.

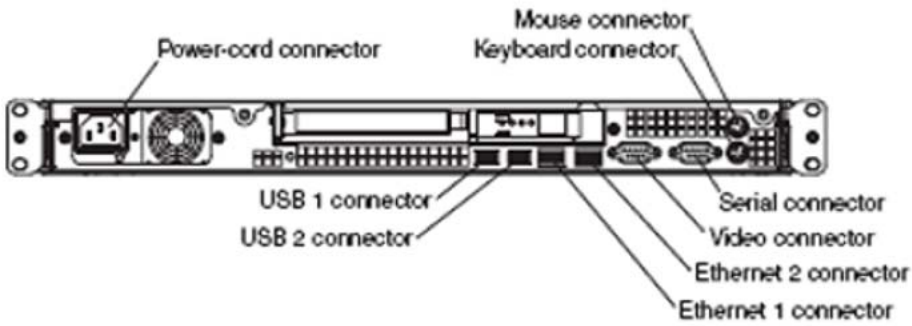
- System-error LED
  - When this LED is lit, it indicates that a system error has occurred.
- USB connectors
  - Connect a USB device to either of these connectors.
- CD-eject button
  - Press this button to release a CD from the CD drive.
- CD drive activity LED
  - When this LED is lit, it indicates that the CD drive is in use.

Back panel connectors and LEDs

This section describes the connectors and LEDs found on the back panel of the IBM X306m server.

The following figure shows the back panel of an IBM X306m server with labeling for all connectors.

Figure 5
Back panel of the IBM X306m server - connectors



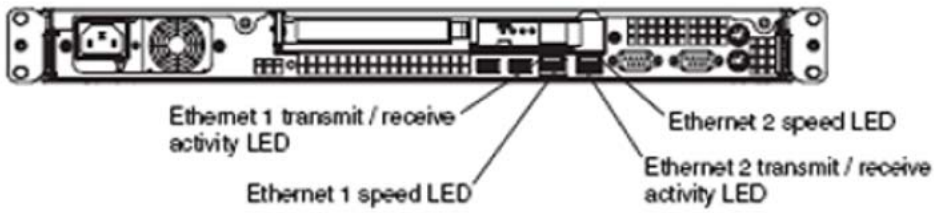
The following list describes the back panel connectors of the IBM X306m server:

- Power-cord connector
  - Connect the power cord to this connector.
- Keyboard connector
  - Connect a PS/2 keyboard to this connector.
- Mouse connector
  - Connect a mouse or other PS/2 device to this connector.

- Serial connector
  - — Connect a 9-pin serial device to this connector.
  - — used to connect a maintenance terminal to the server
- Video connector
  - — Connect a monitor to this connector.
- Ethernet1 connector
  - — used to connect the server to a TLAN Layer 2 Ethernet switch port
- Ethernet2 connector
  - — used to connect the server to an ELAN Layer 2 Ethernet switch port
- USB connectors
  - — used to connect a USB device to the server
  - — either of these connectors can be used as the Removable Media Device (RMD)
    - – the RMD is used to back up IP configuration data from the Signaling Server using the Software Installation Tool

The following figure shows the back panel of an IBM X306m server with labeling for all LEDs.

Figure 6
Back panel of the IBM X306m server - LEDs



The following list describes the back panel LEDs on the IBM X306m server:

- Ethernet transmit/receive activity LED
  - — This LED is on each Ethernet connector. When this LED is lit, it indicates that there is activity between the server and the network.
- Ethernet speed LED
  - — This LED is on each Ethernet connector. When this LED is lit, it indicates that the Ethernet network speed is 1 Gb/s. When this LED

is off, it indicates that the Ethernet network speed is 10 Mb/s or 100 Mb/s.

HP DL320-G4 server

The HP DL320-G4 server is a rack-mountable, Pentium 4, PC-based, commercial off-the-shelf (COTS) 1U server. Please refer to the *HP ProLiant DL320 Generation 4 Server User Guide* shipped with the server for a more detailed description.

The following figures show photos of the front and back of an HP DL320-G4 server.

Figure 7
Front of the HP DL320-G4 server - photo

Figure 8
Back of the HP DL320-G4 server - photo

Product Code

The product code for the HP DL320-G4 Signaling Server is NTDU97AA.

Feature summary

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.
  - — cold-reboots the Signaling Server

Power

The power cord connector is on the right rear corner of the HP DL320-G4 server. The Power On/Off switch is on the right side of the front faceplate. When the GREEN power LED on the right side of the front faceplate is illuminated, the power is on. The power supplies are factory installed and are not customer replaceable.

Cooling

The HP-DL30-G4 server has forced-air cooling. The fan runs whenever the unit is operating. The air flow is front-to-back.

Card slots

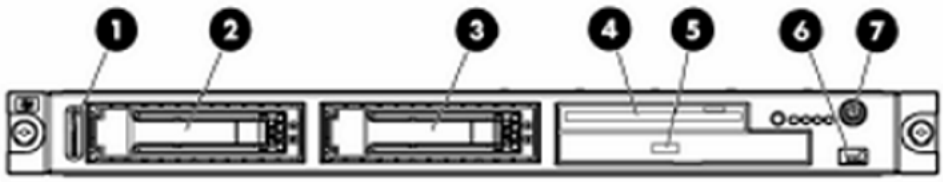
The HP DL320-G4 server has a PCI card slot, but it is not used.

Front components

This section describes the components found on the front panel of the HP DL320-G4 Signaling Server.

The following figure shows the front panel of an HP DL320-G4 server with labeling for all components.

Figure 9
Front panel of the HP DL320-G4 server - components



The following list describes the front panel components of the HP DL320-G4 server:

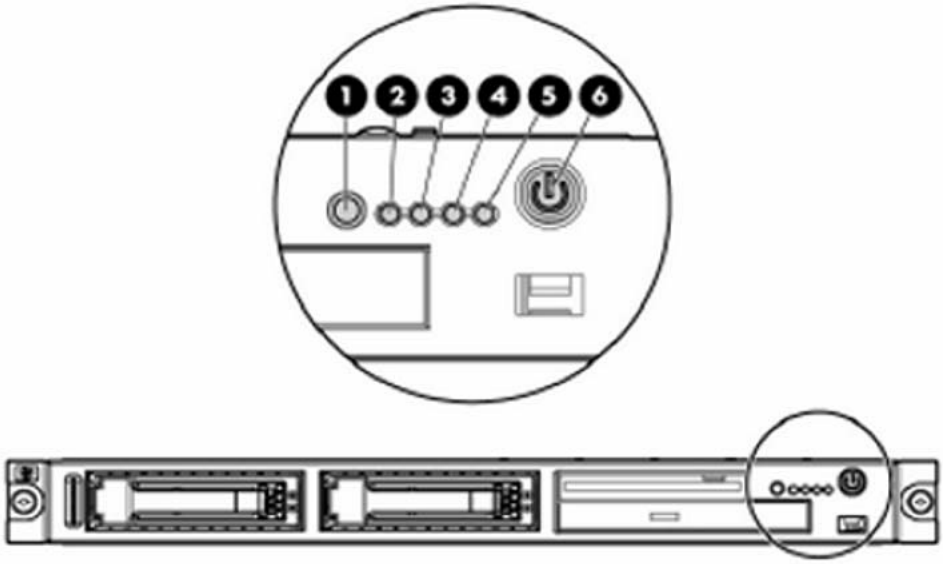
1. Serial label pull tab
2. Hard drive bay 1
3. Hard drive bay 2
4. Diskette drive bay
5. Optical drive bay
    - used to load the Signaling Server software files for the Signaling Server, Voice Gateway Media Cards, and IP Phones
6. Front USB port
    - serves as the Removable Media Device (RMD)

- the RMD is used to back up IP configuration data from the Signaling Server using the Software Installation Tool

7. Power On/Standby button and system power LED

The following figure shows the front panel of the HP DL320-G4 server with labeling for all buttons and LEDs.

Figure 10
Front panel of the HP DL320-G4 server - buttons and LEDs



The following list describes the front panel buttons and LEDs on the HP DL320-G4 server:

1. UID button/LED
   - 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 in a degraded state, refer to system board LEDs in the *HP ProLiant DL320 Generation 4 Server User Guide* shipped with the server.
   - Red: System critical.

— To identify the component in a critical state, refer to system board LEDs in the *HP ProLiant DL320 Generation 4 Server User Guide* shipped with the server.

- 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.

     Note: If power is off, view the LEDs on the RJ-45 connector for status by referring to the rear panel LEDs.

4. NIC 2 link/activity LED
   - Green: Network link exists.
   - Flashing green: Network link and activity exist.
   - Off: No link to network exists.

     Note: If power is off, the front panel LED is not active. View the LEDs on the RJ-45 connector for status by referring to the rear panel LEDs.

5. Drive activity LED
   - Green: Drive activity is normal.
   - Amber: Drive failure occurred.
   - Off: No drive activity.

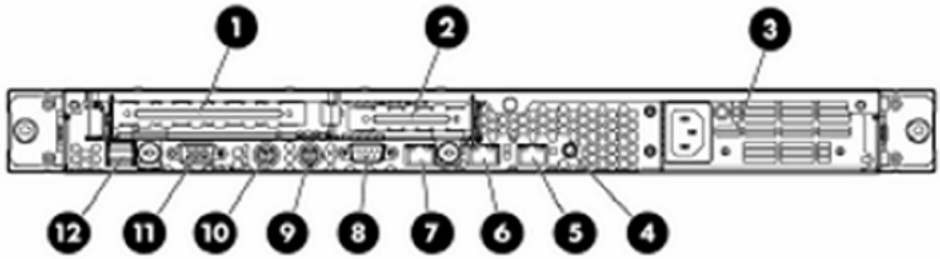
6. Power On/Standby button and system power LED
   - Green: System is on.
   - Amber: System is shut down, but power is still applied.
   - Off: Power cord is not attached, power supply failure has occurred, no power supplies are installed, facility power is not available, or the DC-to-DC converter is not installed.

Back panel components

This section describes the components found on the back panel of the HP DL320-G4 Signaling Server.

The following figure shows the back panel of the HP DL320-G4 server with labeling for all components.

Figure 11
Back panel of the HP DL320-G4 server - components

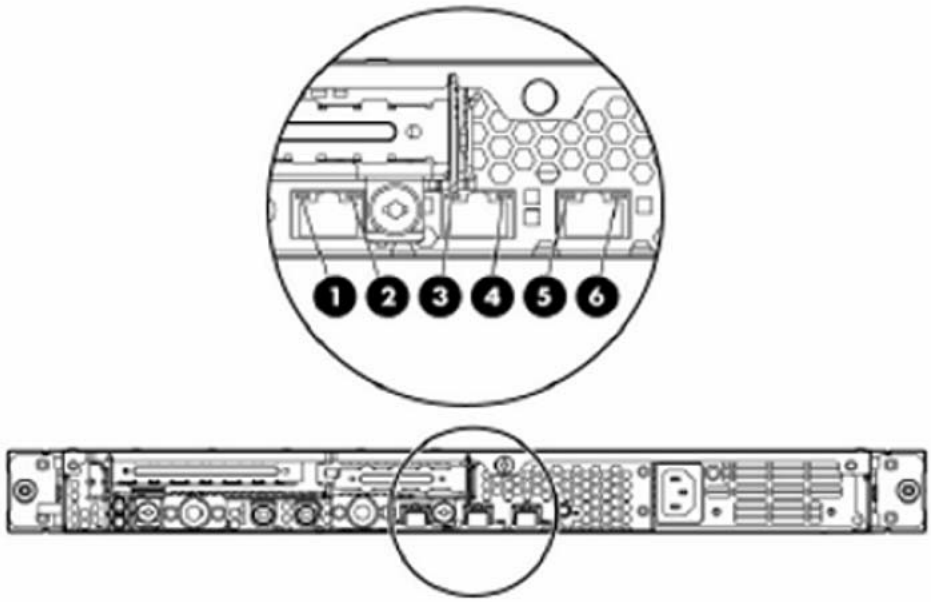


The following list describes the back panel components of the HP DL320-G4 server:

1. PCI-X expansion slot 2, full-length (optional PCI Express slot 1)
2. PCI Express expansion slot 1, low-profile, half-length
3. Power supply
4. UID button/LED
5. 10/100/1000 NIC 2
   - used to connect the server to an ELAN Layer 2 ethernet switch port
6. 10/100/1000 NIC 1
   - used to connect the server to a TLAN Layer 2 Ethernet switch port
7. iLO 2 management port
8. Serial connector
   - used to connect the server to a maintenance and administration terminal (PC)
9. Keyboard connector
10. Mouse connector
11. Video connector
12. USB connectors (2)
    - either of these connectors can be used as the Removable Media Device (RMS)
      — the RMD is used to back up IP configuration data from the Signaling Server

The following figure shows the back panel of the HP DL320-G4 server with labeling for all LEDs.

Figure 12
Back panel of the HP DL320-G4 server - LEDS



The following list describes the back panel LEDs on the HP DL320-G4 server:

1. iLO 2 activity
   - Green: Activity exists.
   - Flashing green: Activity exists.
   - Off: No activity exists.
2. iLO 2 link
   - Green: Link exists.
   - Off: No link exists.
3. 10/100/1000 NIC 1 activity
   - Green: Link exists.
   - Flashing green: Activity exists.
   - Off: No link exists.
4. 10/100/1000 NIC 1 link
   - Green: Link exists.
   - Off: No link exists.

5. 10/100/1000 NIC 2 activity
   - Green: Activity exists.
   - Flashing green: Activity exists.
   - Off: No activity exists.

6. 10/100/1000 NIC 2 link
   - Green: Link exists.
   - Off: No link exists.

Nortel ISP1100 server

The legacy Nortel ISP1100 server hosted Signaling Server functionality in all previous releases of CS 1000. It can also host Signaling Server functionality in CS 1000 Release 5.0.

Product code

The product code for the Nortel ISP1100 server is NTDU27.

Power

The power cord connector is on the left corner on the rear of the Nortel ISP1100 server. When the green power LED, on the left side, is illuminated, the power is on. The Power On/Off switch is on the front faceplate. The power supplies are factory installed and are not customer replaceable.

Cooling

The Nortel ISP1100 server has forced-air cooling. The fan runs whenever the unit is operating. The air flow is front-to-back.

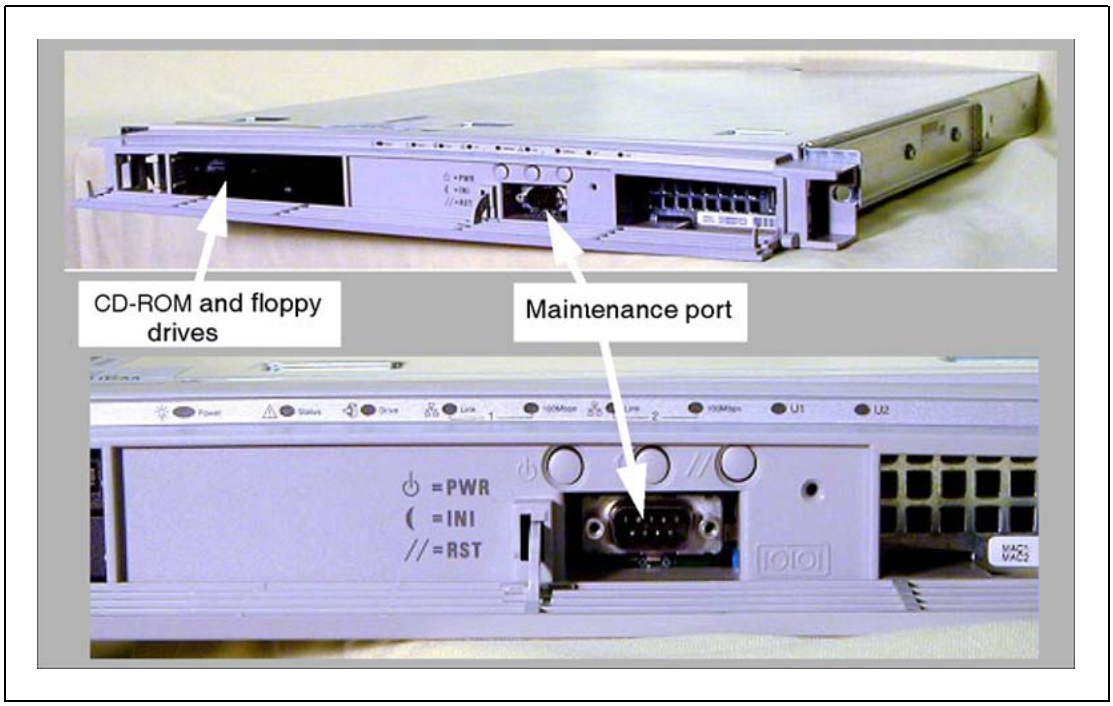
Card slots

The Nortel ISP1100 server has no available card slots.

Connectors

Front connectors Figure 13 "Front of the ISP1100 server" (page 40) shows the connectors on the front of the Nortel ISP1100 server.

Figure 13
Front of the ISP1100 server

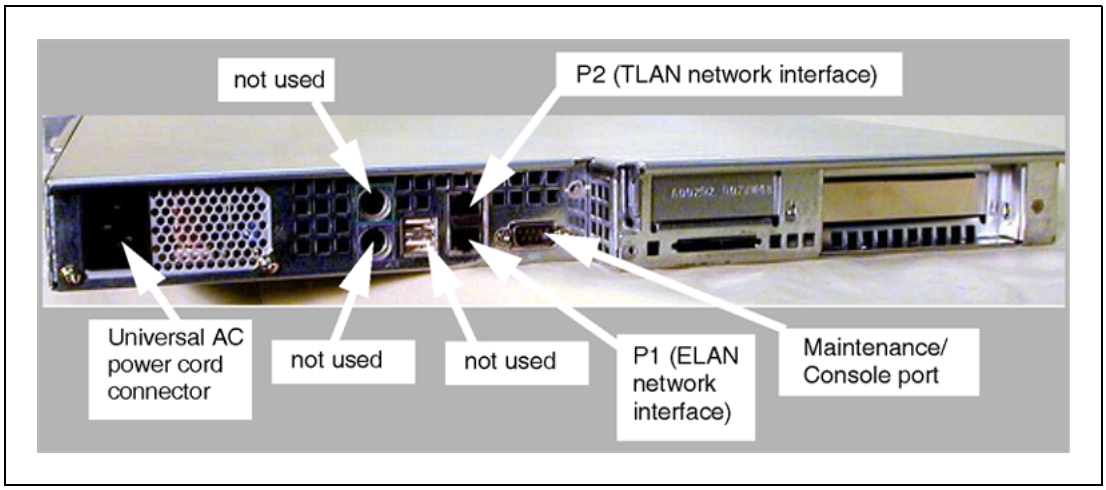


Refer to Figure 13 "Front of the ISP1100 server" (page 40).

- The maintenance port (DB-9 serial port) connects the Signaling Server to a maintenance and administration terminal (PC).
- The CD-ROM drive is used to load the Signaling Server software files for the Signaling Server, Voice Gateway Media Cards, and IP Phones. The Signaling Server software includes the Signaling Server operating system, applications, and all Element Manager web server files.
- The floppy drive is used if the CD-ROM is not bootable. To create a boot floppy, use the files in the mkboot directory on the Signaling Server Software CD-ROM. You can use the same boot floppy for any or all Software CD-ROMs.
  - the floppy drive is also used to back up and restore Nortel ISP1100 Signaling Server IP configuration data.

Back connectors Figure 14 "Back of the ISP1100 server" (page 41) shows the connectors on the back of the Nortel ISP1100 server.

Figure 14
Back of the ISP1100 server



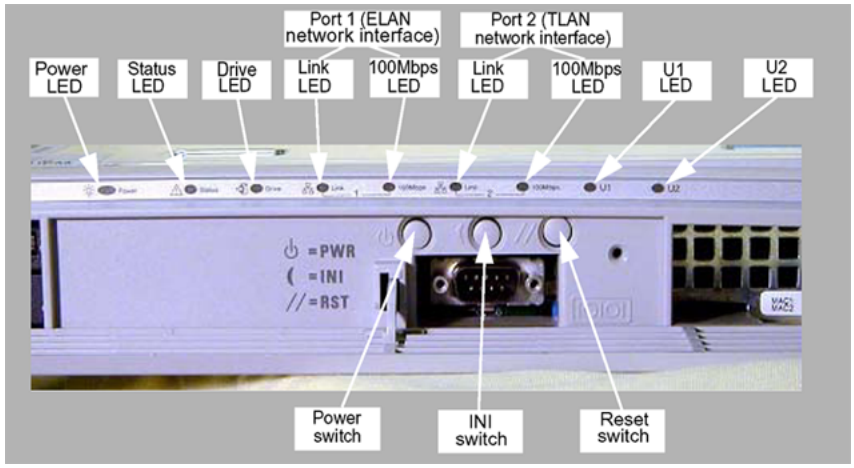
Refer to Figure 14 "Back of the ISP1100 server" (page 41).

- The AC power cord connector is at the back of the server on the left side.
- The TLAN network interface (P2) connects the server to a TLAN Layer 2 Ethernet switch port.
- The ELAN network interface (P1) connects the server to an ELAN Layer 2 Ethernet switch port.
- The maintenance/console port (DB-9 serial port) connects the server to a maintenance and administration terminal (PC). The console port is used for software installation and basic configuration.
- The remaining ports are not used for any function. Do not plug any device into these ports.

LEDs

Figure 15 "Nortel ISP1100 server LEDs" (page 42) shows the LEDs on the Nortel ISP1100 server.

Figure 15
Nortel ISP1100 server LEDs



The Nortel ISP1100 server LED indicators show the following:

- Power: Green LED on, power on; LED off, power off.
- Status: Red LED off, CPU running; LED on, CPU halted.
- Drive: Green LED flashing, Hard Drive or CD ROM Drive active.
- Link: Green LED, Ethernet port active.
- 100 Mb/s: Green LED on, Ethernet port running at 100 Mb/s; LED off, Ethernet port running at 10 Mb/s.

  Note: When the power is turned off on a Nortel ISP1100 server, the two Link LEDs for Port 0 and Port 1 continue to flash. Press the Power button for approximately 7 seconds to turn the power off completely.

Planning and engineering

Contents

This section contains the following information:

Regulatory information

Japanese DenAn warning

Figure 16
Japanese DenAn warning - English

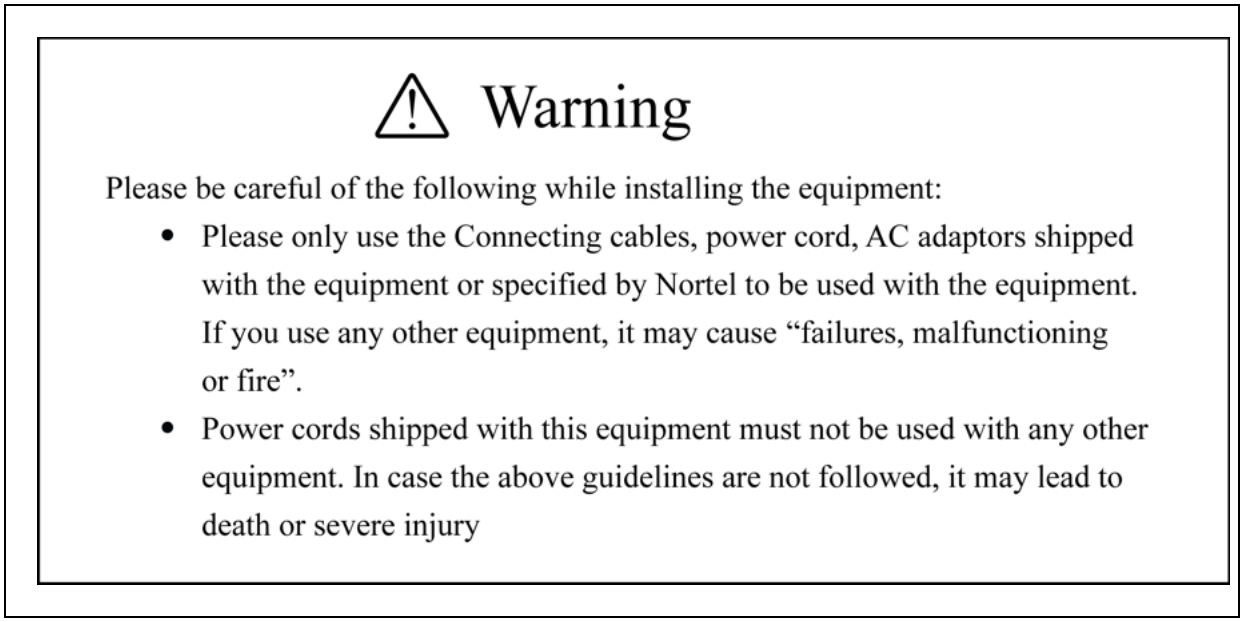
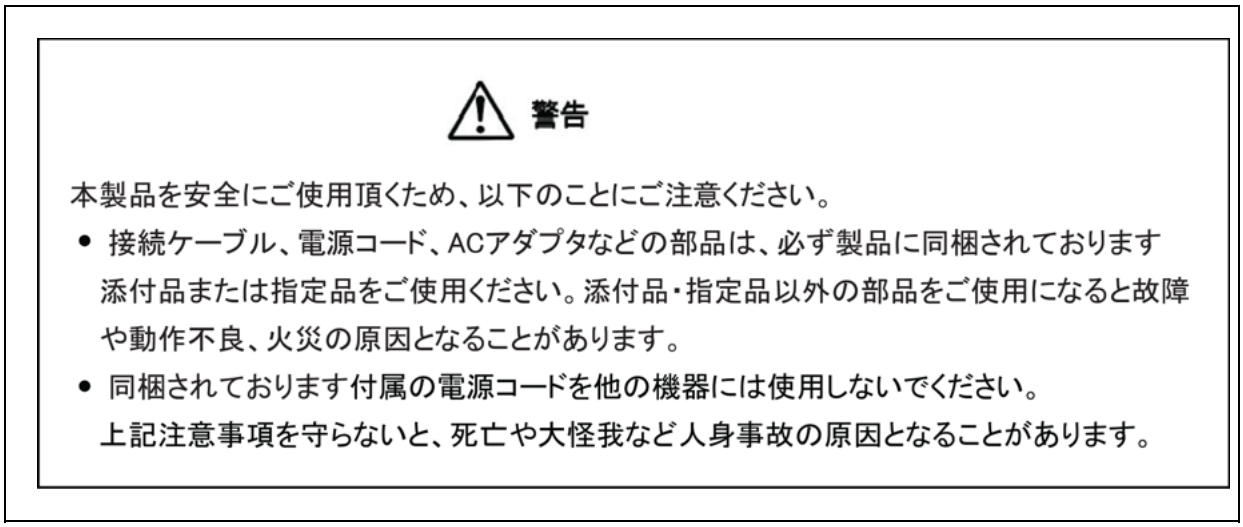


Figure 17
Japanese DenAn warning - Japanese



Regulatory compliance notices for the IBM X306m server

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

ATTENTION
This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

United Kingdom telecommunications safety requirement
Notice to Customers

This apparatus is approved under approval number NS/G/1234/J/100003 for indirect connection to public telecommunication systems in the United Kingdom.

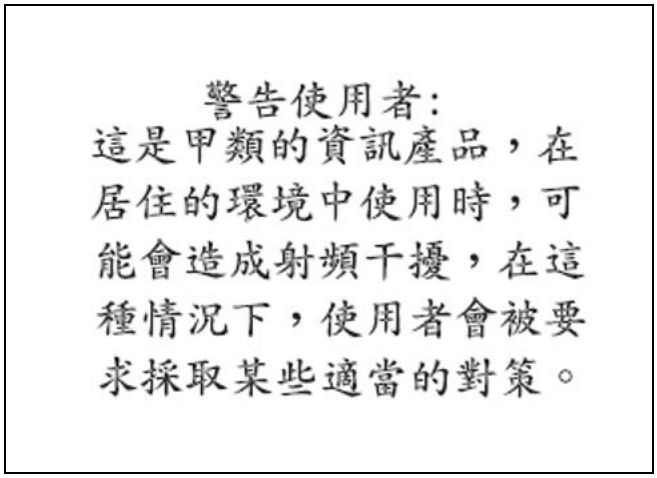
European Union EMC Directive conformance statement
This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

ATTENTION
This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

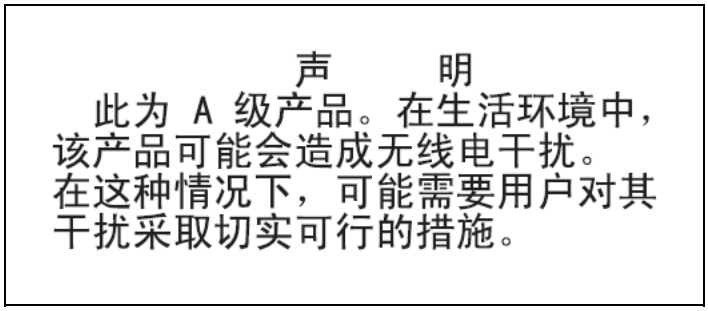
Taiwanese Class A warning statement

Figure 18
Taiwanese Class A warning statement



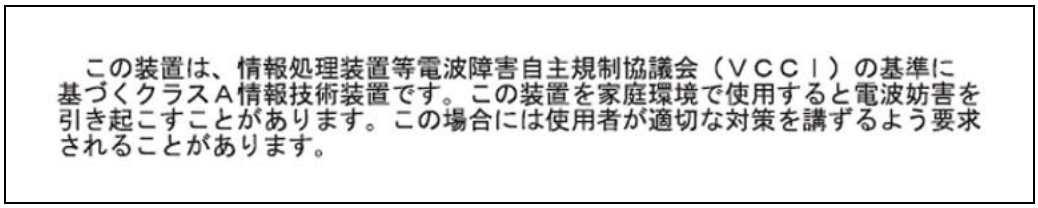
Chinese Class A warning statement

Figure 19
Chinese Class A warning statement



Japanese Voluntary Control Council for Interference statement

Figure 20
Japanese Voluntary Control Council for Interference statement



Regulatory compliance notices for the HP DL320-G4 server

Regulatory compliance identification numbers

For the purpose of regulatory compliance certifications and identification, this product has been assigned a unique regulatory model number. The regulatory model number can be found on the product nameplate label, along with all required approval markings and information. When requesting

compliance information for this product, always refer to this regulatory model number. The regulatory model number is not the marketing name or model number of the product.

Federal Communications Commission notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (for example, personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

FCC rating label The FCC rating label on the device shows the classification (A or B) of the equipment. Class B devices have an FCC logo or ID on the label. Class A devices do not have an FCC logo or ID on the label. After you determine the class of the device, refer to the corresponding statement.

Class A equipment This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Class B equipment This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful

interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit that is different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or television technician for help.

Declaration of conformity for products marked with the FCC logo, United States only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding this product, contact us by mail or telephone:

- Hewlett-Packard Company
  P. O. Box 692000, Mail Stop 530113
  Houston, Texas 77269-2000
- 1-800-HP-INVENT (1-800-474-6836).
  - — For continuous quality improvement, calls may be recorded or monitored.

For questions regarding this FCC declaration, contact us by mail or telephone:

- Hewlett-Packard Company
  P. O. Box 692000, Mail Stop 510101
  Houston, Texas 77269-2000
- 1-281-514-3333

To identify this product, refer to the part, series, or model number found on the product.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Hewlett-Packard Company may void the user's authority to operate the equipment.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Canadian notice (Avis Canadien)

Class A equipment This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Class B equipment This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union regulatory notice

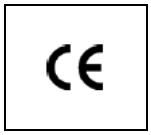
This product complies with the following EU Directives:

- Low Voltage Directive 73/23/EEC
- EMC Directive 89/336/EEC

Compliance with these directives implies conformity to applicable harmonized European standards (European Norms) which are listed on the EU Declaration of Conformity issued by Hewlett-Packard for this product or product family.

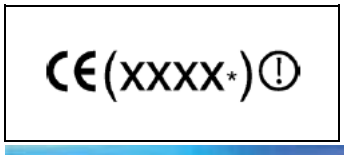
This compliance is indicated by the following conformity marking placed on the product:

Figure 21
EU regulatory mark - harmonized Telecom products



This marking is valid for non-Telecom products and EU harmonized Telecom products (e.g. Bluetooth).

Figure 22
EU regulatory mark - non-harmonized Telecom products

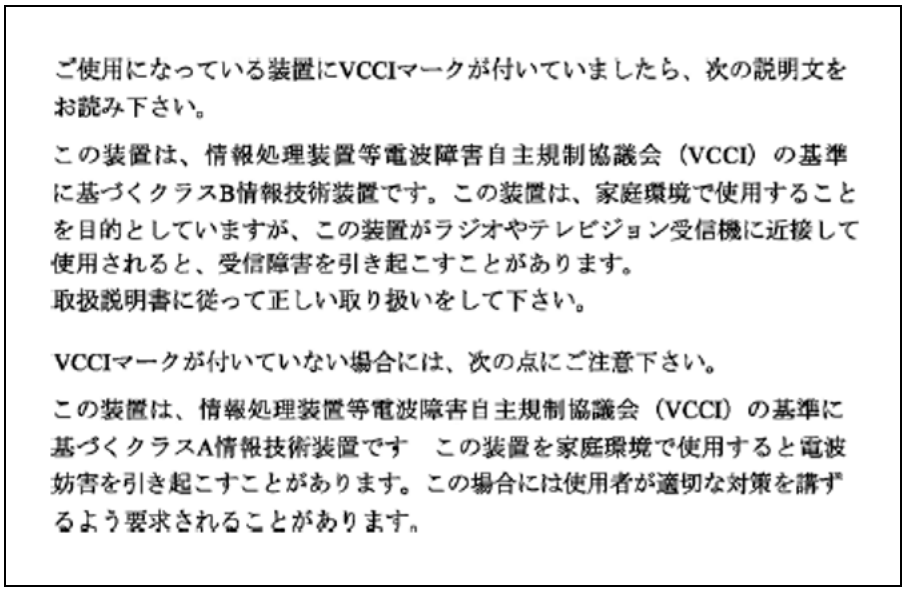


This marking is valid for EU non-harmonized Telecom products.

*Notified body number (used only if applicable—refer to the product label)

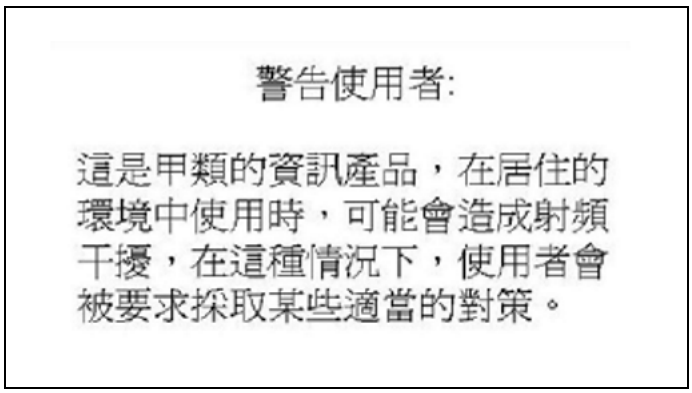
Japanese notice

Figure 23
Japanese notice



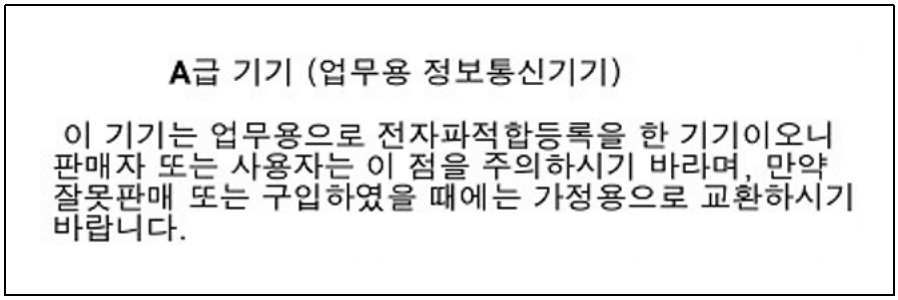
BSMI notice

Figure 24
BSMI notice



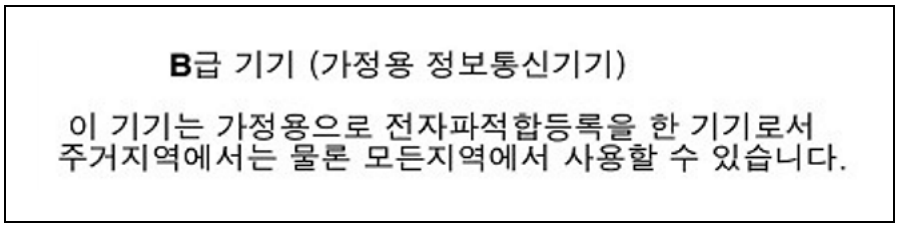
Korean notice A and B
Class A equipment

Figure 25
Korean Class A equipment notice



Class B equipment

Figure 26
Korean Class B equipment notice



Laser compliance

This product may be provided with an optical storage device (that is, CD or DVD drive) and/or fiber optic transceiver. Each of these devices contains a laser that is classified as a Class 1 Laser Product in accordance with US FDA regulations and the IEC 60825-1. The product does not emit hazardous laser radiation.

WARNING

Use of controls or adjustments or performance of procedures other than those specified herein or in the laser product's installation guide may result in hazardous radiation exposure. To reduce the risk of exposure to hazardous radiation:

- Do not try to open the module enclosure. There are no user-serviceable components inside.
- Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
- Allow only HP Authorized Service technicians to repair the unit.

The Center for Devices and Radiological Health (CDRH) of the U.S. Food and Drug Administration implemented regulations for laser products on August 2, 1976. These regulations apply to laser products manufactured from August 1, 1976. Compliance is mandatory for products marketed in the United States.

Battery replacement notice

WARNING

The computer contains an internal lithium manganese dioxide, a vanadium pentoxide, or an alkaline battery pack. A risk of fire and burns exists if the battery pack is not properly handled. To reduce the risk of personal injury:

- Do not attempt to recharge the battery.
- Do not expose the battery to temperatures higher than 60°C (140°F).
- Do not disassemble, crush, puncture, short external contacts, or dispose of in fire or water.

Batteries, battery packs, and accumulators should not be disposed of together with the general household waste. To forward them to recycling or proper disposal, please use the public collection system or return them to HP, an authorized HP Partner, or their agents.

For more information about battery replacement or proper disposal, contact an authorized reseller or an authorized service provider.

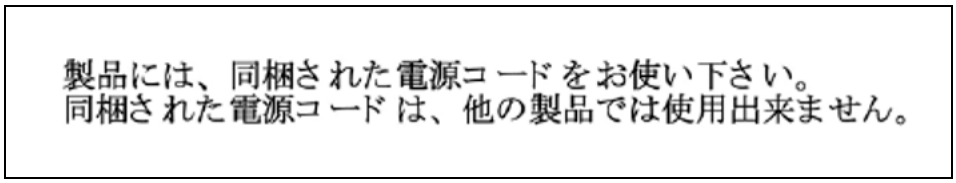
Taiwan battery recycling notice

The Taiwan EPA requires dry battery manufacturing or importing firms in accordance with Article 15 of the Waste Disposal Act to indicate the recovery marks on the batteries used in sales, giveaway or promotion. Contact a qualified Taiwanese recycler for proper battery disposal.

Figure 27
Taiwan battery recycling notice

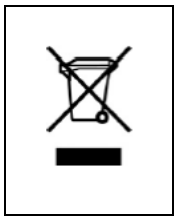
Power cord statement for Japan

Figure 28
Power cord statement for Japan



Disposal of waste equipment by users in private households in the European Union

Figure 29
European Union waste equipment symbol



This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

Environmental conditions

The operational environment for a Signaling Server must meet the following general conditions:

- Ventilation openings on a rack-mounted Signaling Server must be free of obstructions.
- Temperature must be from 0° to 35°/C (32° and 98° F).
- Humidity must be from 5 to 95 percent at 30°/C, non-condensing.
- The Signaling Server must not be subject to constant vibration.
- The Signaling Server and other system equipment must be at least 12 ft. (3.66 m) from sources of electrostatic, electromagnetic, or radio frequency interference. These sources can include:
  - power tools
  - appliances (such as vacuum cleaners)
  - office business machines (such as copying machines)
  - elevators
  - air conditioners and large fans
  - radio and TV transmitters
  - high-frequency security devices
  - all electric motors
  - electrical transformers

Grounding requirements

Like all system equipment, the Signaling Server must be thoroughly grounded. Refer to *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 the CS 1000 system you are installing.

The IBM X306m, HP DL320-G4, and Nortel ISP1100 Signaling Servers are rack-mounted and not connected to a grounding block. The following conditions indicate that the Signaling Sever is properly grounded:

- The Signaling Server power cord is plugged into the rack's AC outlet. The rack's AC outlet must be grounded to its dedicated electrical panel (preferred method).
- The Signaling Server power cord is plugged into a wall AC outlet. The Signaling Server is grounded outside of the rack by the safety grounding conductor in the power cord. This method ensures proper grounding only of the Signaling Server itself andt does not provide grounding

protection for other rack-mounted pieces of equipment. Therefore, ensure that other devices in the rack are properly grounded as required.

Grounding requirements for the Nortel CP PM server are provided by properly grounding the Media Gateway (MG) or Universal Equipment Module (UEM) into which it is inserted.

Current, power and cooling requirements

Current, power and cooling requirements for the various server platforms are summarized in the following table.

Table 1
Server current, power and cooling requirements

Server	Current @ 120/240 V AC (A)		Required UPS power (W)		Thermal dissipation (Btu)	
	Maximum	Typical	Maximum	Typical	Maximum	Typical
NTDU27 (Intel ISP1100)	2.00/0.90	0.50/0.25	200.00	60.00	682.60	204.78
NTDU97 (HP DL320 G4)	6.00/3.0	4.0/2.0	580.00	400.00	1990.00	1370.00
NTDU99 (IBM x306m)	5.50/2.8	3.00/1.5	550.00	350.00	1024.00	682.00
NTDW61/66 CP PM				30		102
Maximum voltage limits: North America – 90 and 132 V, single phase. Europe and UK – 180 and 250 V, single phase. Frequency: North America – 60 Hz. Europe and UK – 50 Hz. Fuse: Germany – 16 A. The Nortel CP PM server is a circuit card, and is therefore not supplied with power from an AC power outlet directly.						

Redundancy

Signaling Server redundancy ensures that telephony services can withstand single hardware and network failures. It also provides a load-sharing basis for the Terminal Proxy Server (TPS) and an alternative route for the SIP and H.323 Gateway software.

When you plan survivability strategies for the Signaling Server, include a second Signaling Server in the plan. Two Signaling Servers can load share when the system contains multiple Voice Gateway Media Cards. One

Signaling Server is a Leader Signaling Server that is the primary (or master) TPS. The other Signaling Server is a Follower Signaling Server that is a secondary, redundant TPS.

If the Leader Signaling Server fails, an election process takes place and the Follower Signaling Server becomes the master TPS. The IP Phones reregister to the Follower Signaling Server, and system operation resumes. If the Follower fails, the IP Phones registered to the Follower reregister to the Leader Signaling Server.

This process is explained in the following steps:

1. The IP Phones are distributed between the two Signaling Servers (load-sharing). The SIP and H.323 Gateways run on the Leader Signaling Server.
2. The Leader Signaling Server fails.
3. The Follower Signaling Server takes on the role of the Leader Signaling Server and acquires the IP address of the Leader Signaling Server if necessary.
4. The Time-to-Live (TTL) of IP Phones registered with the failed Signaling Server expires, which causes those IP Phones to reset and register with the new Leader Signaling Server.

   Note: Only IP Phones registered with the failed Signaling Server are reset.

5. The new Leader Signaling Server assumes responsibility for the SIP and H.323 Gateways.
6. Normal operation resumes.

Scalability

Table 2 "Signaling Server limits" (page 57) summarizes the limits for each Signaling Server. Use the values in the table as a quick overview for planning. For detailed calculations, refer to *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.

Note: You must consider real-time capacity for a specific application, which can constrain an application in reaching resource limits.

Table 2
Signaling Server limits

Signaling Server component	Limit
NRS	• 5000 total endpoints (up to 5000 SIP endpoints and up to 2000 H.323 endpoints) • 20 000 numbering plan entries (total number of endpoints and routing entries) • 100 000 calls per hour
Terminal Proxy Server (TPS)	• 5000 IP Phones
Virtual Trunks	• Up to 1800 trunks. ***Note:*** This limit depends on the split between SIP and incoming and outgoing H.323 calls. Refer to the Planning and Engineering NTP appropriate for your system for details.

Branch offices

There must be at least one Signaling Server at the main office and each branch office. Each main office can support up to 255 branch offices, and each branch office can support up to 400 IP Phones.

ATTENTION

IMPORTANT!
To provide NRS redundancy in a network with branch offices, Nortel recommends that you configure a Failsafe NRS at each branch office that is not otherwise configured with a Primary or Alternate NRS.

A branch office has 30 default Virtual Trunks. The Media Gateway 1000B (MG 1000B) platform can support up to 92 T1 trunks or 120 E1 trunks, and up to 256 trunks in total.

The total number of IP Phones in all offices can be no greater than the capacity of the main office, as determined using *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 system.

Hardware installation and connection

Contents

This section contains the following information:

Introduction

This chapter contains general instructions to install a Nortel CP PM server and detailed instructions to install a legacy Nortel ISP1100 server. This chapter contains no instructions to install an IBM X306m or HP DL320-G4 COTS 1U server. Please 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 detailed installation instructions. Of particular note, the IBM X306m and HP DL320-G4 servers require four-post rack mounting, as opposed to two-post rack mounting for the Nortel ISP1100 server.

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

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.

Hardware installation

Installation checklist

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

Table 3
Installation checklist

Have you:
Received all server equipment and peripherals?
• For Nortel ISP1100 (NTDU27AA), IBM X306m (NTDU99AAE5), and HP DL320-G4 (NTDU97AA) Signaling Servers
— 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 cable (supplied)
• for a 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
— NTDU0606E6 - CP PM Signaling Server 25cm RJ45 Ethernet Cable kit
— a DTE-DTE null modem cable (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

Have you:
— N0106745 - CP PM Signaling Large System Cabling kit installation instructions — a DTE-DTE null modem cable (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?
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 thus is not mounted in a rack. This section contains instructions for installing 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. For instructions, see "Install the hard drive on a Nortel CP PM Signaling Server" (page 311).

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.

Installation in a Nortel CS 1000M system

The NTDW66AAE5 model of the Nortel CP PM server is designed for use in a CS 1000M system. The first task that must be performed is to install the hard drive shipped with the server. For instructions, see "Install the hard drive on a Nortel CP PM Signaling Server" (page 311).

You can insert the NTDW66AAE5 model into any slot of a CS 1000M Universal Equipment Module (UEM) except slot 7. The External Peripheral Equipment Controller (XPEC) is next to slot 7 and prevents the double wide faceplate of the NTDW66AAE5 model from seating into slot 7.

The next task that you must perform is to install ELAN and TLAN Ethernet ports on the back of the CS 1000M UEM. These ports are used to connect your Nortel CP PM Signaling Server to the ELAN and TLAN Ethernet subnets of your CS 1000M system.

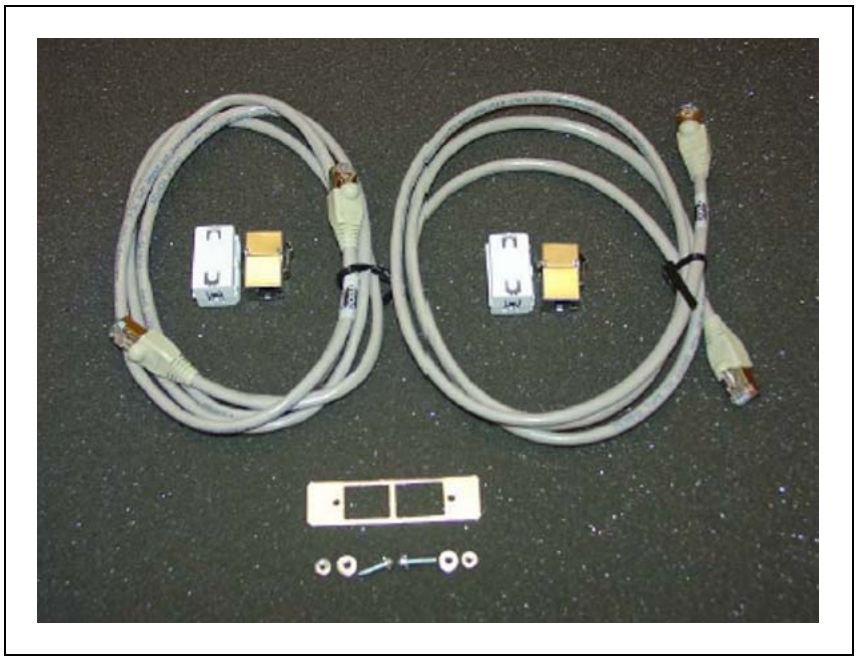
Use the following procedure to install ELAN and TLAN Ethernet ports on the back of a CS 1000M UEM.

ATTENTION
IMPORTANT!
Installing ELAN and TLAN Ethernet ports on the back of a CS 1000M Universal Equipment Module (UEM) is service-disrupting. Power to the shelf must be turned off during this procedure.

Procedure 1
Installing ELAN and TLAN Ethernet ports on the back of a CS 1000M UEM

Step	Action
1	Obtain the special cabling kit (NTDW69AAE5) shipped with the CS 1000M model of the Nortel CP PM Signaling Server (NTDW66AAE5). The NTDW69AAE5 cabling kit should include the items shown in the following figure.

Figure 30
NTDW69AAE5 Cabling Kit contents



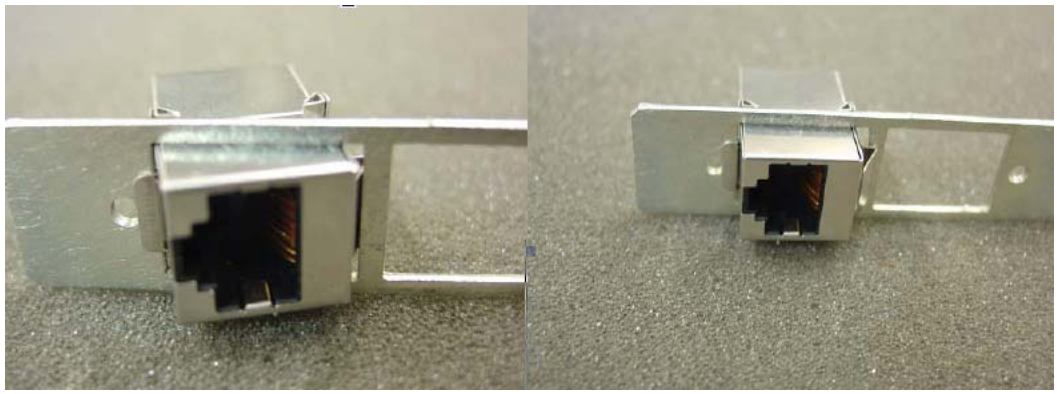
The following is a list of items in the NTDW69AAE5 cabling kit:

- two RJ-45 CAT5 Ethernet patch cables
- two Ethernet port couplers
- one Ethernet port adapter plate
- two screws
- two nuts
- two washers
- two ferrite beads

2 Insert an Ethernet port coupler into the adapter plate.

See the following figure.

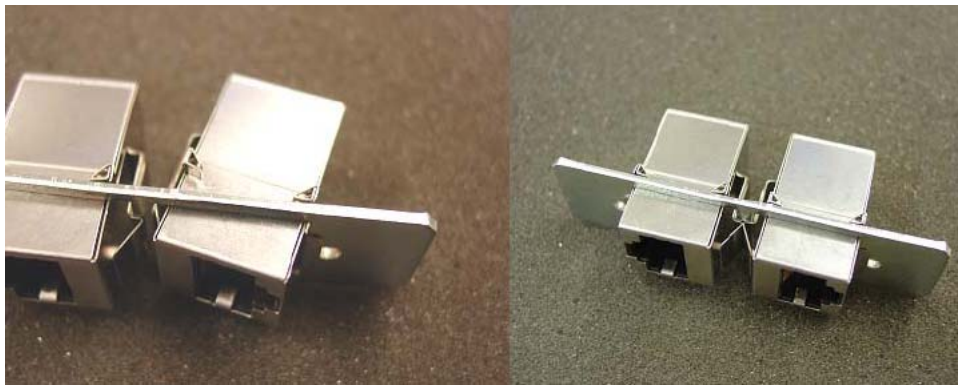
Figure 31
One Ethernet port coupler in adapter plate



3 Insert the other Ethernet port coupler into the adapter plate.

See the following figure.

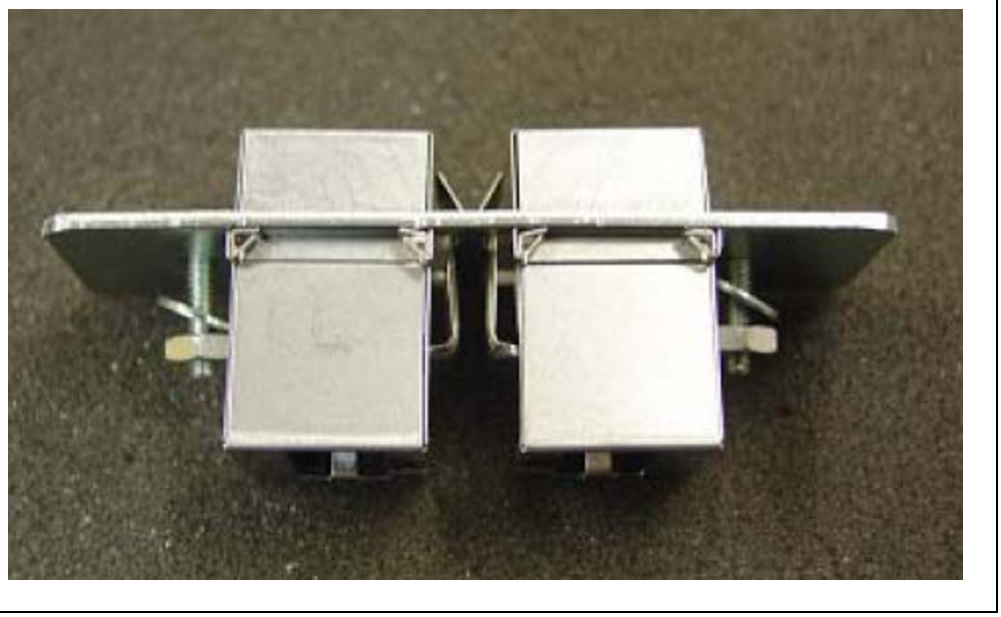
Figure 32
Two Ethernet port couplers in adapter plate



4 Loosely attach screws, washers, and nuts to the Ethernet port adapter plate.

See the following figure.

Figure 33
Ethernet port adapter plate with screws



5 Switch off the UEM power supplies.

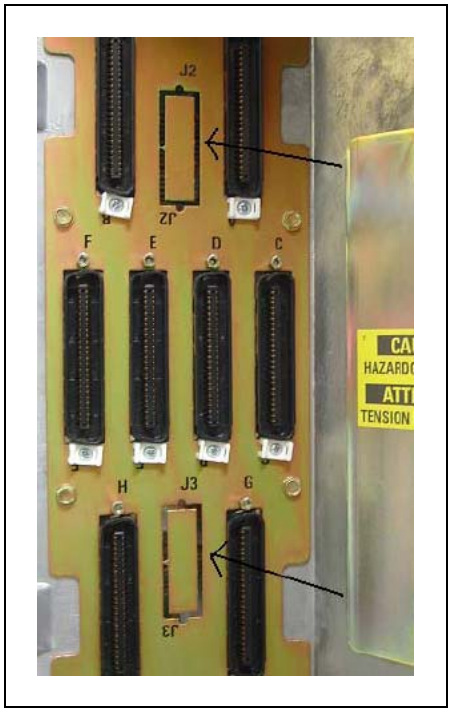
See the following figure.

Figure 34
Shut down UEM power supplies

6 Select one of the J2-J5 knock-out plates on the back of the UEM.

See the following figure.

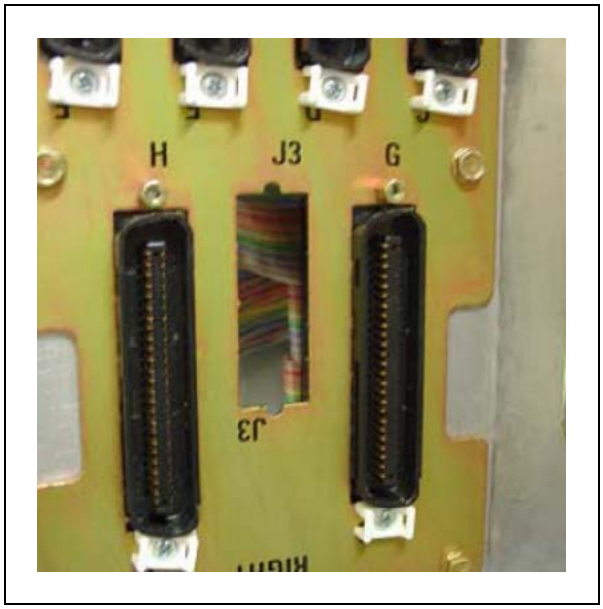
Figure 35
J2-J5 plates on back panel of UEM



7 Knock out the metal plate from selected J2-J5 location.

See the following figure.

Figure 36
Selected J2-J5 plate on back panel of UEM



This provides a hole through which the Ethernet patch cables are routed, and to which the Ethernet port adapter plate is attached.

8 Establish an ELAN port on the back panel of the UEM.

a. Insert the end of one of the RJ-45 CAT5 Ethernet patch cables (supplied) into the ELAN network interface (ELAN port) on the faceplate of the server.

b. Route the Ethernet patch cable through the hole you made in the back panel of the UEM.

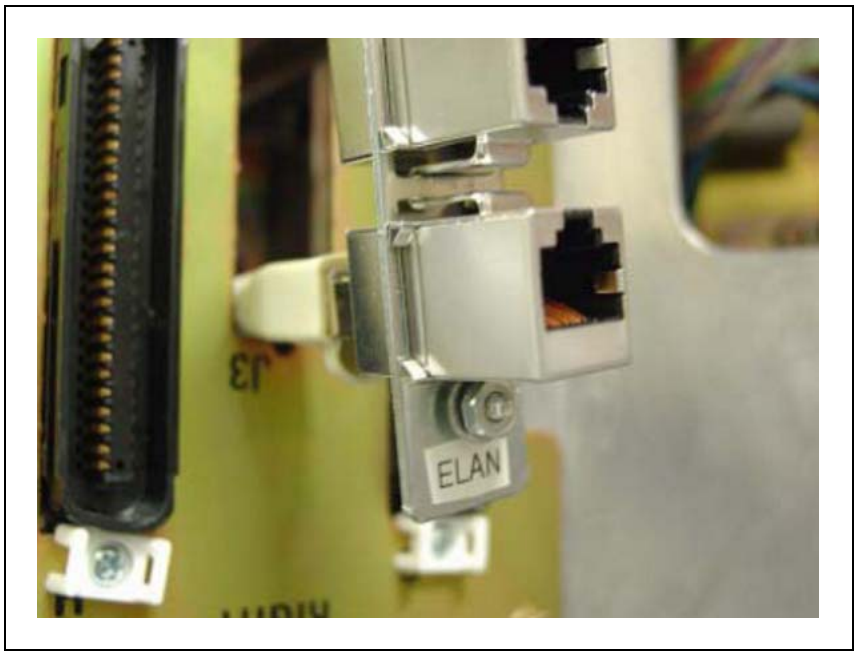
c. Plug the other end of the Ethernet patch cable into one of the Ethernet port couplers mounted in the Ethernet port adapter plate.

d. Label the Ethernet port coupler as ELAN.

See the following figures.

Figure 37
ELAN connection on faceplate

Figure 38
ELAN connection on Ethernet port coupler



9 Connect the server to the TLAN subnet.

a. Insert one end of the remaining RJ-45 CAT5 Ethernet patch cable (supplied) into the TLAN network interface (TLAN port) on the faceplate of the server.

b. Route the Ethernet patch cable through the hole you made in the back panel of the UEM.

c. Plug the other end of the Ethernet patch cable into the remaining Ethernet port coupler mounted in the Ethernet port adapter plate.

d. Label the Ethernet port coupler as TLAN.

See the following figures.

Figure 39
TLAN connection on faceplate

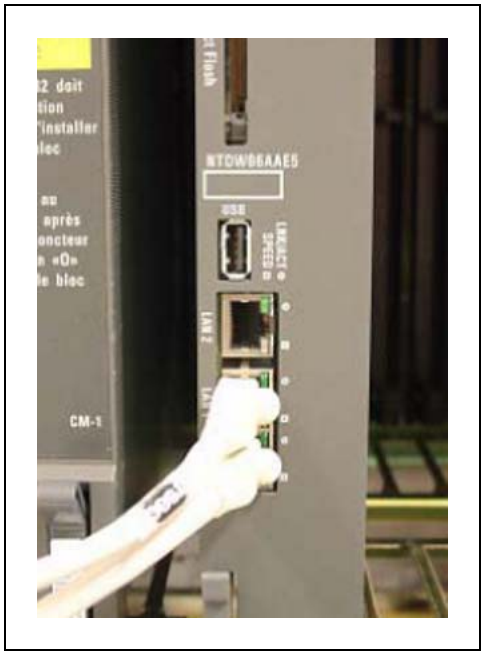
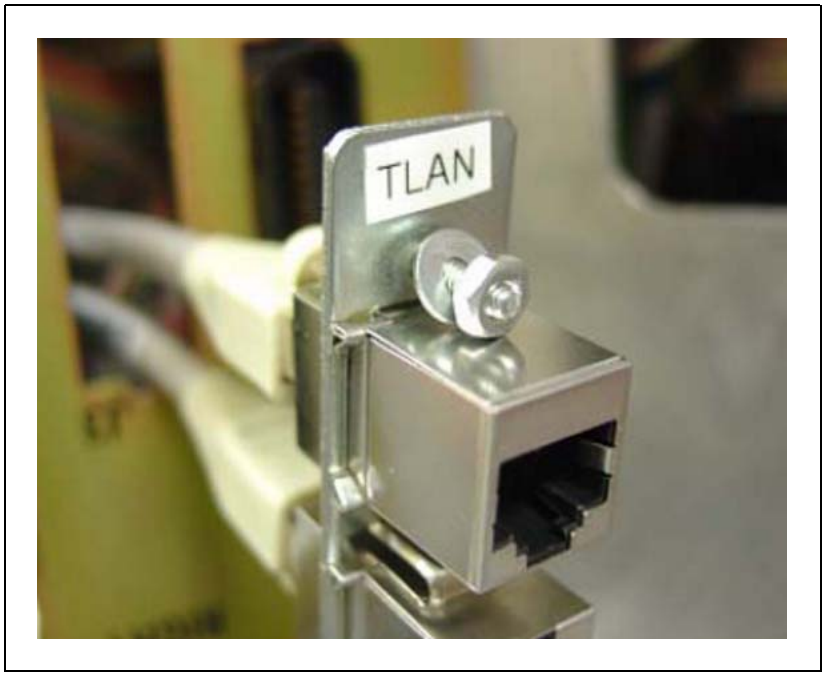


Figure 40
TLAN connection on Ethernet port coupler



10 Fit the Ethernet port adapter plate into the hole on the back of the UEM and tighten the screws.

See the following figure.

Figure 41
Installed Ethernet port adapter plate

11 Attach the ferrite beads to the Ethernet patch cables.

See the following figure.

Figure 42
Attached Ethernet patch cable ferrite beads

—End—

Install a Nortel ISP1100 server

This section describes how to install a Nortel ISP1100 server in a 19-inch rack.

Accessories pouch

You require specific hardware to install the Nortel ISP1100 server in a 19-inch rack. This hardware is included in the Nortel ISP1100 server accessories pouch. The accessories pouch must contain the following items:

- Two support brackets (A)
- Two rack-mounting brackets (B)
- Six rack-mount bracket screws (ten 25 x 1/4 inch pan-head Phillips)

Refer to Figure 43 "Nortel ISP1100 server brackets" (page 72). If any parts are missing, contact your supplier immediately.

Figure 43
Nortel ISP1100 server brackets

CAUTION
The load rating for this mounting kit is 50 pounds (23 kilograms). If you exceed this limit, damage or injury can occur.

Preparing for rack-mounting

Procedure 2
Preparing the Nortel ISP1100 server for rack-mounting

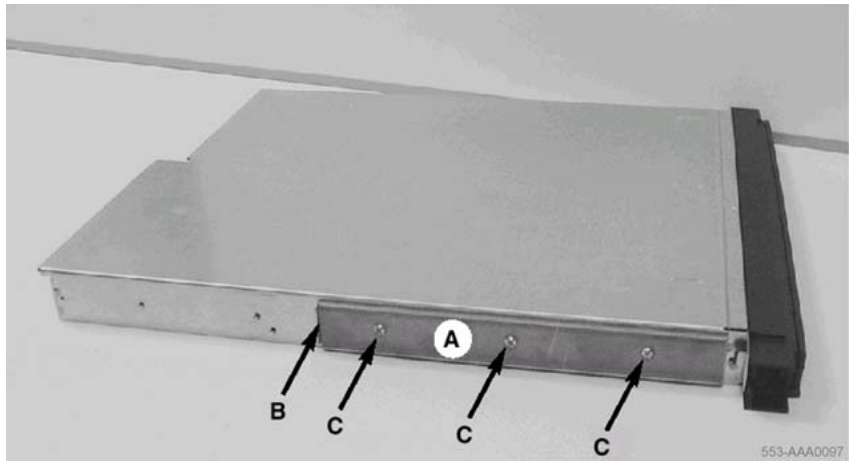
Step	Action

The Front Mount Bracket assembly is not intended for use as a slide rail system. You must firmly attach the Nortel ISP1100 server to the rack.

1 Make sure the Nortel ISP1100 server is not plugged in to an electrical outlet.

2 Align the end of the rail (A in Figure 43 "Nortel ISP1100 server brackets" (page 72)) on the side of the Nortel ISP1100 server with the flange (B in Figure 44 "Nortel ISP1100 Support bracket" (page 73)) toward the back of the Nortel ISP1100 Server. See Figure 44 "Nortel ISP1100 Support bracket" (page 73).

Figure 44
Nortel ISP1100 Support bracket



3 Align the screw holes in the rack-mount rail to the mating holes in the side of the Nortel ISP1100 server. Use three screws (C) on each side.

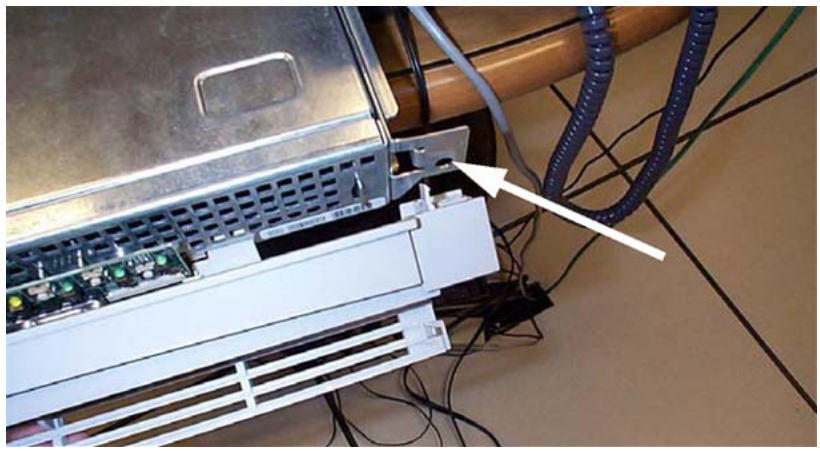
Note: Hand tighten the screws to prevent cross-threading, and use a Phillips screwdriver to secure them.

4 Attach the bezel door to the faceplate of the Nortel ISP1100 server.

Refer to the following two figures.

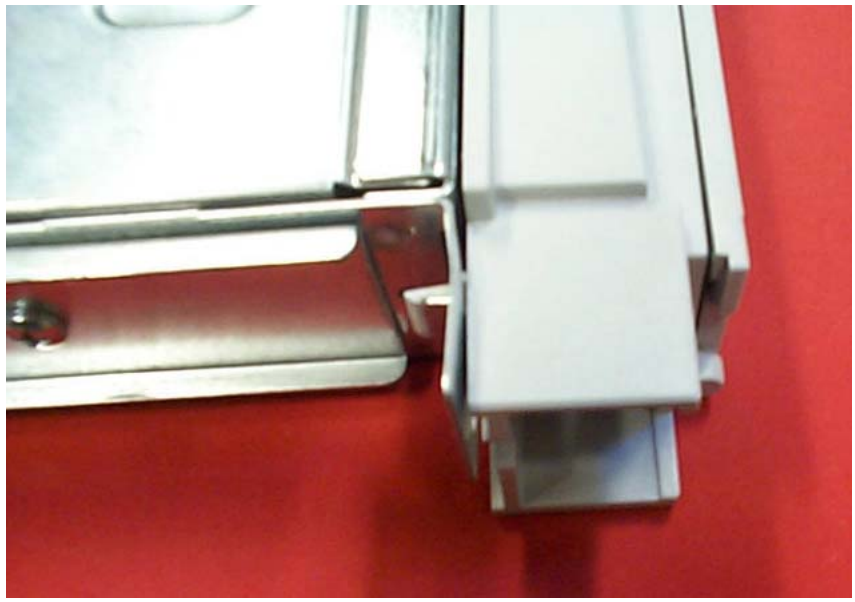
Figure 45
Nortel ISP1100 server - left hinge mount

Figure 46
Nortel ISP1100 server - right hinge mount



When you attach the door to the Nortel ISP1100 server and rack-mount apparatus, it appears as shown in the following figure.

Figure 47
Nortel ISP1100 server - snapped-in bezel door



—End—

Rack-mounting the Nortel ISP1100 server

Carefully read the following warnings before you install the Nortel ISP1100 server in the rack.

DANGER
DISCONNECT AC POWER
Make sure the Nortel ISP1100 server is completely disconnected from any AC power source before you perform this procedure. Pressing the Power button DOES NOT turn off power to the Nortel ISP1100 server. Some circuitry in the Nortel ISP1100 server can continue to operate even though the front panel Power button is off. Failure to disconnect the Nortel ISP1100 server from its AC power source can result in personal injury or equipment damage.

WARNING
MAIN AC POWER DISCONNECT
You must install an AC power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labeled as controlling power to the entire unit, not only to the Signaling Servers.

WARNING
OVERCURRENT PROTECTION
The Nortel ISP1100 server is designed for an AC line voltage source with up to 20 amperes (A) of over-current protection. If you install the power system for the equipment rack on a branch circuit with more than 20 A of protection, provide supplemental protection for the Nortel ISP1100 server. If you install more than one server in the rack, the power source for each server must be from a separate branch circuit.

Procedure 3
Rack-mounting the Nortel ISP1100 server

Step	Action
1	Attach the rack-mount brackets (B in Figure 43 "Nortel ISP1100 server brackets" (page 72) to the front of the equipment rack. Install the left and right side brackets at an equal height. Use standard length screws in the top and bottom drill holes of the bracket. See Figure 48 "Nortel ISP1100 server - installed rack-mount bracket" (page 76).

Figure 48
Nortel ISP1100 server - installed rack-mount bracket

Step	Action
2	When both brackets are in place, perform the following tasks: a. Align the rack-mount brackets on the Nortel ISP1100 server with the slide rail system on the rack posts. b. Slide the Nortel ISP1100 server into place. Refer to Figure 49 "Rack-mounting the Nortel ISP1100 server" (page 77).

Figure 49
Rack-mounting the Nortel ISP1100 server

3 Tighten the screws through the faceplate of the Nortel ISP1100 server to the rack-mount bracket.

Note: Do not apply excessive torque while you tighten the bolts. The bezel door is plastic and does not require or withstand overtightening.

—End—

Hardware connection

Connection checklist

Before you connect a server, complete the following checklist.

Table 4
Connection checklist

Have you:
Obtained the power cable if you are connecting an IBM X306m, HP DL320-G4, or Nortel ISP1100 Server? Check that the power cord is the correct type for the host region. Replace the cord with one of the correct type if necessary.

Have you:
WARNING Do not modify or use a supplied AC power cord if it is not the correct type required for the host region. **ATTENTION** Nortel CP PM servers are powered through the backplane of the Media Gateway, Universal Equipment Module or 11C cabinet into which they are installed and thus require no power cord.
Obtained a serial cable (DTE-DTE null modem cable) to connect the server to a maintenance terminal?
Obtained the NTAK19EC cable (if you are connecting a Nortel CP PM server)? This cable adapts the 50-pin MDF connector on the back of the shelf of the Media Gateway, Universal Equipment Module, or 11C cabinet to a 25-pin DB connector.
Obtained the CAT5 cables (or better) to connect the server to the ELAN and TLAN subnets?

Connect a Nortel CP PM server

This section contains instructions for connecting 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. It also contains instructions for connecting a maintenance terminal to the Nortel CP PM Signaling Server.

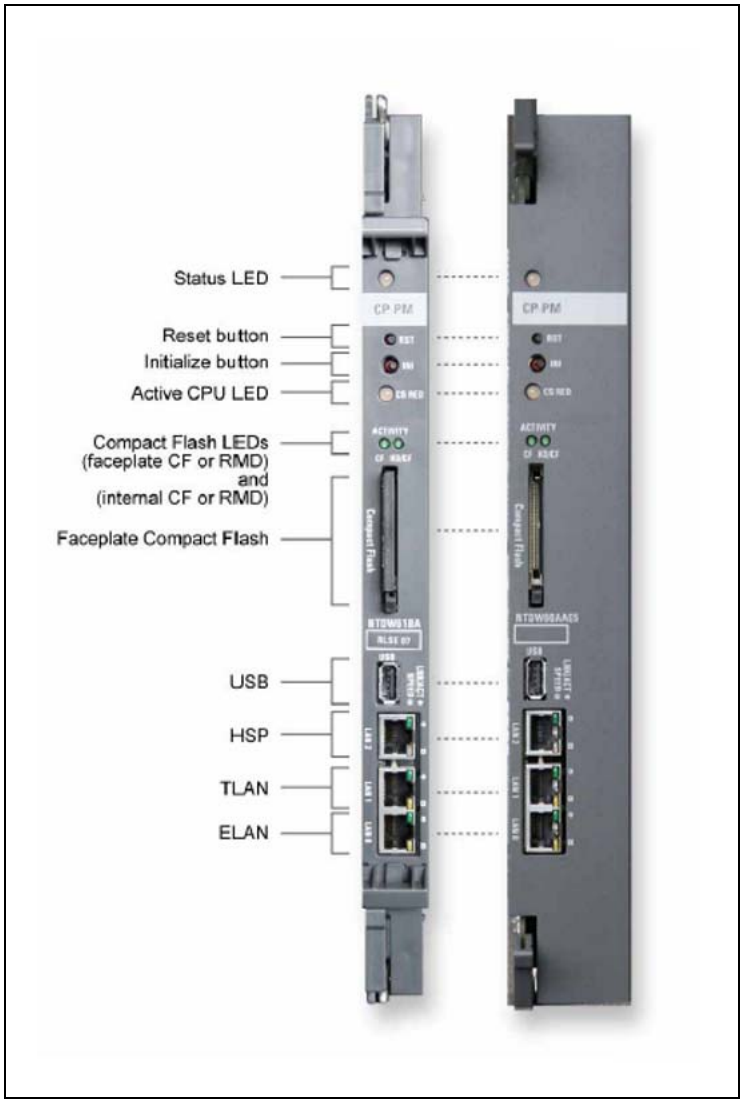
The NTDW61BAE5 model of the Nortel CP PM Signaling Server was designed for use in a CS 1000E system. As such, it is inserted into a slot of the Media Gateway (MG 1000E or MG 1000B). The Media Gateway also hosts the Media Gateway Controller (MGC) that has Ethernet ports for connecting to the ELAN and TLAN subnets of your CS 1000 system. However, it is common in a CS 1000E system for the Call Server to be connected to the MGC through these ELAN and TLAN Ethernet ports. If the Call Server is not connected to the MGC through these Ethernet ports, the NTDW61BAE5 model of the CP PM Signaling Server uses them to connect to the ELAN and TLAN subnets of the CS 1000E system. If the Call Server is using the MGC ELAN and TLAN Ethernet ports, the Nortel CP PM Signaling Server is connected 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 was designed for use in a CS 1000M system. As such, 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 (see Procedure 1 "Installing ELAN and TLAN Ethernet ports on the back of a CS 1000M UEM" (page 62)).

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 50
Faceplates of the Nortel CP PM server



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

Procedure 4
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 DTE-DTE null modem 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 DTE-DTE null modem serial cable to the 25-pin DB connector at the end of the NTAK19EC cable. c. Connect the other end of the DTE-DTE null modem 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 5 "Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000E system " (page 81) • If you have a CS 1000M system, perform Procedure 6 "Connecting a CP PM Signaling Server to the ELAN and TLAN subnets of a CS 1000M system " (page 82)
4	Set the baud rate for the serial port on the Signaling Server to 9 600 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 7 "Changing the baud rate on a Nortel CP PM Signaling Server" (page 83).

5 Configure the connected maintenance terminal (see "Configure a maintenance terminal" (page 291).

—End—

Use 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 5

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 Call Server is not connected to the Media Gateway Controller (MGC) — Insert the end of one of the 25-cm RJ-45 CAT5 Ethernet cables shipped with the server (NTDU0606E6) into the ELAN network interface port (ELAN port) on the faceplate of the server — Insert the other end of the 25-cm RJ-45 CAT5 Ethernet cable into the MGC ELAN 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 ELAN network interface port (ELAN port) on the faceplate of the 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 Call Server is not connected to the Media Gateway Controller (MGC) — Insert the end of one of the 25-cm RJ-45 CAT5 Ethernet cables shipped with the server (NTDU0606E6) into the TLAN network interface port (TLAN port) on the faceplate of the 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 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 can not use the 25-cm CAT5 Ethernet cables shipped with the Signaling Server (NTDU0606E6). 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.

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

ATTENTION

IMPORTANT!

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

Procedure 6

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 (see Procedure 1 "Installing ELAN and TLAN Ethernet ports on the back of a CS 1000M UEM" (page 62).
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 (see Procedure 1 "Installing ELAN and TLAN Ethernet ports on the back of a CS 1000M UEM" (page 62).

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

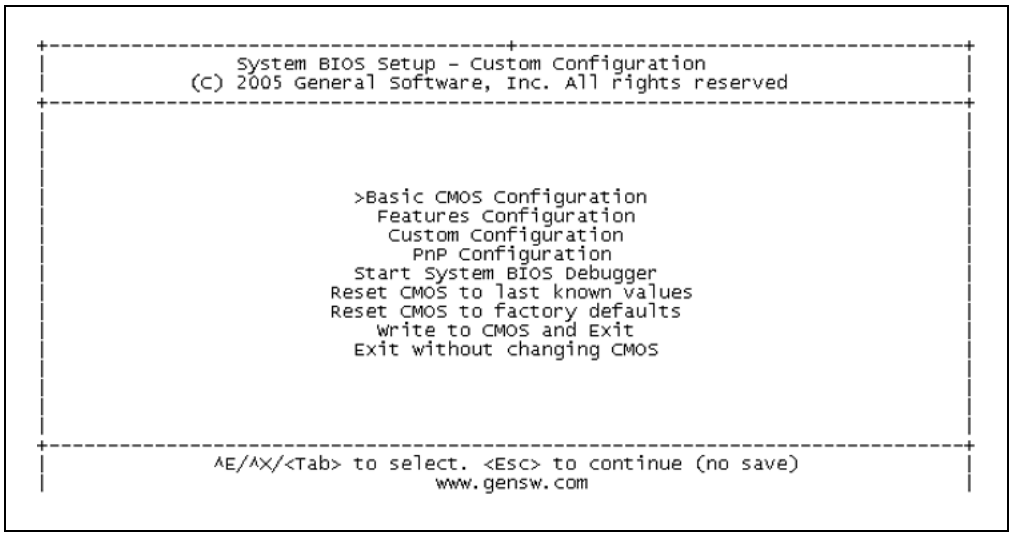
—End—

Use the following procedure to verify or change the baud rate on a Nortel CP PM Signaling Server.

Procedure 7
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.

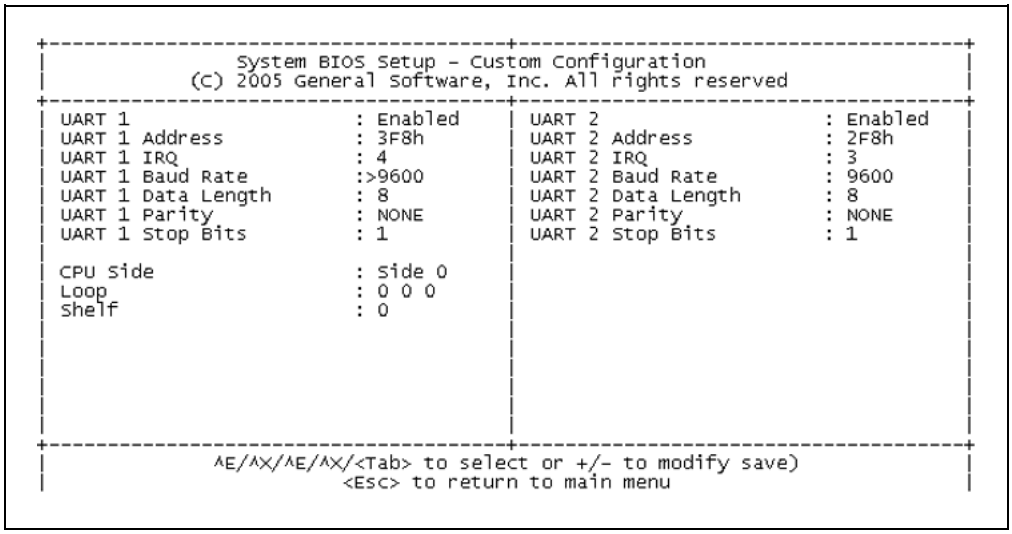
Figure 51
Nortel CP PM System BIOS menu



3 Navigate to and select the **Custom Configuration** option.

The Custom Configuration screen appears.

Figure 52
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 the **Esc** key to save the settings and return to the BIOS Menu screen.,

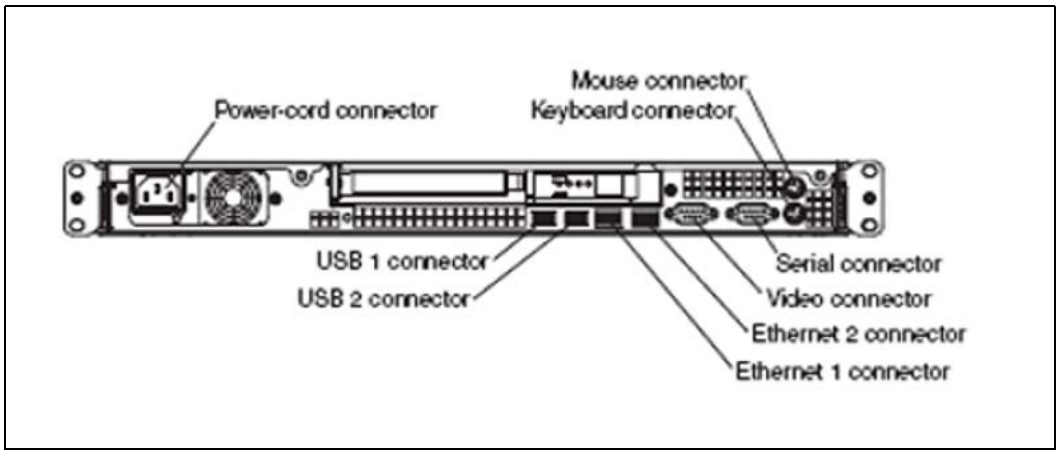
7 Select the **Write to CMOS and Exit** option to exit the Nortel CP PM server BIOS menu system.

—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 53
Back of an IBM X306m server



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

Procedure 8
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 the server is used. 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's back panel. Plug the male end of the AC power cord into the AC power source (wall outlet).

5 Set the baud rate for the serial port on the Signaling Server to 9 600 b/ps. See Procedure 9 "Changing the baud rate on an IBM X306m Signaling Server" (page 86) for instructions.

Note: The IBM X306m Signaling Server ships with the serial port configured to 9600 b/ps.

6 Configure the connected maintenance terminal (see "Configure a maintenance terminal" (page 291)).

—End—

Use the following procedure to verify or change the baud rate on an IBM X306m Signaling Server.

Procedure 9
Changing the baud rate on an IBM X306m Signaling Server

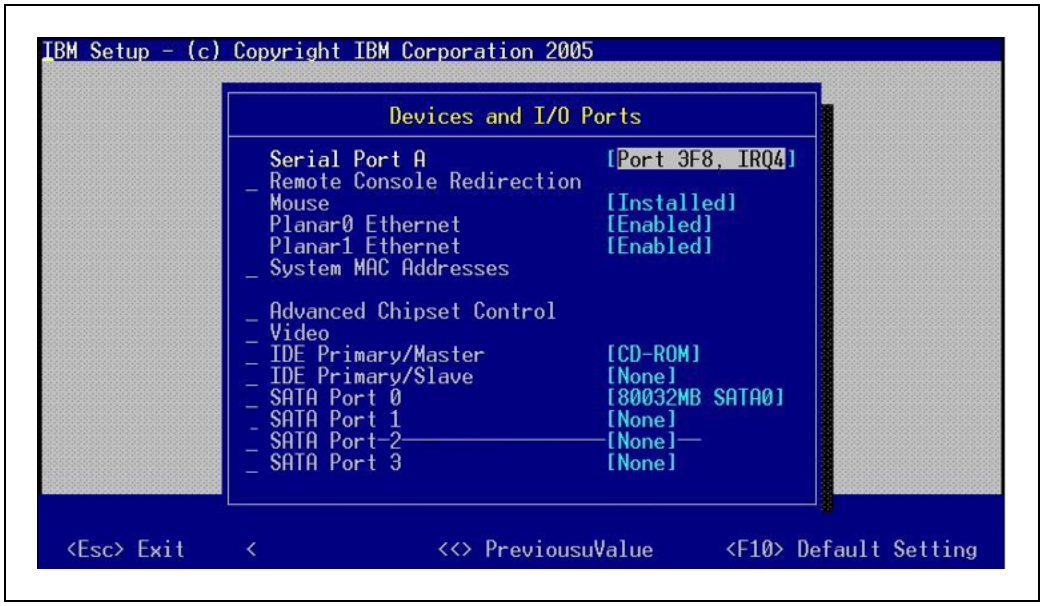
Step	Action
1	Press the Power switch to boot the server. The server boots and a **Press F1 for Configuration/Setup** message appears on the maintenance terminal. ***Note:*** If the server is already up and running, press the **Reset** button on the front of the IBM X306m server to reboot and receive 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 54
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.

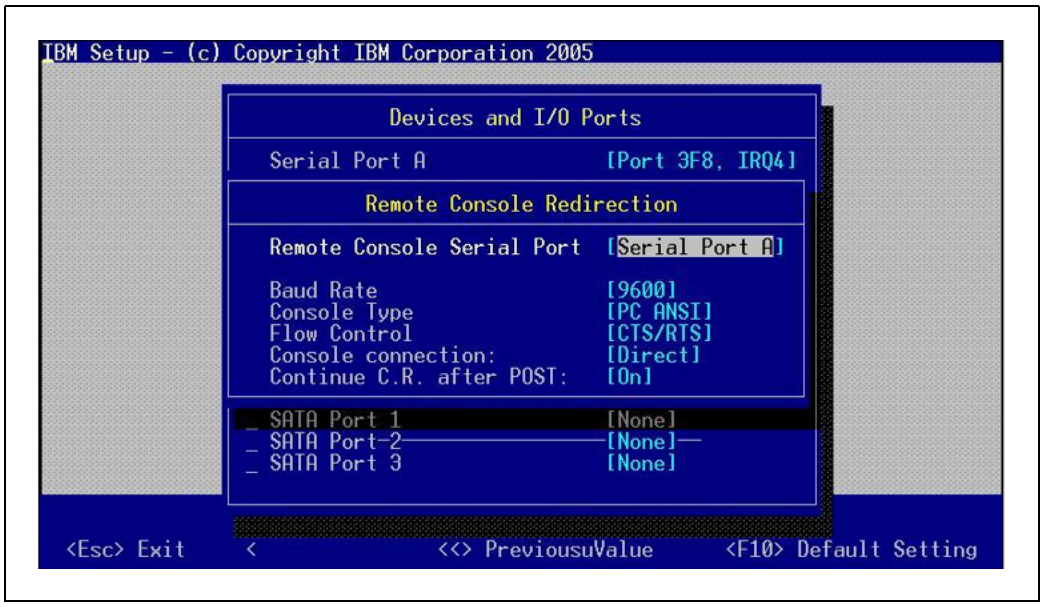
Figure 55
IBM X306m server Devices and I/O Ports menu



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

The Remote Console Redirection screen appears.

Figure 56
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 will reboot automatically.

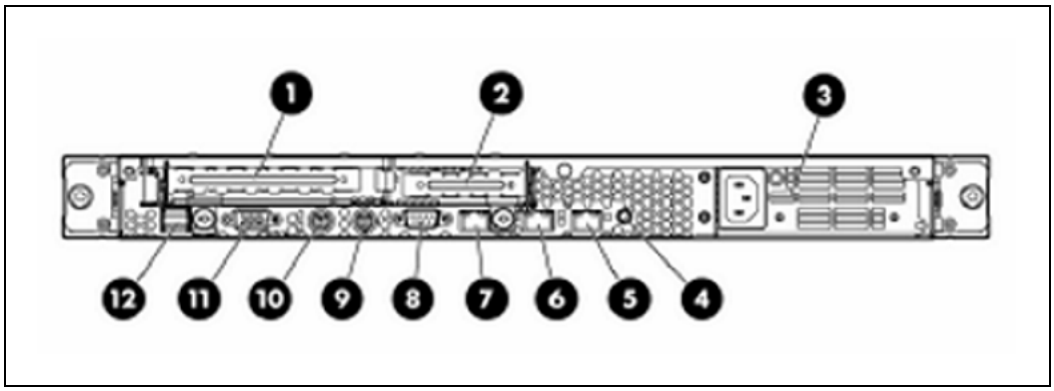
—End—

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

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 57
Back of an HP DL320-G4 server



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

Procedure 10
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 11 "Configuring the COM1 serial port on an HP DL320-G4 Signaling Server" (page 90) for instructions.

6 Set the baud rate for the COM1 serial port on the Signaling Server to 9 600 b/ps.

See Procedure 12 "Changing the baud rate on an HP DL320-G4 Signaling Server" (page 92) 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 (see "Configure a maintenance terminal" (page 291).

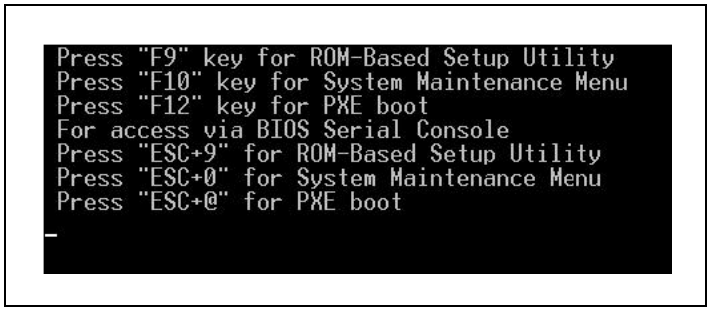
—End—

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 11
Configuring the COM1 serial port on an HP DL320-G4 Signaling Server

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

Figure 58
HP DL320-G4 server boot screen



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

The RBSU menu screen appears.

Figure 59
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.

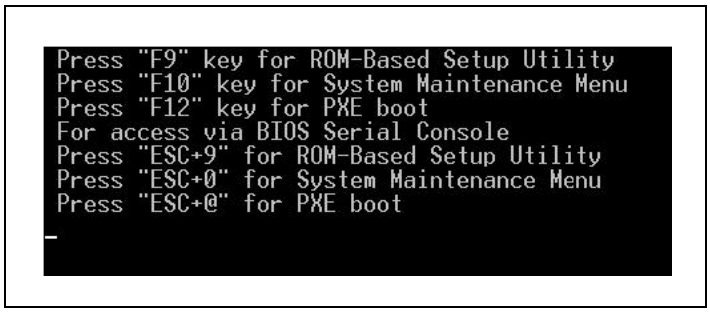
—End—

Use the following procedure to verify or change the baud rate on an HP DL320-G4 Signaling Server.

Procedure 12
Changing the baud rate on an HP DL320-G4 Signaling 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



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 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.

Connect a Nortel ISP1100 server

In geographic regions that are susceptible to electrical storms, Nortel recommends that you plug the Nortel ISP1100 server into an AC surge suppressor.

Figure 62
Back of a Nortel ISP1100 server

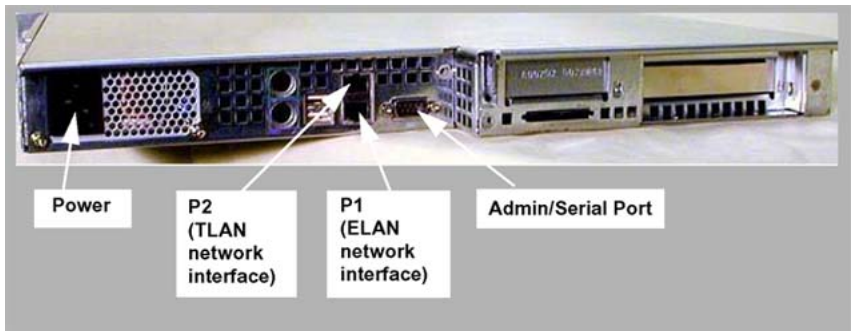


Figure 63
Nortel ISP1100 server with open bezel door

Refer to the two preceding figures when performing the following procedure.

Procedure 13
Connecting a Nortel ISP1100 server

Step	Action
1	Connect the server to the TLAN subnet.

Insert the RJ-45 CAT5 (or better) cable into the P2 port (TLAN network interface) on the back of the server. The P2 port (TLAN network interface) is the top port of the two network interface ports.

2 Connect the server to the ELAN subnet.

Insert the RJ-45 CAT5 (or better) cable into the P1 port (ELAN network interface). The P1 port (ELAN network interface) is the bottom port of the two network interface ports.

3 Connect a DTE–DTE null modem serial cable (shipped with the Nortel ISP1100 server) from the serial port on the back of the server 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 left side of the back panel. Plug the male end of the AC power cord into the AC power source (wall outlet).

5 Power up the server.

a. Open the bezel door on the front of the server to access the Power switch:

1. Grasp the tab at each end of the bezel door.
2. Gently pull the tabs out and down to open the hinged bezel door.

b. Press the Power switch.

6 Change the baud rate for the serial port on the Signaling Server to 9 600 b/ps if desired.

Note: The Nortel ISP1100 Signaling Server ships with the serial port configured to 19200 b/ps. The baud rate can be left at this speed with no operational impact.

Other available speeds for the serial port are 9600, 38400, and 115200 b/ps. To verify or change the baud rate on an Nortel ISP1100 Signaling Server, see Procedure 14 "Changing the baud rate on a Nortel ISP1100 Signaling Server" (page 96).

7 Configure the maintenance terminal (see "Configure a maintenance terminal" (page 291).

—End—

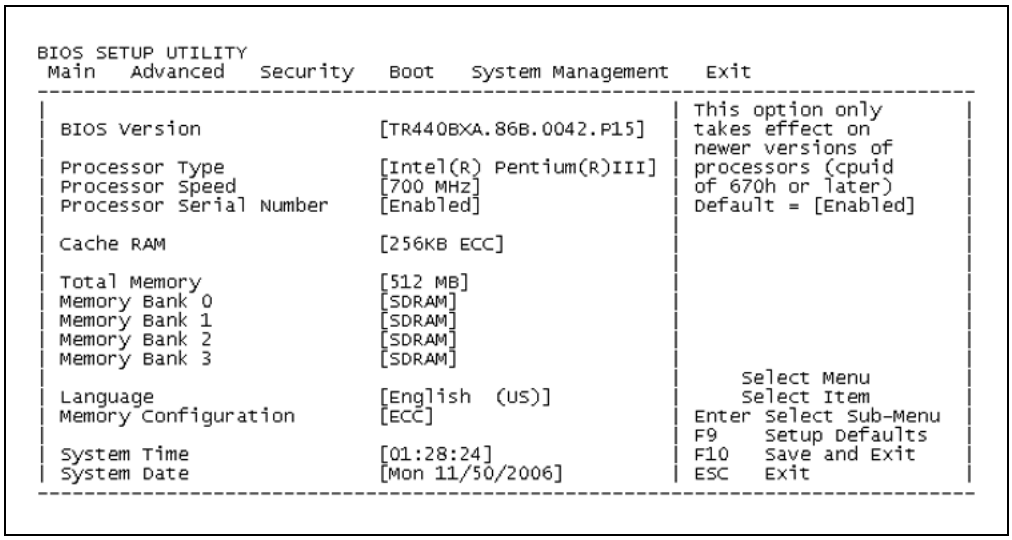
Refer to the Signaling Server Product Guide on the resource CD-ROM shipped with the Nortel ISP1100 server for additional operating information.

Use the following procedure to verify or change the baud rate on a Nortel ISP1100 Signaling Server.

Procedure 14
Changing the baud rate on a Nortel ISP1100 Signaling Server

Step	Action
1	Press the **INI** button on the front of the Signaling Server to reboot the Signaling Server.
2	Press the **F2** key to invoke the BIOS Setup menu. The Nortel ISP1100 System BIOS Menu screen appears.

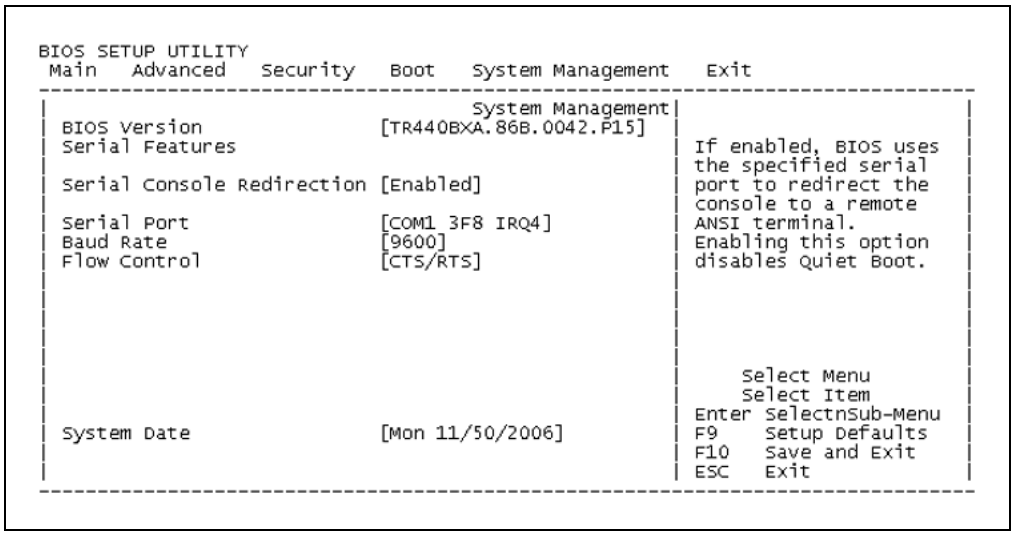
Figure 64
Nortel ISP1100 system BIOS menu



3 Navigate to the Sytem Management page and select the Serial Features option.

The Serial Features screen appears.

Figure 65
Nortel ISP1100 Serial Features



4 Navigate to the **Baud Rate** option and change as necessary.

5 Press the **F10** key to save your changes and to exit the Nortel ISP1100 server BIOS menu system.

—End—

Software Installation Tool

Contents

This section contains information on the following topics:

Introduction

The Signaling Server Software Installation Tool is used to perform the following tasks:

- Install Signaling Server software and basic system components, and capture (restore) basic system configuration parameters (see "Software installation" (page 111).
- Upgrade installed Signaling Server software and basic system components (see "Software upgrade from Succession 3.0" (page 151) and "Software upgrade from Communication Server 4.0 or 4.5" (page 185).
- Reconfigure an installed Signaling Server (see "Signaling Server reconfiguration" (page 199).
- Perform Signaling Server maintenance activities (see "Signaling Server Maintenance" (page 291).

ATTENTION

Important!
The Signaling Server is out of service during the software installation and upgrade processes.

The Signaling Server Software Installation Tool runs from the CD drive on IBM X306m, HP DL320-G4 and Nortel ISP1100 servers, and directly from the hard drive on new Nortel CP PM Signaling Servers. However, if you

replace the hard drive on a Nortel CP PM server, you will need to install CS 1000 Release 5.0 Signaling Server software and system components on the new hard drive. In this case, the Signaling Server Software Installation Tool runs from the faceplate CF drive on the Nortel CP PM server.

> ***Note:*** A new Nortel CP PM Signaling Server has CS 1000 Release 5.0 Signaling Server software, operating system, and web files preloaded on the hard drive.

After you install the Signaling Server software and enter basic system configuration information, you can configure the Signaling Server components using the web-based Element Manager interface. See *Element Manager: System Administration (NN43001-632).*

Signaling Server Software

The Signaling Server Software Installation Tool and all Signaling Server software and system components are provided on a Signaling Server Software compact disk (CD) for use in IBM X306m, HP DL320-G4, and Nortel ISP1100 Signaling Servers. To obtain a copy of the Signaling Server Software CD, see "Obtain a Signaling Server software compact disk" (page 100).

The Signaling Server Software Installation Tool and all Signaling Server software and system components are provided on a CP PM Signaling Server Software compact flash (CF) card for use in Nortel CP PM Signaling Servers. To obtain a copy of the CP PM Signaling Server Software CF, card, see "Obtain a CP PM Signaling Server software compact flash card" (page 102).

Obtain a Signaling Server software compact disk

This section describes the steps necessary to download a Signaling Server Software CD image from the Nortel Electronic Software Download site and to create a Signaling Server Software CD. This CD is used to load Signaling Server software and system components onto an IBM X306m, HP DL320-G4, and Nortel ISP1100 Signaling Server.

A single .ISO file is provided to create the Software CD. This file is a ready-to-burn ISO9660 CD image that creates a bootable CD that complies to the El Torito specification. You must use CD writer software that can create a CD from this image. Because the CD image is preconfigured, your software automatically creates a bootable CS 1000 Release 5.0 CD that contains the Signaling Server Software Installation Tool and all required components. See your CD writer software help pages for instructions to create a CD from an .ISO file. Also review the README file that is associated with the Nortel Signaling Server Software download.

Use the following procedure to download the Signaling Server Software CD image.

Procedure 15
Downloading the Signaling Server Software CD image

Step	Action
1	Connect to the Nortel website at www.nortel.com.
2	Navigate to the **Software Downloads** page. a. Click **Software Downloads** in the **Support & Training** menu. The **Technical Support** page appears. b. Click **Product Families.** The **Products Families** list appears. c. Click **Communication Servers.** The **By Product Family** web page appears. d. Under the **Enterprise Communication Servers > Signaling Server and IP Peer Networking** headings, click **Software.**
3	Download the Signaling Server CD image. a. Click the link for the appropriate **Signaling Server CD image.** The CD image includes the Signaling Server software as well as IP Phone firmware and Voice Gateway Media Card loadware. b. If you are not logged on to a My Nortel account, click **Log In** to sign in. ***Note:*** If you are not registered to access this web site, refer to the CS 1000 product bulletin for registration instructions. c. The **Software: Software Details Information** page appears. Click the link next to **File Download.** d. In the **Save As** window, choose the desired path to save the file to the local disk on your PC, and click **Save.**

—End—

Use the following procedure to create a Signaling Server Software CD from a Signaling Server Software CD image.

Procedure 16
Creating a Signaling Server Software CD

Step	Action
1	Use the software option to "create" a CD from the CD image. Do not drag and drop, as this can result in a file copy and a CD that does not work. Do not write the .ISO file to the CD. ***Note:*** Select the disk-at-once write option.
2	Close the session.
3	Label the CD appropriately. For example, Signaling Server, sse-x.xx.xx where x.xx.xx represents the Signaling Server software version.

—End—

The Software CD must be readable in a standard CD drive. After you create a CD from the CD image, the CD contains several directories and files. If you cannot create a CD, refer to the CD writer documentation.

Obtain a CP PM Signaling Server software compact flash card

This section describes the steps necessary to download a Signaling Server Software Load zip file from the Nortel Electronic Software Download site and to create a Signaling Server Software CF Card. This CF card is necessary to load Signaling Server software and system components onto a CP PM Signaling Server.

When all Signaling Server Software and system components are loaded successfully onto the CP PM Signaling Server CF Card, it can be used to load the Signaling Server software and system components onto a CP PM Signaling Server.

Use the following procedure to download the CP PM Signaling Server Software Load zip file.

Procedure 17
Downloading the CP PM Signaling Server Software Load zip file

Step	Action
1	Connect to the Nortel website at www.nortel.com.
2	Navigate to the **Software Downloads** page. a. Click **Software Downloads** in the **Support & Training** menu. The **Technical Support** page appears.

b. Click **Product Families.** The **Products Families** list appears.

c. Click **Communication Servers.** The **By Product Family** web page appears.

d. Under the **Enterprise Communication Servers > Signaling Server and IP Peer Networking** headings, click **Software.**

3 Download the Signaling Server Software Load zip file.

a. Click the link for the appropriate **Signaling Server Software Load zip file.**

The zip file includes the Signaling Server software as well as IP Phone firmware and Voice Gateway Media Card loadware.

b. If you are not logged on to a My Nortel account, click **Log In** to sign in.

Note: If you are not registered to access this web site, refer to the CS 1000 product bulletin for registration instructions.

c. The **Software: Software Details Information** page appears. Click the link next to **File Download.**

d. In the **Save As** window, identify a folder on your local PC in which to save the zip file, and click **Save.**

—End—

Use the following procedure to create a CP PM Signaling Server Software CF Card.

Procedure 18
Creating a CP PM Signaling Server Software CF Card

Step	Action
1	Navigate to the **Temp** folder on your local PC (or the folder into which you downloaded the CP PM Signaling Server Load zip file).
2	Unzip the Signaling Server Software Load zip file. This results in: • parent directory (cf:\) • six child directories (plus other required loadware files) — \licenses — \load — \mkboot

— \opensrc

— \sse49105.p (identifies current release of Signaling Server software in body of folder name)

— \symtabs

3 Open the **\mkboot** directory and locate the mkbootrmd.bat file.

This batch file is used to format the CF card.

4 Insert the CF card into a PCMCIA adapter and insert it into your PC.

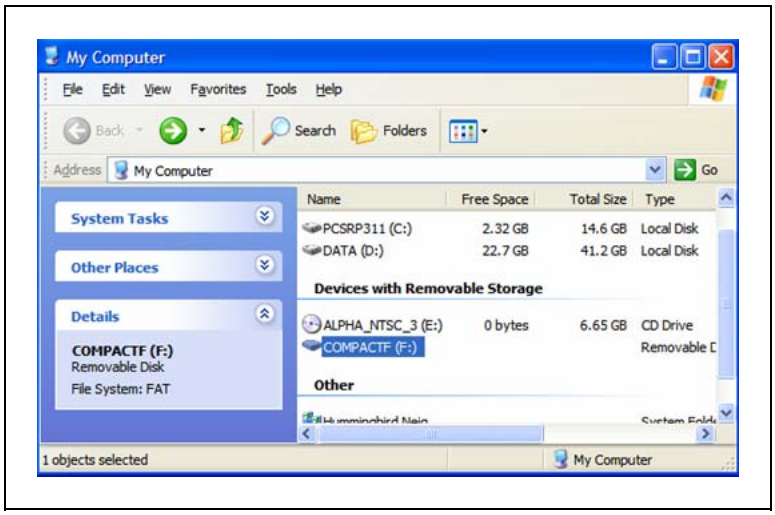
ATTENTION

IMPORTANT!
The CF card must be 512Mb (CPC# A0548249).

5 Click on **My Computer** to verify the drive letter assigned to the CF drive.

The **My Computer** screen appears.

Figure 66
My Computer



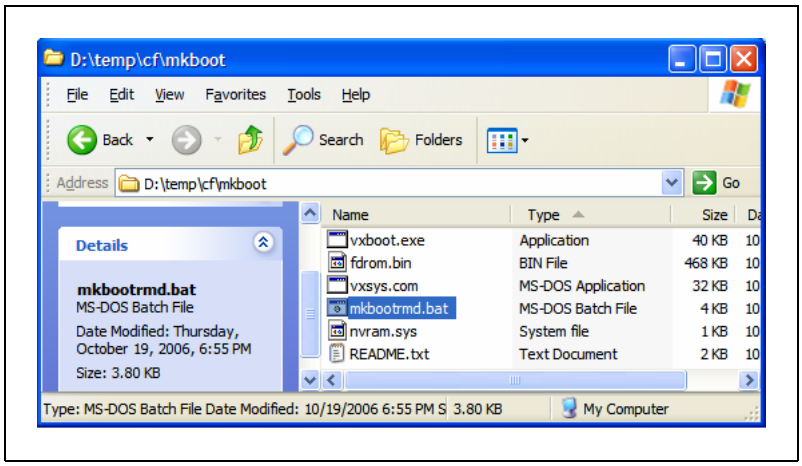
In this example, drive F: is assigned to the CF drive.

6 Navigate to the **Temp** folder on your local PC ((or the folder into which you downloaded the CP PM Signaling Server Load zip file).

7 Open the \mkboot folder and locate the mkbootrmd.bat file.

The following is an example of what you should see on the screen.

Figure 67
Run mkbootrmd.bat

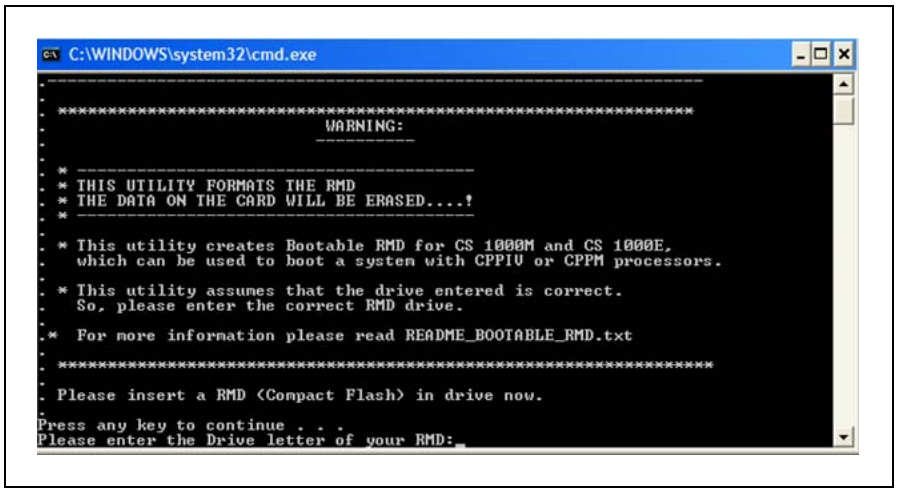


8 Double click the mkbootrmd.bat file to start the application (this batch file is used to format the CF card).

You can press any key to continue when prompted.

The line asking you to enter a CF drive letter appears on the screen.

Figure 68
Enter CF drive letter

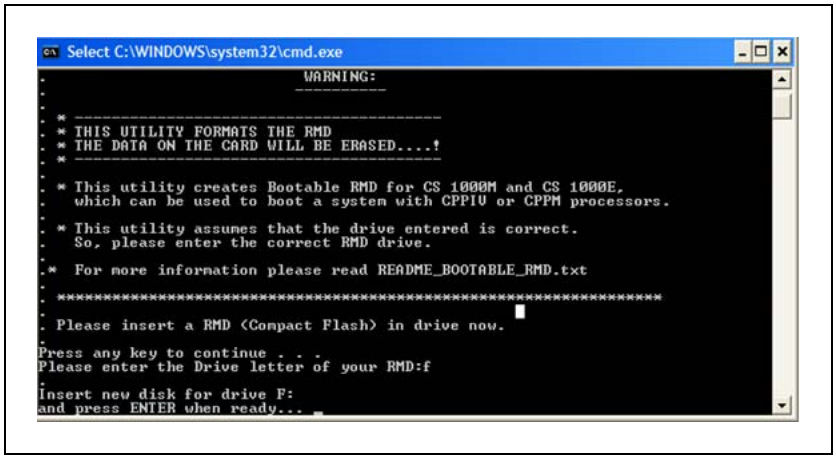


CAUTION
IMPORTANT!
The mkbootrmd.bat file does not verify the drive assignment; it is possible to format your C:\ drive.

9 Enter the drive letter assigned to the CF drive on your PC.

A line asking you to insert a new CF card in the CF drive appears on the screen.

Figure 69
Insert new CF card in drive

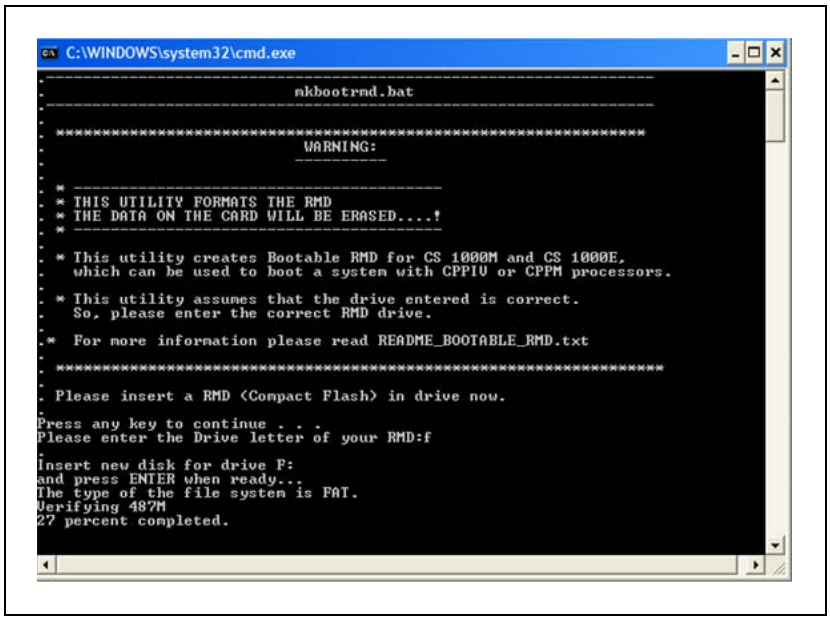


Although a CF card is already in the CF drive, you are requested to insert a new CF card in the drive. Ignore this request and proceed to the next step.

10 Press **Enter** to start formatting the CF card.

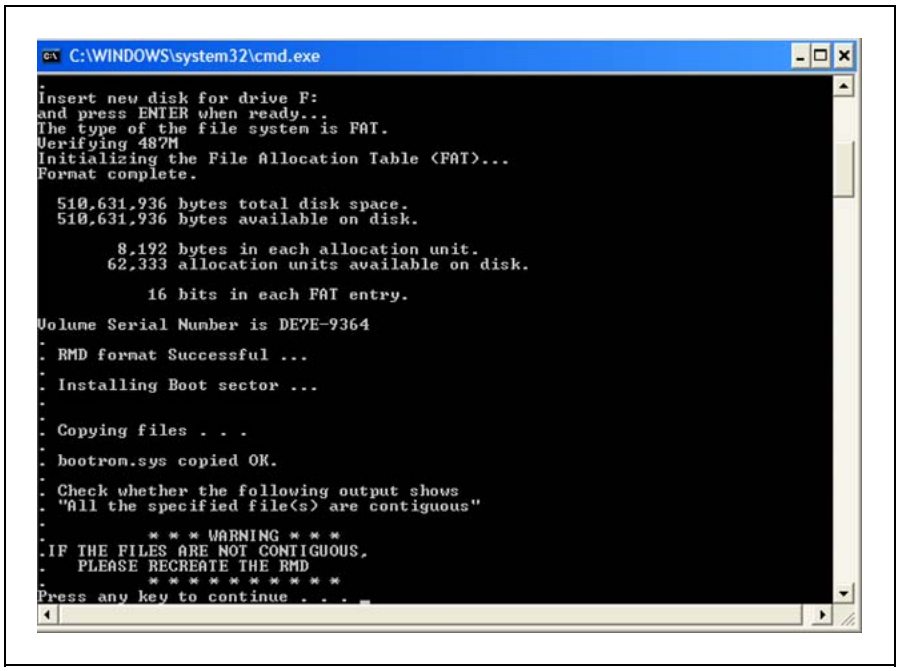
The Start of CF card formatting process screen appears.

Figure 70
Start of CF card formatting process



When the formatting process is almost complete, the End of CF card formatting process screen appears.

Figure 71
End of CF card formatting process



You see the following messages (among others):

`RMD format Successful ...` (after the Volume Serial Number string)

`bootrom.sys copied OK.`

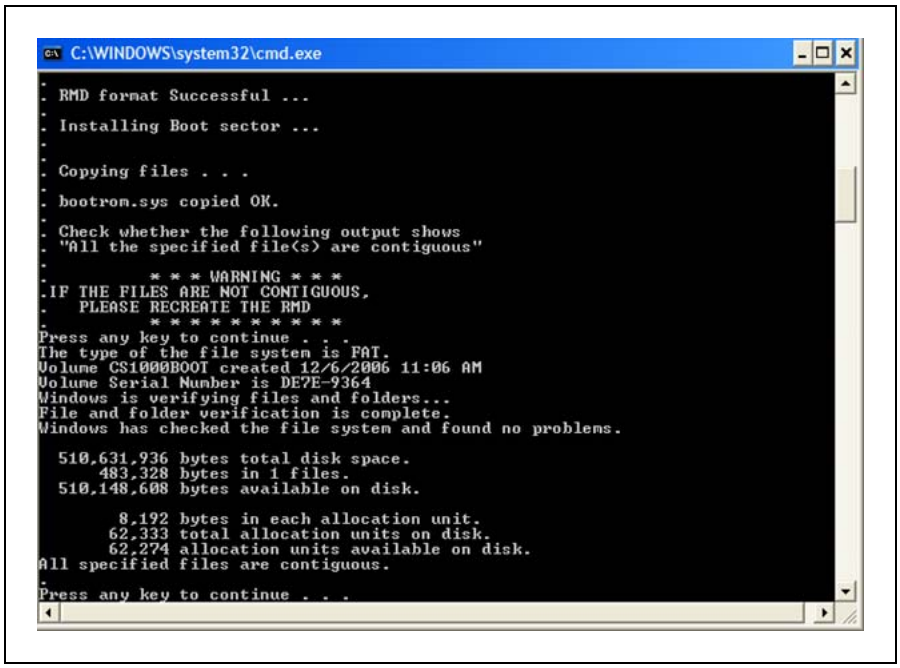
You should also see a very important warning message:

```
Check whether the following output shows
"All the specified file(s) are contiguous".
```

11 Press any key to continue.

The Verify CF card formatting process screen appears.

Figure 72
Verify CF card formatting



Look for the following message near the bottom of the screen:

```
All specified files are contiguous.
```

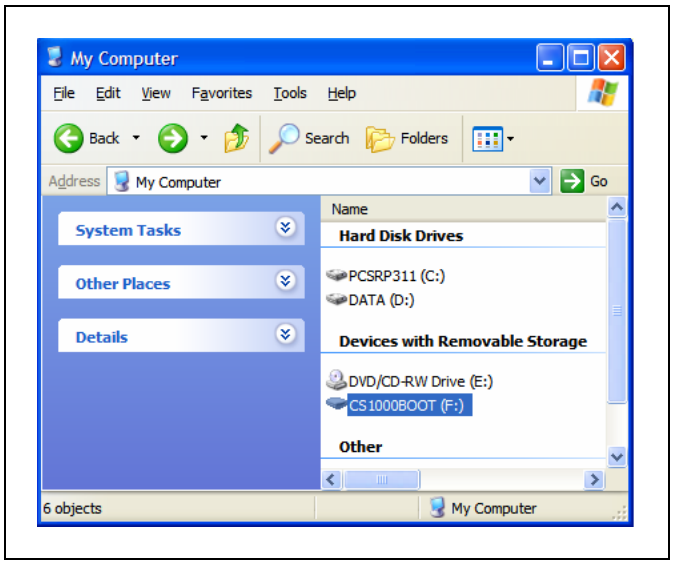
This message indicates that the CF card formatting process has ended successfully and the CF card is now ready to be loaded with the CS 1000 Release 5.0 Signaling Server Software and system components.

12 Press any key to close the batch file and associated MS-DOS window.

13 **Click** on **My Computer** to verify that the CF drive has been renamed to **CS1000BOOT**.

The following is an example of what you should see on the screen.

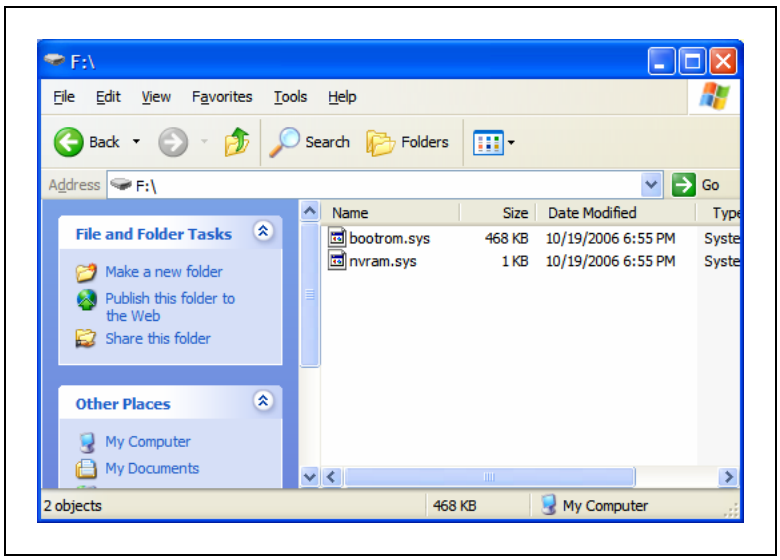
Figure 73
CF drive renamed to CS1000BOOT



14 Double click the CF drive to verify that it contains the bootrom.sys and nvram.sys files.

The following is an example of what you should see on the screen.

Figure 74
Verify contents of CS1000BOOT



15 Navigate to the **Temp** folder on your local PC (or the folder into which you downloaded the CP PM Signaling Server Load zip file).

16 Copy all of the subfolders and files from the parent directory (\cf) to the CF drive.

Note: This can take up to 12 minutes depending on the speed of your computer. You are copying files from the hard drive on your local PC to the CF card in the CF drive.

When all subfolders and files are copied successfully to the CF card, it can be used to install and upgrade Signaling Server software on a CP PM Signaling Server.

17 Remove the CF card from the CF drive and label it appropriately.

An example for a label is, Signaling Server, sse-x.xx.xx, where x.xx.xx represents the Signaling Server software version.

—End—

Software installation

Contents

This chapter contains the following information:

Introduction

This chapter contains detailed instructions for installing CS 1000 Release 5.0 Signaling Server software and entering basic system configuration parameters on all Signaling Server platforms.

CS 1000 Release 5.0 introduces three new server platforms that can host a Signaling Server:

- the Nortel CP PM server
- the IBM X306m server
- the HP DL320-G4 server

CS 1000 Release 5.0 Signaling Server software and system components require the Signaling Server to have at least 1 GB of RAM configured prior to beginning the software installation process. The Nortel CP PM Signaling Server ships with 1 GB of RAM configured. The IBM X306m and HP DL320-G4 servers ship with 2 GB of RAM configured.

The legacy Nortel ISP1100 server platform (NTDU27AA) can still be used as a Signaling Server in CS 1000 Release 5.0, but you need to update the RAM to 1 GB. To update the RAM on your legacy Nortel ISP1100 Signaling Server, a Nortel ISP1100 RAM Upgrade Kit (NTDU80CA) is available. Two NTDU80CA RAM Upgrade Kits are required to configure 1 GB of RAM on a legacy Nortel ISP1100 Signaling Server (see "Upgrade the RAM on a Nortel ISP1100 Signaling Server" (page 304).

If you only need to upgrade the software on a legacy Nortel ISP1100 Signaling Server from a previous release to CS 1000 Release 5.0, see "Software upgrade from Succession 3.0" (page 151) or "Software upgrade from Communication Server 4.0 or 4.5" (page 185) as appropriate.

To install CS 1000 Release 5.0 Signaling Server software and system components on an IBM X306m, HP DL320-G4, or Nortel ISP1100 server platform, you need to obtain a CS 1000 Release 5.0 Signaling Server Software CD. See "Obtain a Signaling Server software compact disk" (page 100) for instructions.

You do not need to install CS 1000 Release 5.0 software and system components on a new Nortel CP PM Signaling Server; it ships with the CS 1000 Release 5.0 operating system, web files and Signaling Server software already loaded on the hard drive. You need only enter basic system configuration parameters to make the Signaling Server operational. See "First boot of a new Nortel CP PM Signaling Server" (page 130) for instructions.

If you replace the hard drive on a Nortel CP PM Signaling Server due to a disk crash or some other hard drive failure, you need to install the CS 1000 Release 5.0 Signaling Server software and system components on the new hard drive. To execute this task, you need to obtain a CS 1000 Release 5.0 CP PM Signaling Server Software CF Card. See "Obtain a CP PM Signaling Server software compact flash card" (page 102) for instructions.

Before you begin

Before you install the Signaling Server software and enter basic system configuration parameters, you must perform the following tasks:

- If you are installing the Signaling Server software and system components on an IBM X306m, HP DL320-G4 or Nortel ISP1100 Signaling Server, you must obtain the CS 1000 Release 5.0 Signaling Server Software CD. See "Obtain a Signaling Server software compact disk" (page 100) for instructions.
- If you are installing the Signaling Server software and system components on a Nortel CP PM Signaling Server, you must obtain the CS 1000 Release 5.0 Signaling Server Software CF Card. See "Obtain

a CP PM Signaling Server software compact flash card" (page 102) for instructions.

- If you are installing the Signaling Server software on a Nortel ISP1100 Signaling Server, you must ensure that it has 1 GB of RAM configured. If not, see "Upgrade the RAM on a Nortel ISP1100 Signaling Server" (page 304) for instructions to upgrade the RAM before starting the installation procedure.
- Install and connect the Signaling Server (refer to "Hardware installation and connection" (page 59).
- Obtain the network and IP Telephony data for the Signaling Server from your Planning and Engineering group:
  - node ID for the IP Telephony node
  - node IP address for the IP Telephony node
  - host name for the Signaling Server
  - ELAN network interface IP address, Subnet mask, and Gateway
  - TLAN network interface IP address, Subnet mask, and Gateway
  - ELAN network interface IP address of the Call Server
  - Primary and Alternate NRS IP addresses for this networked system (refer to *IP Peer Networking Installation and Commissioning (NN43001-313)*)
  - NRS role, if applicable (refer to *IP Peer Networking Installation and Commissioning (NN43001-313)*)

Install the software

Use the following procedure to install the CS 1000 Release 5.0 Software and system components on a new Signaling Server and enter basic system configuration parameters.

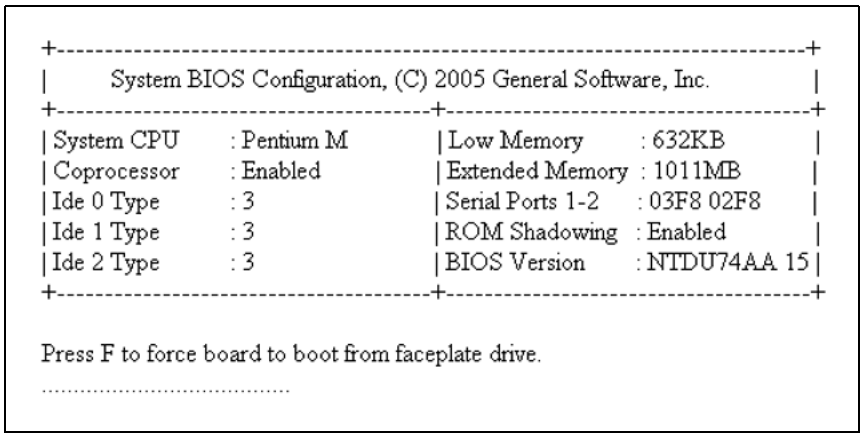
Procedure 19
Installing Signaling Server software

Step	Action
1	Boot the Signaling Server from the Removable Media Device (RMD): • For IBM X306m, HP DL320-G4, or Nortel ISP1100 Signaling Servers, insert the CS 1000 Release 5.0 Signaling Server Software CD into the CD drive and press the **RST** button on the front panel of the Signaling Server to trigger a cold boot. This forces the Signaling Server to boot from the CD. • For a Nortel CP PM Signaling Server, insert the CS 1000 Release 5.0 Signaling Server Software CF card into the faceplate

CF drive and press the **RST** button on the faceplate of the Signaling Server to trigger a cold boot.

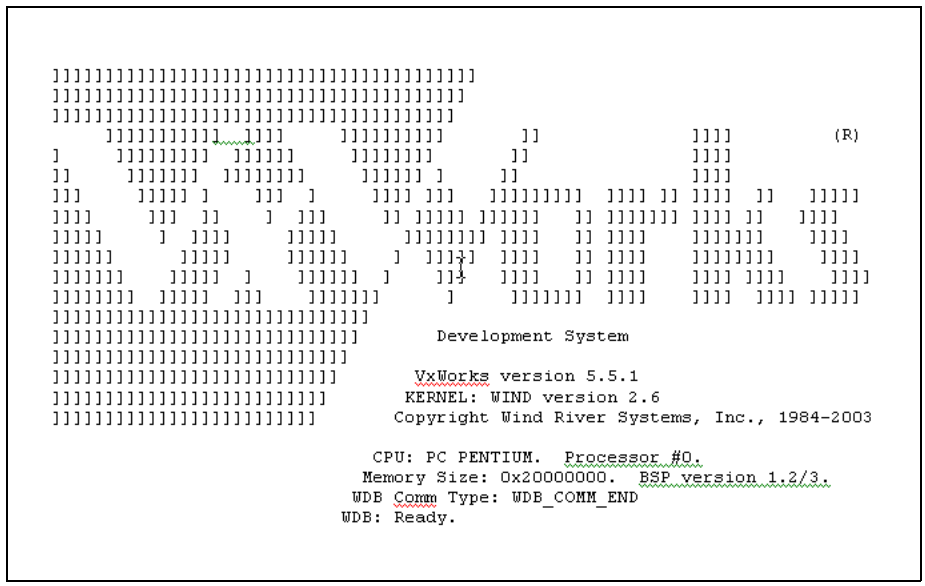
The CP PM System BIOS Configuration screen appears with an instruction to press **F** to force the Signaling Server to boot from the CF card.

Figure 75
Nortel CP PM system BIOS configuration



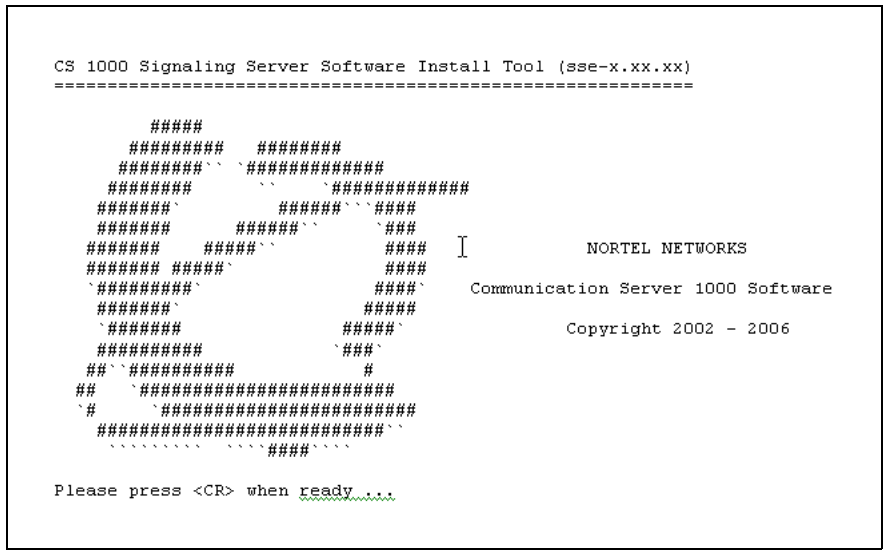
The VxWorks™ banner screen appears followed by system messages indicating that the Signaling Server Software Installation Tool is being loaded from either the Signaling Server Software CD or CF Card.

Figure 76
VxWorks system banner



After the Signaling Sever Software Installation Tool is loaded, the Installation Tool banner screen appears.

Figure 77
Installation Tool banner



2 Press **<CR>** to perform system checks.

The system verifies the RAM.

If the Signaling Server has less than 1 GB of RAM, the following error message appears:

```
*** ERROR: This Signaling Server has less than 1GB
RAM.
*** In order to run Rls 5.0 and later software you
must
*** upgrade RAM to 1GB and repeat install.
q<CR>:  quit and reboot
```

If the error message appears, press **<CR>** to quit. Use Procedure 55 "Upgrading the RAM of a Nortel ISP1100 server" (page 307) to upgrade to 1 GB of RAM and start the procedure again.

The system verifies the file systems.

- If the hard drive of the Signaling Server is not partitioned, the file systems verification process fails and the File systems verification failure screen appears.

Figure 78
File systems verification failure

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
======================================================================

The filesystems verification failed! (This is normal for a new
system.)

The hard disk must be (re)partitioned and (re)initialized. This will
erase all data on the hard disk. The system will then reboot and
the Install Tool will restart.

        Please enter:
<CR> -> <a> - Partition and initialize the hard disk, then reboot.

        Enter Choice> a
```

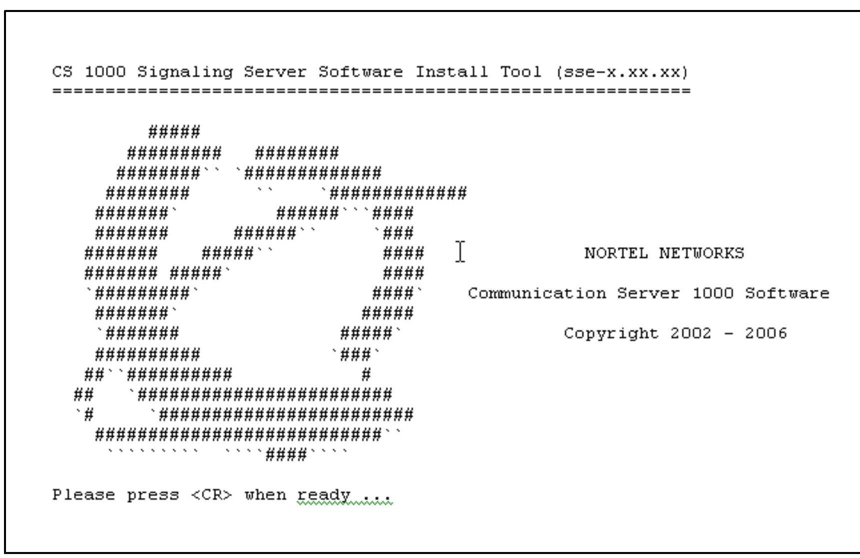
Enter **a** to partition and initialize the hard disk, and to reboot the Signaling Server.

The following system messages appear:

```
Partitioning hard disk ...
Hard disk partitioning succeeded.
Creating filesystems ...
Filesystems creation succeeded.
Rebooting system ...
```

The Installation Tool banner screen reappears.

Figure 79
Installation Tool banner



Go back to beginning of step 2.

- If the hard drive of the Signaling Server is partitioned, the following system messages appear.

  ```
  Verifying filesystems ...
  Filesystems verification succeeded.
  ```

  Then, the Date and Time screen appears.

Figure 80
Date and Time

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

You should ensure that the system date and time are correct prior to
installation, since all files copied or created during install will
be time-stamped.

You can press <CR> to accept the current values.

Current date is: FRIDAY 27-10-2006
Enter new date (dd mm yyyy):
Date not changed.

Current time is: 10:43:08
Enter new time (hh mm ss): 10 47 00
Time is set to: 10:47:00

Current date and time is:
FRIDAY 27-10-2006, 10:47:00
```

3 Confirm or enter the date and time.

The System Information screen appears.

Figure 81
System Information screen

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
====================================================================

           ------------------------------------------
                       SYSTEM INFORMATION
           ------------------------------------------

+==================================================================+
|  Hostname: SS_Node276_Ldr          S/W Ver: x.xx.xx              |
|                                                                  |
|      Role: Leader                  Set TPS: Disabled             |
|   Node ID:                        Vtrk TPS: Disabled             |
|   Node IP:                      NRS Config: Alternate SIP        |
|  H.323 ID: SS_Node276_Ldr            CS IP:                      |
|                                                                  |
|   ELAN IP: 192.168.10.20           TLAN IP: 192.168.20.20        |
|   ELAN SM: 255.255.255.0           TLAN SM: 255.255.255.0        |
|   ELAN GW: 192.168.10.1            TLAN GW: 192.168.20.1         |
|  ELAN MAC: 00:02:b3:c5:51:c6      TLAN MAC: 00:02:b3:c5:51:c7    |
+==================================================================+
        Please enter:
<CR> -> <a> - Continue with Install Tool.
        <q> - Quit.

        Enter Choice>
```

Note: For a new installation, data fields in the system information screen are normally blank.

4 Press **<CR>** or enter **a** to continue the installation.

The Installation Tool Main Menu appears.

Figure 82
Installation Tool Main Menu

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
================================================================

                        M A I N    M E N U

The Install Tool will install Signaling Server software and related
files. You will be prompted throughout the installation.

        Please enter:
<CR> -> <a> - To perform a complete installation/upgrade (Signaling
              Server s/w, Internet Telephone f/w, Voice Gateway Media
              Card l/w, basic Signaling Server configuration).
        <b> - To install/upgrade Signaling Server software only.
        <c> - To copy Internet Telephone firmware only.
        <d> - To copy Voice Gateway Media Card loadware only.
        <e> - To perform basic Signaling Server configuration only.
        <f> - To selectively change initial system parameters.
        <g> - To change board location information (CPPM only).
        <t> - To go to the Tools Menu.
        <q> - Quit.

        Enter Choice>
```

5 Press **<CR>** or enter **a** to perform a complete system installation and enter basic system configuration data.

Note: Option **a** performs options **b**, **c**, **d**, and **e**.

System messages appear on the screen as the Installation Tool processes the option you chose, followed by the Dependency lists installation screen.

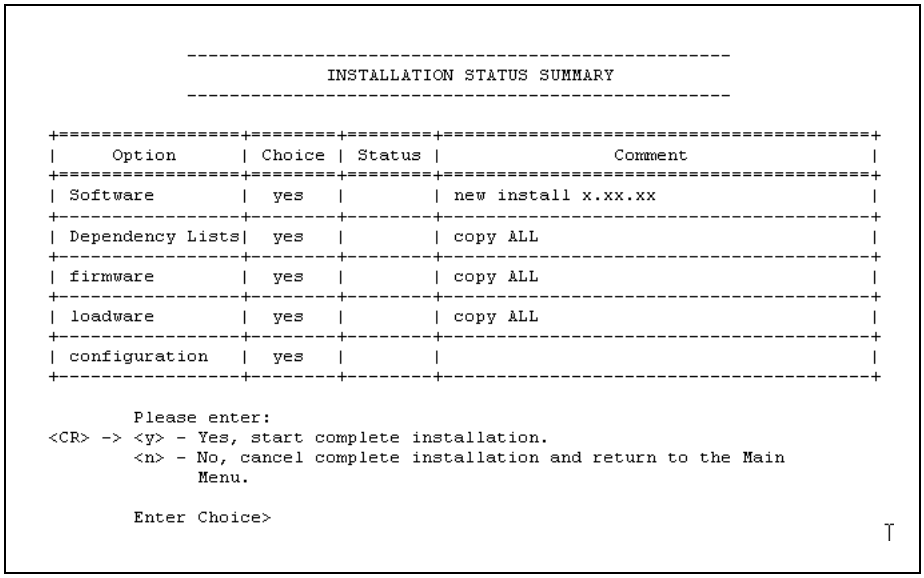
Figure 83
Dependency lists installation

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
================================================================


Do you want to install Dependency Lists?.


        Please enter:
<CR> -> <y> - Yes, Do the Dependency Lists installation
        <n> - No, Continue without Dependency Lists installation

        Enter Choice>
```

6 Press **<CR>** or enter **y** to install the dependency lists.

The Installation Status Summary screen appears.

Figure 84
Installation Status summary



```
                ------------------------------------------------
                          INSTALLATION STATUS SUMMARY
                ------------------------------------------------

+=================+========+========+=======================================+
|     Option      | Choice | Status |               Comment                 |
+=================+========+========+=======================================+
| Software        |  yes   |        | new install x.xx.xx                   |
+-----------------+--------+--------+---------------------------------------+
| Dependency Lists|  yes   |        | copy ALL                              |
+-----------------+--------+--------+---------------------------------------+
| firmware        |  yes   |        | copy ALL                              |
+-----------------+--------+--------+---------------------------------------+
| loadware        |  yes   |        | copy ALL                              |
+-----------------+--------+--------+---------------------------------------+
| configuration   |  yes   |        |                                       |
+-----------------+--------+--------+---------------------------------------+

        Please enter:
<CR> -> <y> - Yes, start complete installation.
        <n> - No, cancel complete installation and return to the Main
              Menu.

        Enter Choice>
```

7 Press **<CR>** or enter **y** to confirm your selected installation option and start the installation.

The following screens and messages appear in succession.

The first screen deals with installing the Signaling Server software and presents messages indicating the progress of the software installation process.

Figure 85
Software installation start

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

You have selected to install version x.xx.xx on the system. As this
is a new install, all necessary directories and files will be
created on the hard disk.

Starting new install of version x.xx.xx.

Initializing protected partition ...
Retrieved old volume params with %95 confidence:
Volume Parameters: FAT type: FAT32, sectors per cluster 8
  2 FAT copies, 0 clusters, 4096 sectors per FAT
  Sectors reserved 32, hidden 0, FAT sectors 8192
  Root dir entries 0, sysId (null) , serial number f9200
  Label:"           " ...
Disk with 4194304 sectors of 512 bytes will be formatted with:
Volume Parameters: FAT type: FAT32, sectors per cluster 8
  2 FAT copies, 523260 clusters, 4096 sectors per FAT
  Sectors reserved 32, hidden 0, FAT sectors 8192
  Root dir entries 0, sysId VX5DOS32, serial number f9200
  Label:"           " ...
"/p" initialized.

/p/  - Volume is OK
Creating directory "/p/data".
Creating directory "/p/etc".
Creating directory "/p/gk".
Creating directory "/p/gk/webfiles".
……
Copying "/cd0/ssexxxxx.p/target/u/fw/currency.xml" to "/u/fw/currency.xml".
Copying "/cd0/ssexxxxx.p/target/u/ssl/SipTls.org" to "/u/ssl/siptls.org".
Copying "/cd0/ssexxxxx.p/target/u/web/zonesconfiguration.xls" to "/u/web/zonesco
nfiguration.xls".

Erasing /u/patch/reten/reten.pch.
```

The second screen presented indicates the successful installation of the Signaling Server software.

Figure 86
Software installation success

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

Software version x.xx.xx was installed successfully.

All files were copied to the hard disk.

/boot/  - Volume is OK
```

The third screen deals with installing the IP phone firmware and presents messages indicating the progress of the IP phone firmware installation process.

Figure 87
IP Phone firmware installation

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

The installation source contains multiple Internet Telephone firmware
files.

Copying "/cd0/0603B76.bin" to "/u/fw/0603B76.bin".
Copying "/cd0/0602B76.bin" to "/u/fw/0602B76.bin".
Copying "/cd0/0604DB6.bin" to "/u/fw/0604DB6.bin".
Copying "/cd0/0621C45.bin" to "/u/fw/0621C45.bin".
Copying "/cd0/0624C44.bin" to "/u/fw/0624C44.bin".
Copying "/cd0/0625C44.bin" to "/u/fw/0625C44.bin".
Copying "/cd0/0627C44.bin" to "/u/fw/0627C44.bin".
```

The fourth screen deals with installing the Voice Gateway Media Card loadware and presents messages indicating the progress of the Voice Gateway Media Card loadware installation process.

Figure 88
Voice Gateway Media Card loadware installation

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

The installation source contains multiple Voice Gateway Media Card
loadware files.

Copying "/cd0/IPL49106.p2" to "/u/fw/IPL49106.p2".
Copying "/cd0/IPL49106.sa" to "/u/fw/IPL49106.sa".
Copying "/cd0/IPL49106.mc32s" to "/u/fw/IPL49106.mc32s".
```

After the Signaling Server software and system components are installed, the Restore IP configuration screen appears.

Figure 89
Restore IP configuration

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

Please insert the database diskette in the removable drive
to restore the IP configuration to the hard disk

        Please enter:
<CR> -> <a> - Diskette is now in the removable drive.
               Continue.
        <b> - Continue without restoring the IP configuration
        <q> - Quit.

        Enter Choice> b
```

8 Select **b** to bypass the restoration of IP configuration data.

You need to enter the IP configuration data in the subsequent steps of this procedure.

The Signaling Server role selection screen appears.

Figure 90
Signaling Server role selection

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
================================================================================
Note: This step will over-write all existing configuration parameters
      on this Signaling Server.

Please select the role of this Signaling Server.

If this Signaling Server will be a Leader then its data networking
and IP Telephony parameters must be entered now. (This will pre-
configure the IP Telephony node files.)

If this Signaling Server will be a Follower then its data networking
and IP Telephony parameters must be configured through Element
Manager later.

        Please enter:
<CR> -> <a> - Set this Signaling Server as a Leader.
        <b> - Set this Signaling Server as a Follower.
        <q> - Quit.

        Enter Choice>
```

9 Configure the Signaling Server as a Leader or Follower.

- If a Leader Signaling Server already exists in the IP Telephony node, enter **b** at the prompt to configure this Signaling Server as a Follower. The Follower Signaling Server configuration screen appears.

  Figure 91
  Follower Signaling Server configuration

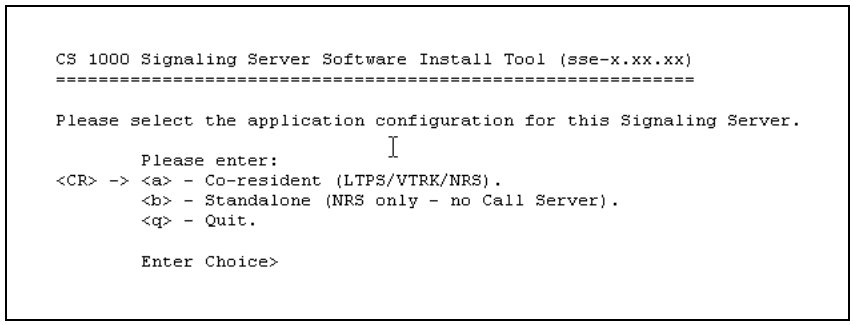
  ```
  CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
  ================================================================================

  This Follower Signaling Server will obtain its data network and IP
  telephony configuration from the Leader Signaling Server at boot.

  To identify this Signaling Server, please enter a Hostname.

  Hostname : SS_Node276_Ldr
  ```

  Go to step 13.

- If a Leader Signaling Server does not already exist in the IP Telephony node, or if the Signaling Server is to be a Standalone Signaling Server - NRS only, press **<CR>** or enter **a** at the prompt to configure this Signaling Server as Leader.

  The Application configuration screen appears.

Figure 92
Application configuration



10 Select the appropriate application configuration for this Signaling Server.

- If the IP Phone TPS, Virtual Trunk TPS, and optional Network Routing Service (NRS) applications are to be enabled on this Signaling Server, press **<CR>** or enter **a** at the prompt to configure this Signaling Server as a Coresident Signaling Server.
- If only the NRS is to be enabled on this Signaling Server:
  - If this Signaling Server is to be associated with a Call Server, press **<CR>** or enter **a** at the prompt to configure this Signaling Server as a Coresident Signaling Server. After you finish installing the Signaling Server software, you can disable the IP Phone TPS and Virtual Trunk TPS using Element Manager (refer to *Element Manager: System Administration (NN43001-632)*).
  - If this Signaling Server is not to be associated with a Call Server, enter **b** at the prompt to configure this Signaling Server as a Standalone Signaling Server - NRS only.

Depending on the application configuration selected, either the NRS - Coresident Signaling Server screen or the NRS - Standalone Signaling Server screen appears.

Figure 93
Network Routing Service (NRS): Coresident Signaling Server

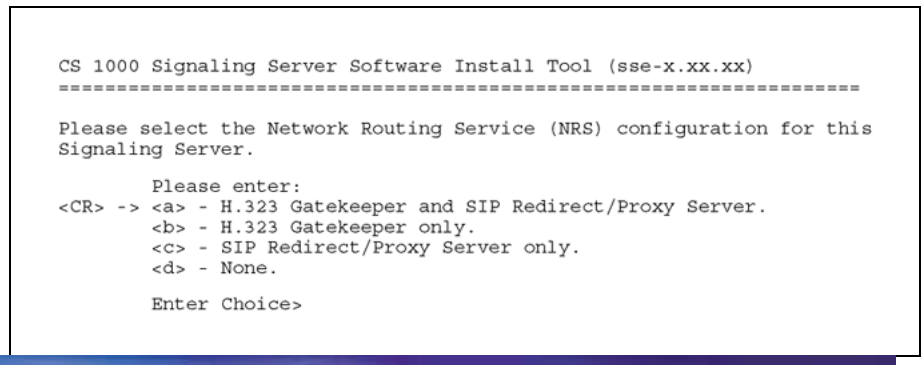


Figure 94
Network Routing Service (NRS): Standalone Signaling Server

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
========================================================================

Please select the Network Routing Service (NRS) configuration for this
Signaling Server.

        Please enter:
<CR> -> <a> - H.323 Gatekeeper and SIP Redirect/Proxy Server.
        <b> - H.323 Gatekeeper only.
        <c> - SIP Redirect/Proxy Server only.

        Enter Choice>
```

11 Select the Network Routing Service (NRS) configuration for this Signaling Server.

- Enter **d** if this Signaling Server is configured as a Coresident Leader and is not providing an NRS. Go to step 13.
- Press **<CR>** or enter **a** if this Signaling Server is to provide an H.323 Gatekeeper and a SIP Redirect/Proxy Server.
- Enter **b** if this Signaling Server is to provide only an H.323 Gatekeeper.
- Enter **c** if this Signaling Server is to provide only a SIP Redirect/Proxy Server.

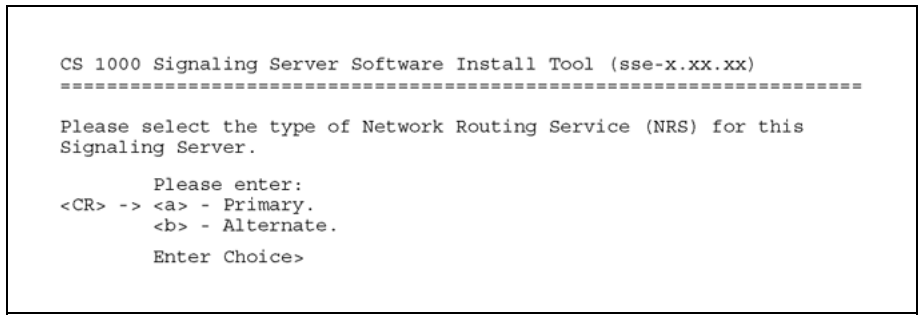
Refer to *IP Peer Networking Installation and Commissioning (NN43001-313)* for more information on the NRS.

Depending on the application configuration selected, either the NRS type: Coresident Signaling Server screen or the NRS type: Standalone Signaling Server screen appears.

Figure 95
NRS type: Coresident Signaling Server

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
========================================================================

Please select the type of Network Routing Service (NRS) for this
Signaling Server.

        Please enter:
<CR> -> <a> - Primary.
        <b> - Alternate.
        <c> - Failsafe.

        Enter Choice>
```

Figure 96
NRS type: Standalone Signaling Server



12 Select the type of NRS that this Signaling Server is to provide.

- If this Signaling Server is to be the Primary NRS, press **<CR>** or enter **a**.
- If this Signaling Server is to be the Alternate NRS, enter **b**.
- If this Signaling Server is configured as Coresident and is to be the Failsafe NRS, enter **c**.

Refer to *Network Routing Service Installation and Commissioning NN43001-564)* for more information on the NRS.

Depending on whether the Signaling Server is configured as Leader or Standalone, either the Leader Signaling Server configuration screen or the Standalone Signaling Server - NRS only configuration screen appears.

Figure 97
Leader Signaling Server configuration

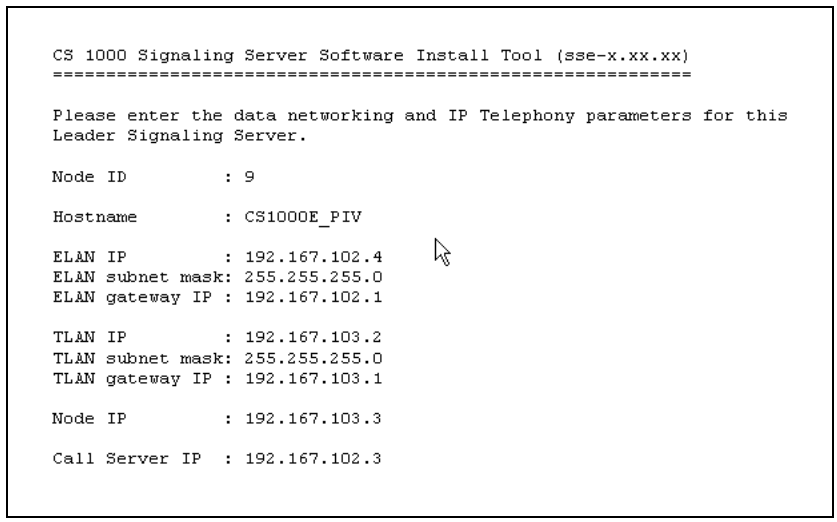
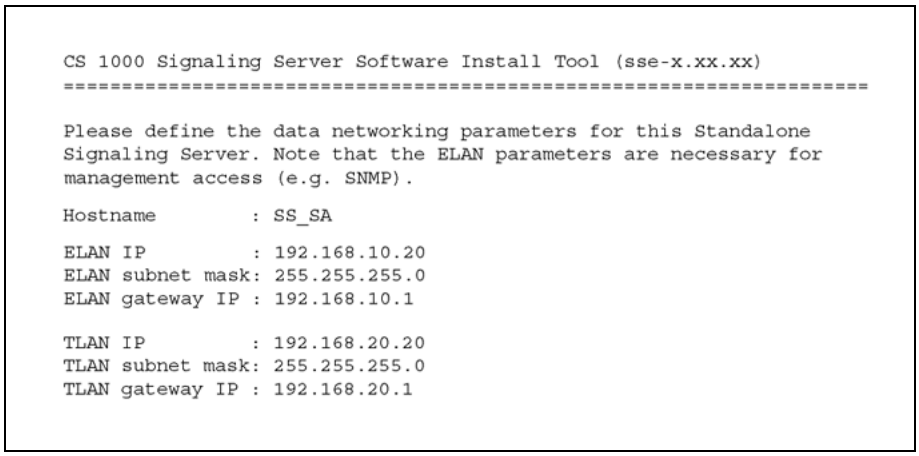


Figure 98
Standalone Signaling Server - NRS only configuration



13 Enter the data networking and IP telephony parameters for the Signaling Server, as prompted.

The IP information applies to a temporary IP Telephony node, to ensure that the existing node is not affected. The entry of data networking and IP telephony parameters also preconfigures the IP Telephony node files. After the Signaling Server software installation, the node files are imported into Element Manager for further configuration (see "Importing IP Telephony nodes" (page 251)).

- For a Leader Signaling Server, enter the parameters for the Node, ELAN network interface, TLAN network interface, and Call Server as required.

  If you install the Leader Signaling Server at an office that is not a branch office, enter the ELAN network interface IP address of the Call Server.

  If you install the Leader Signaling Server at a branch office, enter the ELAN network interface IP address of the MG 1000B Core.
- For a Follower Signaling Server, enter the host name of the Leader Signaling Server, and then go to step 15.
- For a Standalone Signaling Server - NRS only that is not associated with a Call Server (that is, **b** was selected in step 10), enter the TLAN subnet parameters as required. The Call Server IP address is automatically configured to 0.0.0.0.

Depending on whether the Signaling Server is configured as Primary, Alternate, or Standalone, either the Primary NRS IP address screen, the Alternate NRS IP address screen, or both (in succession) appear. Both screens appear in succession for a Standalone Signaling Server - NRS only.

Figure 99
Primary NRS IP address

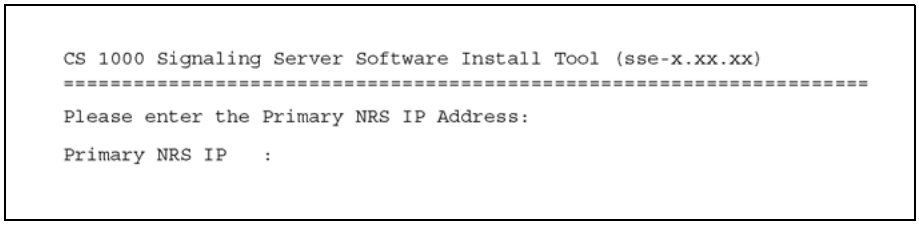
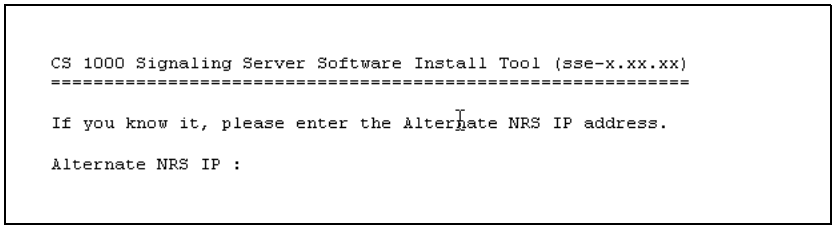


Figure 100
Alternate NRS IP address



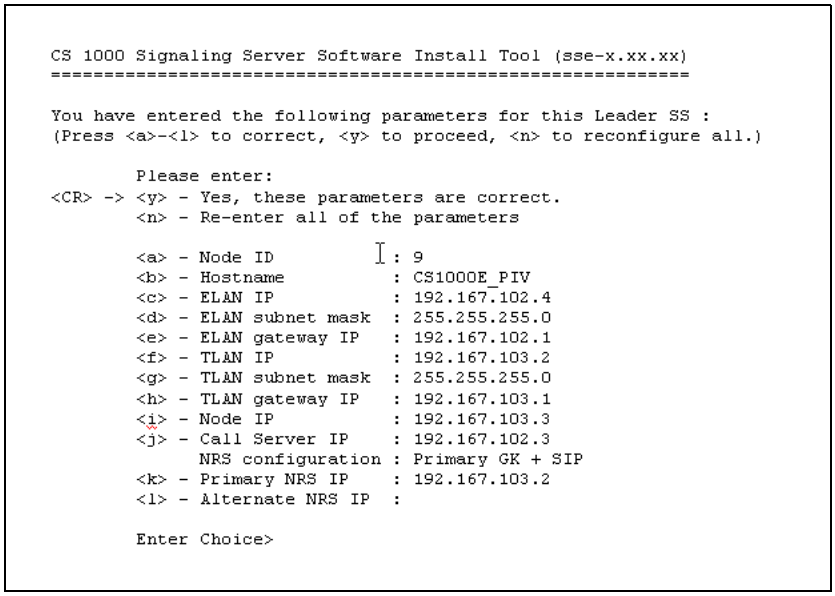
14 Enter the Primary NRS IP address or the Alternate NRS IP address, depending on the option entered in step 11 or step 12.

- If you entered **a** in step 12, you can enter the address of the Alternate NRS if you know it, but it is not required.
- If you entered **b** in step 12, enter the address of the Primary NRS.
- If you entered **c** in step 12:
  - — Enter the address of the Primary NRS.
  - — Enter the address of the Alternate NRS.
- If you entered **d** in step 11:
  - — Enter the address of the Primary NRS (optional).
  - — If you entered the address of the Primary NRS, enter the address of the Alternate NRS (optional).

  Note: You can later update the Gatekeeper configuration using Element Manager.

The IP Telephony parameter confirmation screen appears.

Figure 101
IP telephony parameter confirmation



15 Press **<CR>** or enter **y** to confirm all parameters, or enter the letter preceding any parameter to dynamically change its value.

The example in Figure 101 "IP telephony parameter confirmation" (page 128) is for a Leader Signaling Server configured with an Alternate H.323 and SIP NRS. The configuration screens for a Follower and a Standalone Signaling Server - NRS only are similar, showing the same list of parameters.

- The configuration screen for a Follower Signaling Server contains only a value for the host name; all other values are blank.
- The configuration screen for a Standalone Signaling Server - NRS only contains values for the host name, ELAN network interface, TLAN network interface, and NRS parameters. The Node ID parameter is configured to 0. The Call Server IP parameter is configured to 0.0.0.0.

After you confirm the IP configuration, the following system messages appear:

```
For future reference, the ELAN MAC address is:
"00:02:b3:c5:5l:c6".
Wrote config file "/u/config/bootp.tab".
Wrote config file "/boot/nvram.sys".
Wrote config file "/u/config/config.ini".
Wrote config file "/u/config/nrsconf.xml".
```

Note: You must configure the ELAN network interface MAC address for the newly installed Signaling Server in the Element Manager node configuration web page.

The Installation Status Summary screen appears.

Figure 102
Installation Status Summary

```
                    ------------------------------------------------
                                INSTALLATION STATUS SUMMARY
                    ------------------------------------------------

+=================+========+========+=========================================+
|      Option     | Choice | Status |                Comment                  |
+=================+========+========+=========================================+
| software        |  yes   |   ok   | new install x.xx.xx                     |
+-----------------+--------+--------+-----------------------------------------+
| Dependency Lists|  yes   | ignore | copy NONE                               |
+-----------------+--------+--------+-----------------------------------------+
| firmware        |  yes   |   ok   | copy Ixxxx version x.xx                 |
| firmware        |  yes   |   ok   | copy Ixxxx version x.xx                 |
| firmware        |  yes   |   ok   | copy PhaseX IP Firmware version x.xx    |
| firmware        |  yes   |   ok   | copy Ixxxx IP Firmware version x.xx     |
| firmware        |  yes   |   ok   | copy Ixxxx IP Firmware version x.xx     |
| firmware        |  yes   |   ok   | copy Ixxxx IP Firmware version x.xx     |
| firmware        |  yes   |   ok   | copy Ixxxx IP Firmware version x.xx     |
+-----------------+--------+--------+-----------------------------------------+
| loadware        |  yes   |   ok   | copy IP Line x.xx.xx for P2             |
| loadware        |  yes   |   ok   | copy IP Line x.xx.xx for SA             |
| loadware        |  yes   |   ok   | copy IP Line x.xx.xx for MC32S          |
+-----------------+--------+--------+-----------------------------------------+
| configuration   |  yes   |   ok   | set as Leader                           |
+-----------------+--------+--------+-----------------------------------------+

Please press <CR> when ready ...
```

16 Press **<CR>** to exit to the Main Menu.

The Installation Tool Main Menu screen appears.

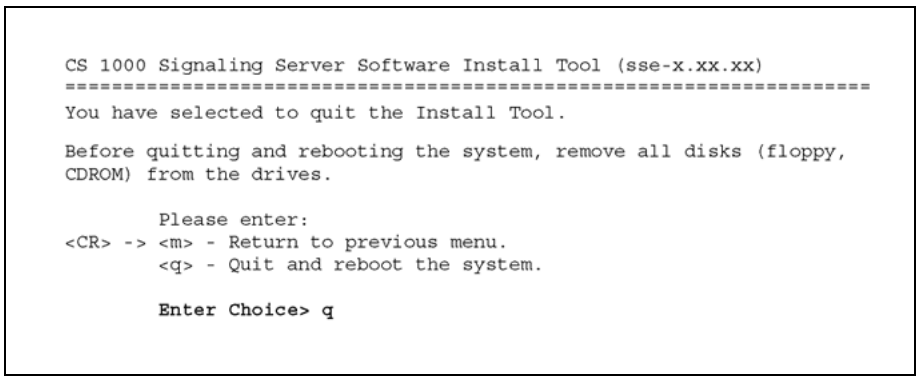
Figure 103
Installation Tool Main Menu

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

                        M A I N    M E N U

The Install Tool will install Signaling Server software and related
files. You will be prompted throughout the installation.

        Please enter:
<CR> -> <a> - To perform a complete installation/upgrade (Signaling
              Server s/w, Internet Telephone f/w, Voice Gateway Media
              Card l/w, basic Signaling Server configuration).
        <b> - To install/upgrade Signaling Server software only.
        <c> - To copy Internet Telephone firmware only.
        <d> - To copy Voice Gateway Media Card loadware only.
        <e> - To perform basic Signaling Server configuration only.
        <f> - To selectively change initial system parameters.
        <g> - To change board location information (CPPM only).
        <t> - To go to the Tools Menu.
        <q> - Quit.

        Enter Choice> q
```

17 Enter **q** to close/terminate the Installation Tool.

The Installation Tool quit confirmation screen appears.

Figure 104
Installation Tool quit confirmation



18 Remove the Signaling Server Software CD or the Signaling Server Software CF Card (as appropriate) from the RMD drive of the Signaling Server and enter **q** to close/terminate the Installation Tool and reboot the system.

The following system messages appear:

```
Removing temporary file "/u/disk.sys".
Rebooting system ...
```

—End—

First boot of a new Nortel CP PM Signaling Server

Nortel CP PM Signaling Servers have CS 1000 Release 5.0 software, applications, operating system, and web files preloaded on the hard drive when they are shipped. On the first boot of a Nortel CP PM Signaling Server, the Signaling Server Software Installation Tool prompts you to enter basic system configuration parameters.

Before you begin

Before you boot the new Nortel CP PM Signaling Server for the first time and start entering basic system configuration parameters, you must perform the following tasks:

- Install and connect the Signaling Server (refer to "Hardware installation and connection" (page 59).
- Obtain the network and IP Telephony data for the Signaling Server from your Planning and Engineering group:
  - node ID for the IP Telephony node

— node IP address for the IP Telephony node

— host name for the Signaling Server

— ELAN network interface IP address, Subnet mask, and Gateway

— TLAN network interface IP address, Subnet mask, and Gateway

— ELAN network interface IP address of the Call Server

— Primary and Alternate NRS IP addresses for this networked system (refer to *IP Peer Networking Installation and Commissioning (NN43001-313)*)

— NRS role, if applicable (refer to *IP Peer Networking Installation and Commissioning (NN43001-313)*)

Enter basic system configuration parameters

Use the following procedure to enter basic system configuration parameters during the first boot of a Nortel CP PM Signaling Server.

Procedure 20
Entering basic system configuration parameters

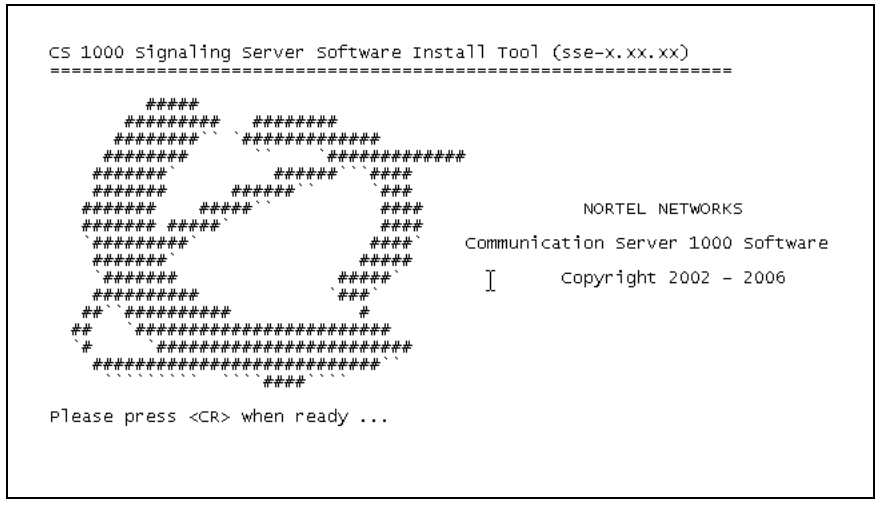
Step	Action

1 Press **RST** on the faceplate of the Nortel CP PM Signaling Server to trigger a cold boot.

The Signaling Server Software Installation Tool is triggered from the hard drive of a new Nortel CP PM Signaling Server.

The Installation Tool banner screen appears.

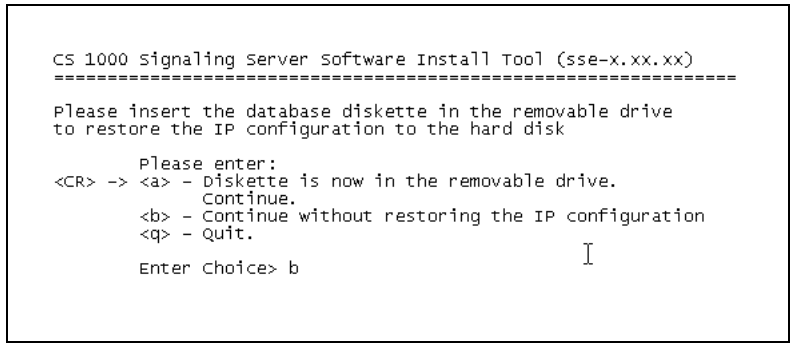
Figure 105
Installation Tool banner



2 Press **<CR>** to continue with the configuration.

The Restore IP configuration screen appears.

Figure 106
Restore IP configuration



3 Do one of the following:

- If you are migrating a Leader Signaling Server (see "Signaling Server migration" (page 215)

  insert the Removable Media Device (RMD) containing the IP configuration data into the appropriate drive, and press **<CR>** or enter **a** to restore the IP configuration data. After the restore is complete, the following system message appears:

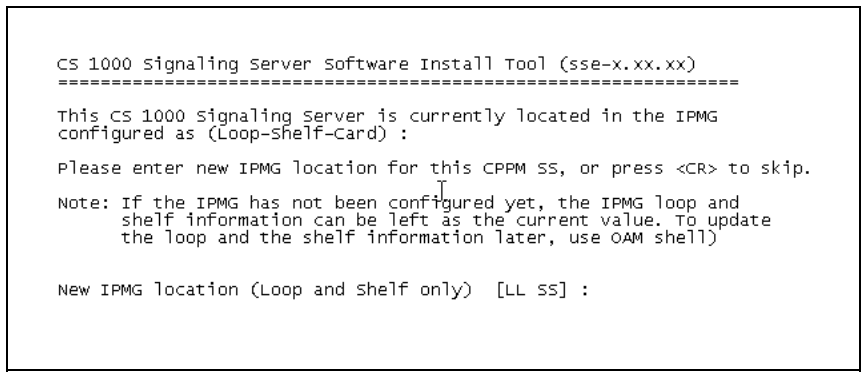
  ```
  Done copying IP configuration to disk
  ```

- If you are adding a new Leader, Follower, or Standalone Signaling Server - NRS only, or you are migrating a Follower or Standalone Signaling Server - NRS only

  Select **b** to bypass the restoration of IP configuration data.

Regardless of the option chosen, the CP PM board location screen appears.

Figure 107
CP PM board location

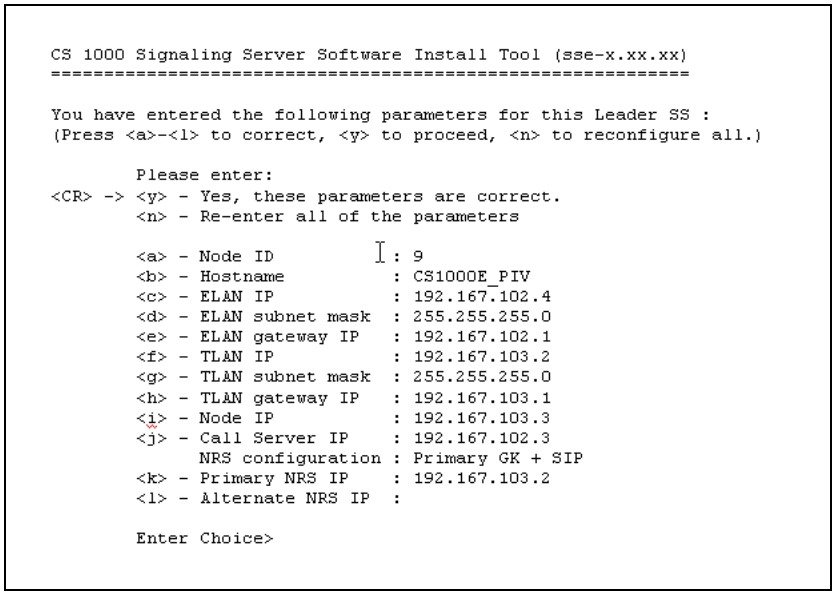


4 Enter the location (loop and shelf) of the Nortel CP PM Signaling Server.

Note: If the Media Gateway (MG) chassis or Universal Equipment Module (UEM) is not configured yet, you can leave the current location values in place. You can update the location later using OAM shell commands in Element Manager (EM).

- If you restored the IP configuration parameters from the RMD in the prior step, the IP Telephony parameter confirmation screen appears.

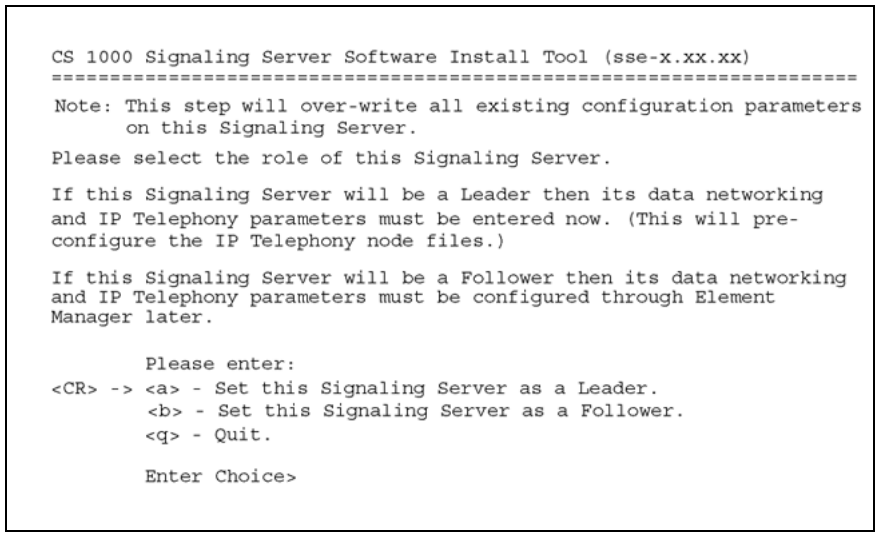
Figure 108
IP telephony parameter confirmation



Go to step 11.

- If you did not restore IP configuration parameters in the prior step, the Leader/Follower configuration screen appears.

Figure 109
Signaling Server role selection

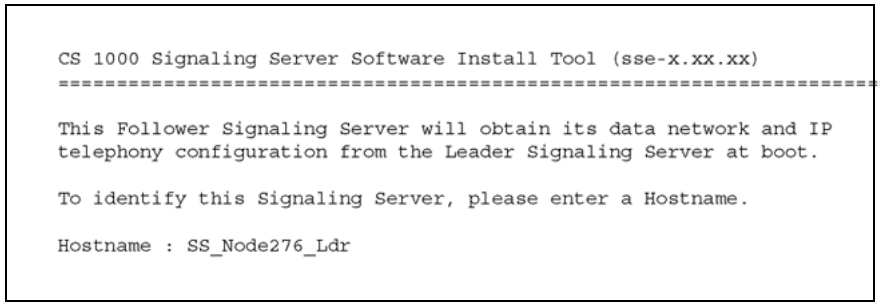


5 Configure the Signaling Server as a Leader or Follower.

- If a Leader Signaling Server already exists in the IP Telephony node, enter **b** at the prompt to configure this Signaling Server as a Follower.

  The Follower Signaling Server configuration screen appears.

  Figure 110
  Follower Signaling Server configuration

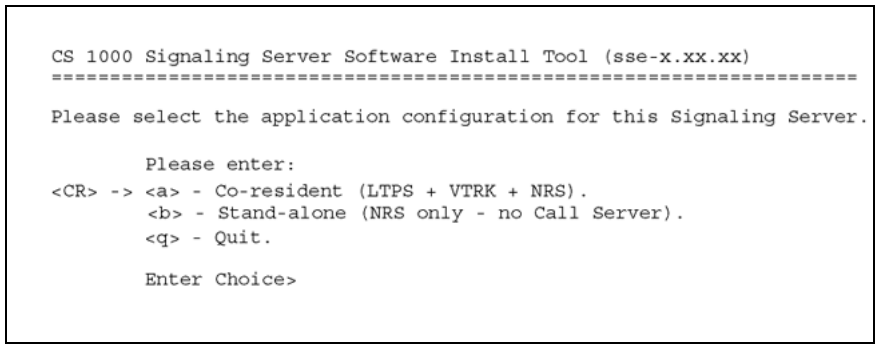
  

  Go to step 9.

- If there is not already a Leader Signaling Server in the IP Telephony node, or if the Signaling Server is to be a Standalone Signaling Server - NRS only, press **<CR>** or enter **a** at the prompt to configure this Signaling Server as a Leader.

  The Application configuration screen appears.

Figure 111
Application configuration



6 Select the appropriate application configuration for this Signaling Server.

- If the IP Phone TPS, Virtual Trunk TPS, and optional Network Routing Service (NRS) applications are to be enabled on this Signaling Server, press **<CR>** or enter **a** at the prompt to configure this Signaling Server as a Coresident Signaling Server.
- If only the NRS is to be enabled on this Signaling Server:
  - If this Signaling Server is to be associated with a Call Server, press **<CR>** or enter **a** at the prompt to configure this Signaling Server as a Coresident Signaling Server. After you install the Signaling Server software, you can disable the IP Telephone TPS and Virtual Trunk TPS in Element Manager (refer to *Element Manager: System Administration (NN43001-632)*).
  - If this Signaling Server is not to be associated with a Call Server, enter **b** at the prompt to configure this Signaling Server as a Standalone Signaling Server - NRS only.

Depending on the application configuration selected, either the NRS: Coresident Signaling Server screen or the NRS: Standalone Signaling Server screen appears.

Figure 112
Network Routing Service (NRS): Coresident Signaling Server

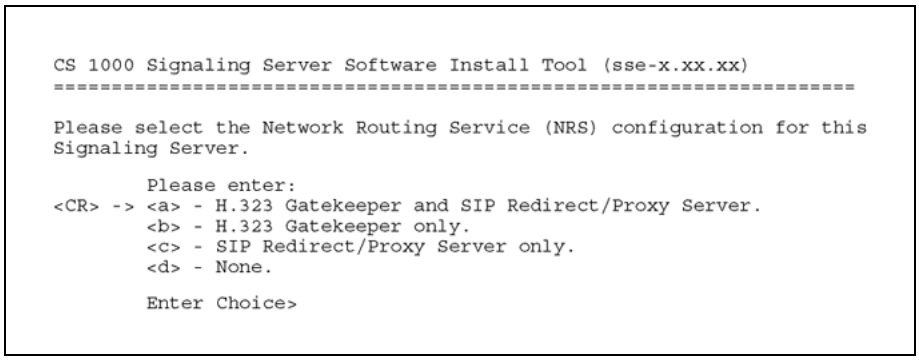
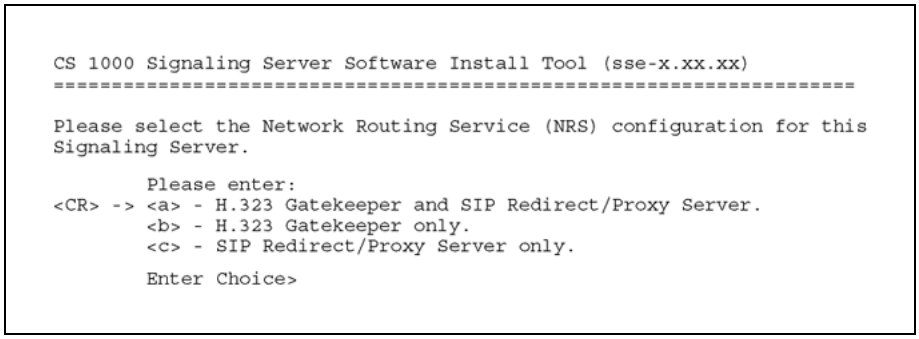


Figure 113
Network Routing Service (NRS): Standalone Signaling Server

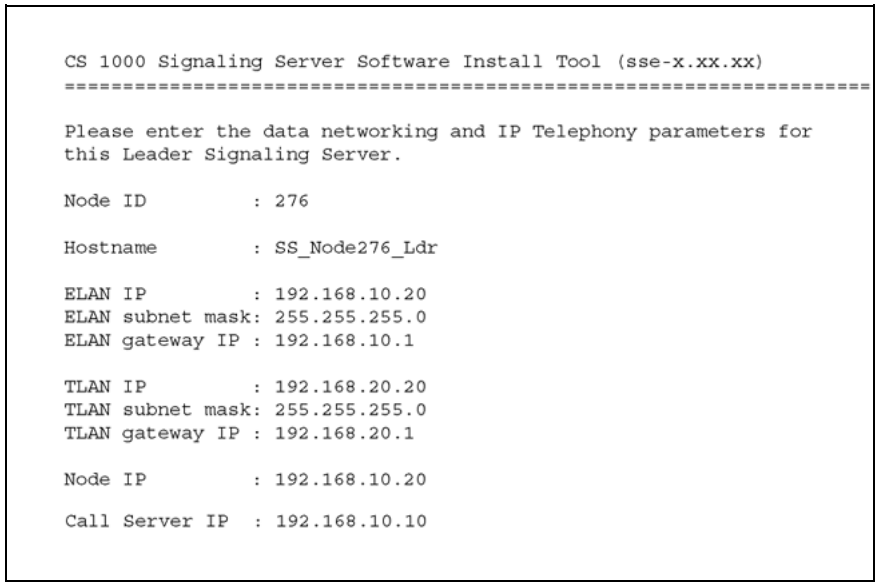


7 Select the Network Routing Service (NRS) to be provided by this Signaling Server.

- If this Signaling Server is configured as a Coresident Leader and is not providing an NRS, enter **d** .

  The Leader Signaling Server configuration screen appears.

Figure 114
Leader Signaling Server configuration



Go to step 9.

- If this Signaling Server is to provide an H.323 Gatekeeper and a SIP Redirect/Proxy Server, press **<CR>** or enter **a** .
- If this Signaling Server is to provide only an H.323 Gatekeeper, enter **b** .
- If this Signaling Server is to provide only a SIP Redirect Server, enter **c** .

Note: For more information on NRS, see *IP Peer Networking Installation and Commissioning (NN43001-313)*.

Depending on the application configuration selected, either the NRS type: Coresident Signaling Server screen or the NRS type: Standalone Signaling Server screen appears.

Figure 115
NRS type: Coresident Signaling Server

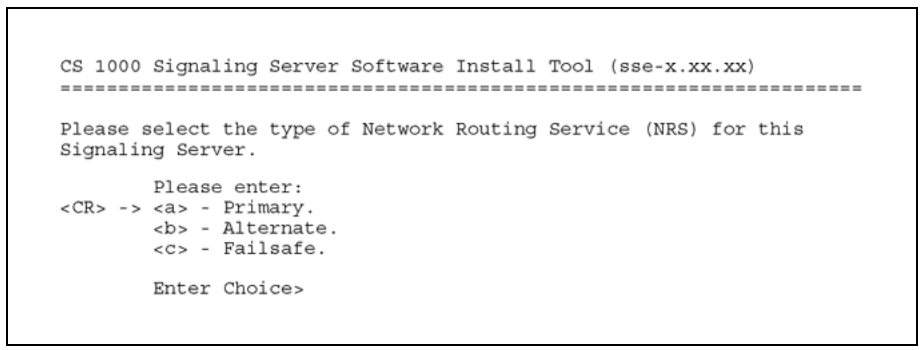


Figure 116
NRS type: Standalone Signaling Server

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
================================================================

Please select the type of Network Routing Service (NRS) for this
Signaling Server.

        Please enter:
<CR> -> <a> - Primary.
        <b> - Alternate.

        Enter Choice>
```

8 Select the type of NRS that this Signaling Server provides.

- If this Signaling Server is to be the Primary NRS, press **<CR>** or enter **a** .
- If this Signaling Server is to be the Alternate NRS, enter **b** .
- If this Signaling Server is configured as Coresident and is to be the Failsafe NRS, enter **c** .

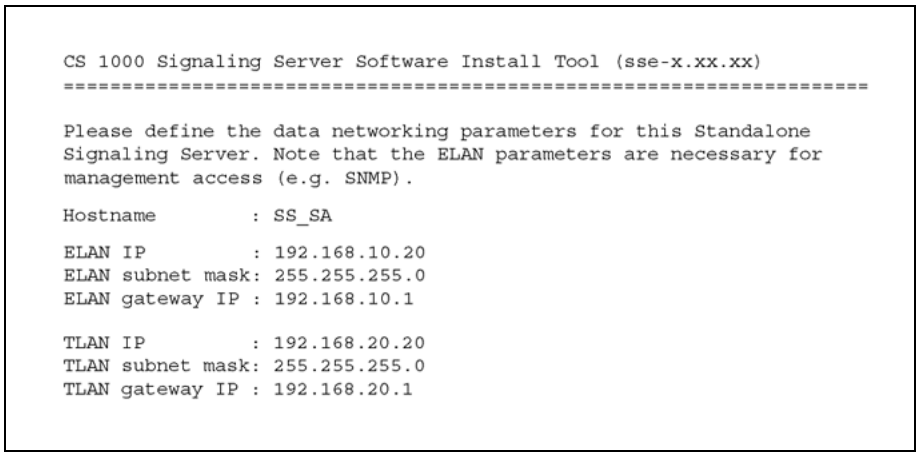
Refer to *Network Routing Service Installation and Commissioning NN43001-564)* for more information on the NRS.

Depending on whether the Signaling Server is configured as Leader or Standalone, the Leader Signaling Server configuration screen or the Standalone Signaling Server - NRS only configuration screen appears.

Figure 117
Leader Signaling Server configuration

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
================================================================

Please enter the data networking and IP Telephony parameters for
this Leader Signaling Server.

Node ID          : 276

Hostname         : SS_Node276_Ldr

ELAN IP          : 192.168.10.20
ELAN subnet mask: 255.255.255.0
ELAN gateway IP : 192.168.10.1

TLAN IP          : 192.168.20.20
TLAN subnet mask: 255.255.255.0
TLAN gateway IP : 192.168.20.1

Node IP          : 192.168.10.20

Call Server IP   : 192.168.10.10
```

Figure 118
Standalone Signaling Server - NRS only configuration



9 Enter the data networking and IP telephony parameters for the Signaling Server, as prompted.

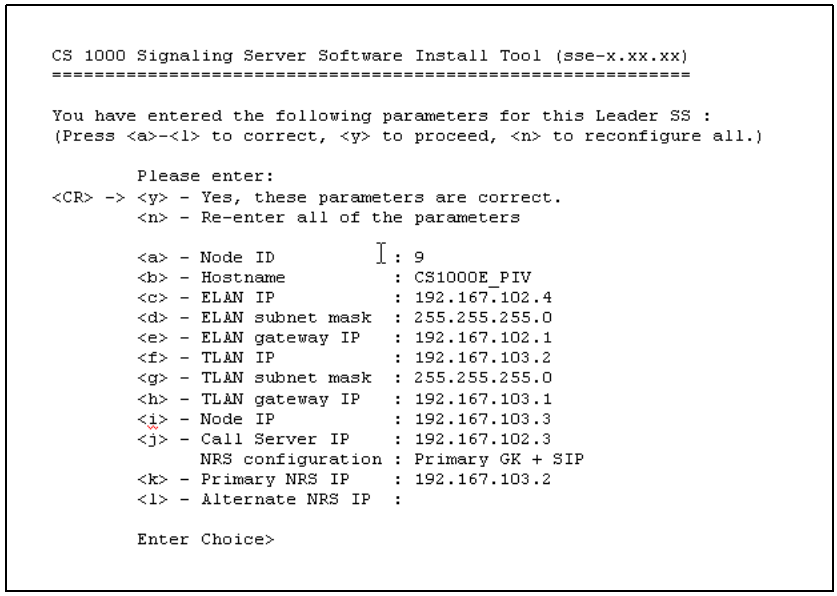
- For a Leader Signaling Server, enter the parameters for the Node, ELAN network interface, TLAN network interface, and Call Server as required. For the Call Server:

  If you install the Signaling Server at an office that is not a branch office, enter the ELAN network interface IP address of the Call Server.

  If you install the Signaling Server at a branch office, enter the ELAN network interface IP address of the MG 1000B Core.

- For a Follower Signaling Server, enter the host name of the Leader Signaling Server. The IP telephony parameter confirmation screen appears.

Figure 119
IP telephony parameter confirmation



Go to step 11.

- For a Standalone Signaling Server - NRS only not associated with a Call Server (that is, **b** was selected in step 6, enter the TLAN subnet parameters as required. The Call Server IP address is automatically configured to 0.0.0.0.

The data networking and IP telephony information applies to a temporary IP Telephony node to ensure that the existing node is not impacted. The entry of the data networking and IP telephony information also preconfigures the IP Telephony node files. After you configure the Signaling Server, the node files are imported to Element Manager for further configuration (see "Importing IP Telephony nodes" (page 251).

Depending on whether the Signaling Server is configured as Primary, Alternate, or Standalone, the Primary NRS IP address screen, the Alternate NRS IP address screen, or both in succession (for a Standalone Signaling Server - NRS only) appear.

Figure 120
Primary NRS IP address

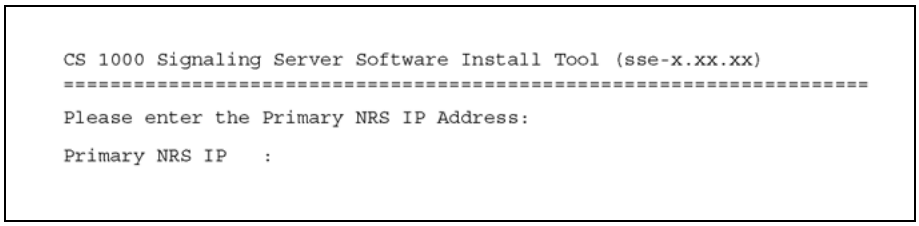
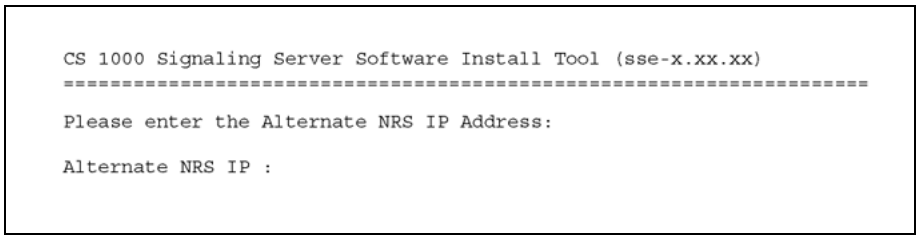


Figure 121
Alternate NRS IP address



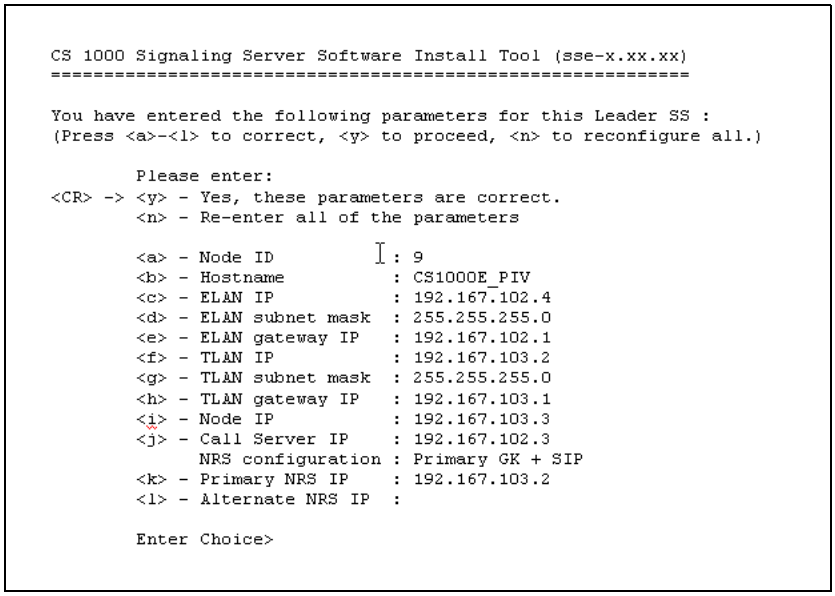
10 Enter the Primary NRS IP address or the Alternate NRS IP address, depending on the option that you entered in step 7 or step 8.

- If you entered **a** in step 8, you can enter the address of the Alternate NRS if you know it, but it is not required.
- If you entered **b** in step 8, enter the address of the Primary NRS.
- If you entered **c** in step 8:
  - — Enter the address of the Primary NRS.
  - — Enter the address of the Alternate NRS.
- If you entered **d** in step 7:
  - — Enter the address of the Primary NRS (optional).
  - — If you entered the address of the Primary NRS, enter the address of the Alternate NRS (optional).

  Note: You can later update the Gatekeeper configuration using Element Manager.

The IP Telephony parameter confirmation screen appears.

Figure 122
IP telephony parameter confirmation



11 Press **<CR>** or enter **y** to confirm all parameters, **n** to re-enter all parameters, or a letter **a** through **l** to change the value of the corresponding system parameter.

The configuration screens for a Follower and a Standalone Signaling Server - NRS only are similar, showing the same list of parameters.

- The configuration screen for a Follower Signaling Server contains only a value for the host name parameter; all other values are blank.
- The configuration screen for a Standalone Signaling Server - NRS only contains values for the host name, ELAN network interface, TLAN network interface, and NRS parameters. The Node ID parameter is configured to 0. The Call Server IP parameter is configured to 0.0.0.0.

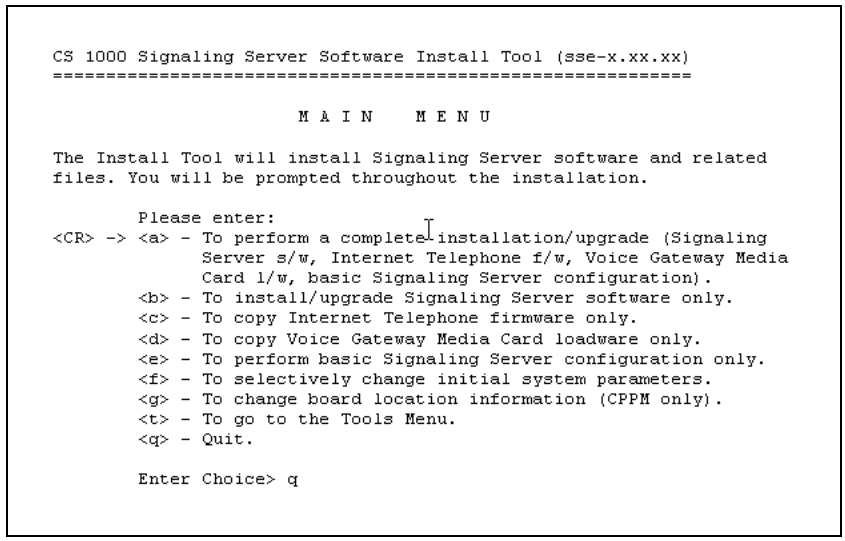
The following system message appears:

```
For future reference, the ELAN MAC address is:
"00:02:b3:c5:5l:c6".
```

Note: You must configure the ELAN network interface MAC address for the newly configured Signaling Server on the node configuration web page in Element manager (EM).

The Installation Tool Main Menu screen appears.

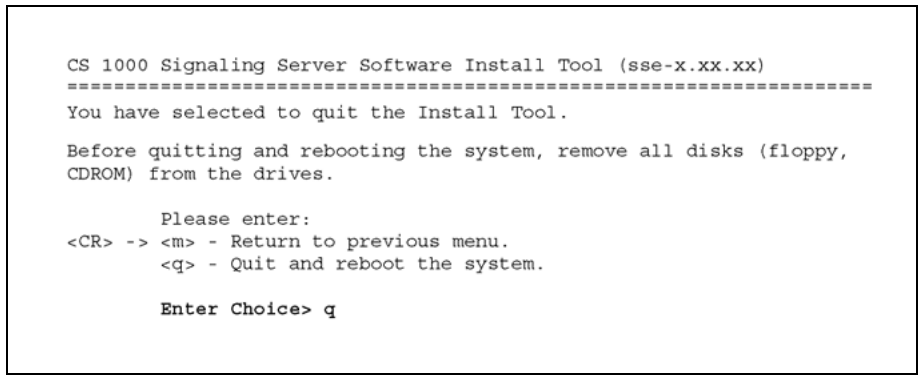
Figure 123
Installation Tool Main Menu



12 Enter **q** to close/terminate the Installation Tool.

The Installation Tool quit confirmation screen appears.

Figure 124
Installation Tool quit confirmation



13 Enter **q** to close/terminate the Installation Tool and reboot the Signaling Server.

—End—

After you configure and reboot the system, a Follower Signaling Server sends out BOOTP requests and waits for a response. Because the Follower Signaling Server is not yet configured in an IP Telephony node, no BOOTP response occurs. Do not wait for this response; use Element Manager to add the Follower Signaling Server to the IP Telephony node. Refer to "Adding a Follower Signaling Server to a node" (page 251)

Add a Follower Signaling Server to a node

Use the following procedure to add a Follower Signaling Server to an IP Telephony node.

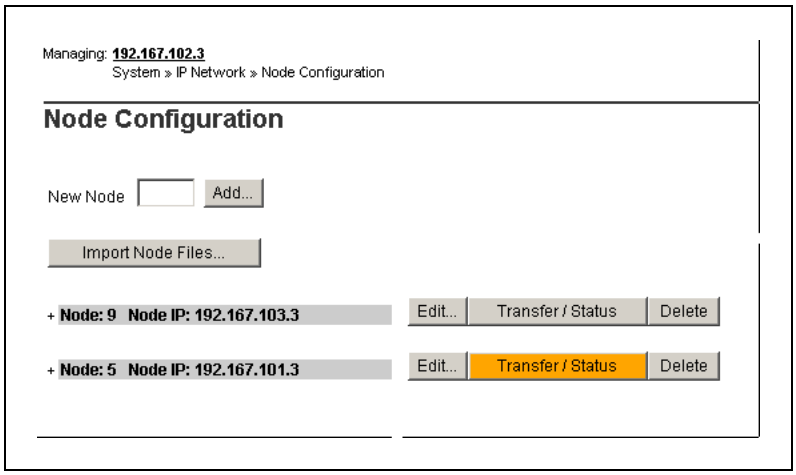
Note: The first time you install a Follower Signaling Server, the FTP fails. The failure occurs because the Follower cannot obtain the system logon and password, and does not have the current config.ini file with the Call Server IP address. In subsequent Follower installations, FTP succeeds.

Procedure 21

Adding a Follower Signaling Server to an IP Telephony node

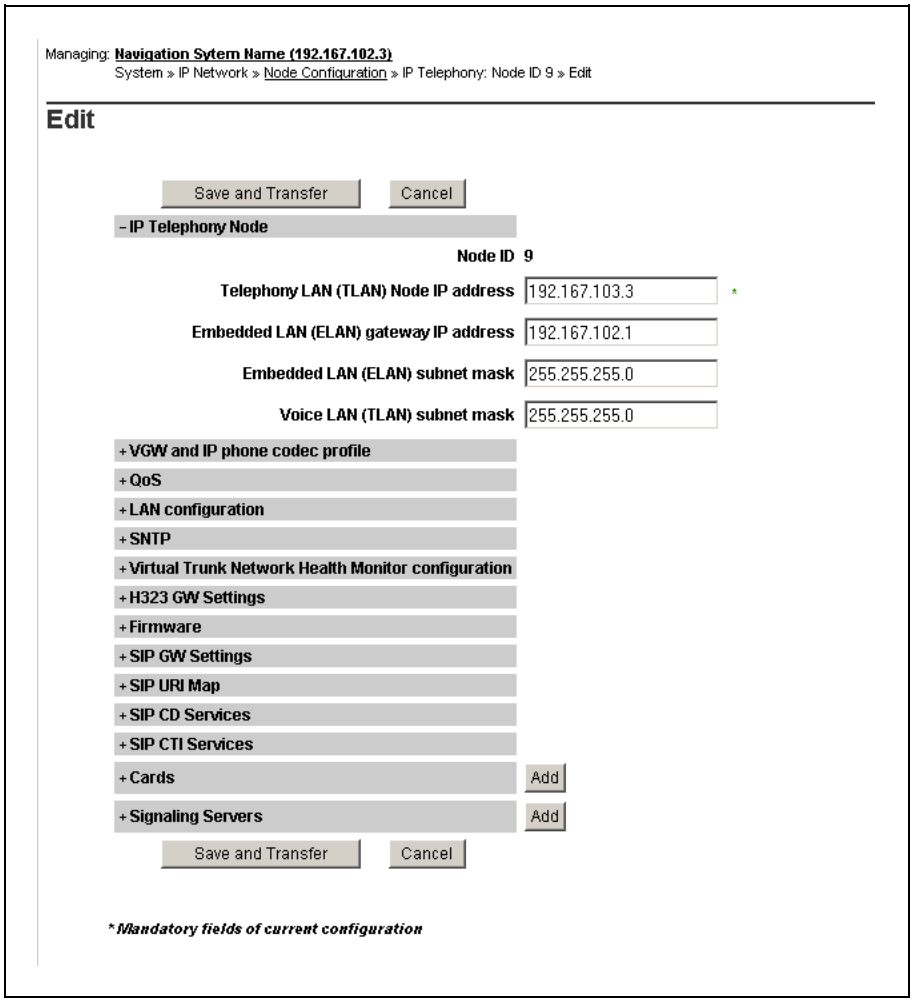
Step	Action
1	Log on to Element Manager (see Procedure 46 "Logging on to Element Manager" (page 243).
2	From the navigation tree, select **IP Network > Nodes: Servers, Media Cards** . The **Node Configuration** web page appears.

Figure 125
Node configuration



3	Click **Edit** next to the node where the Follower Signaling Server is to be added. The Edit node web page appears.

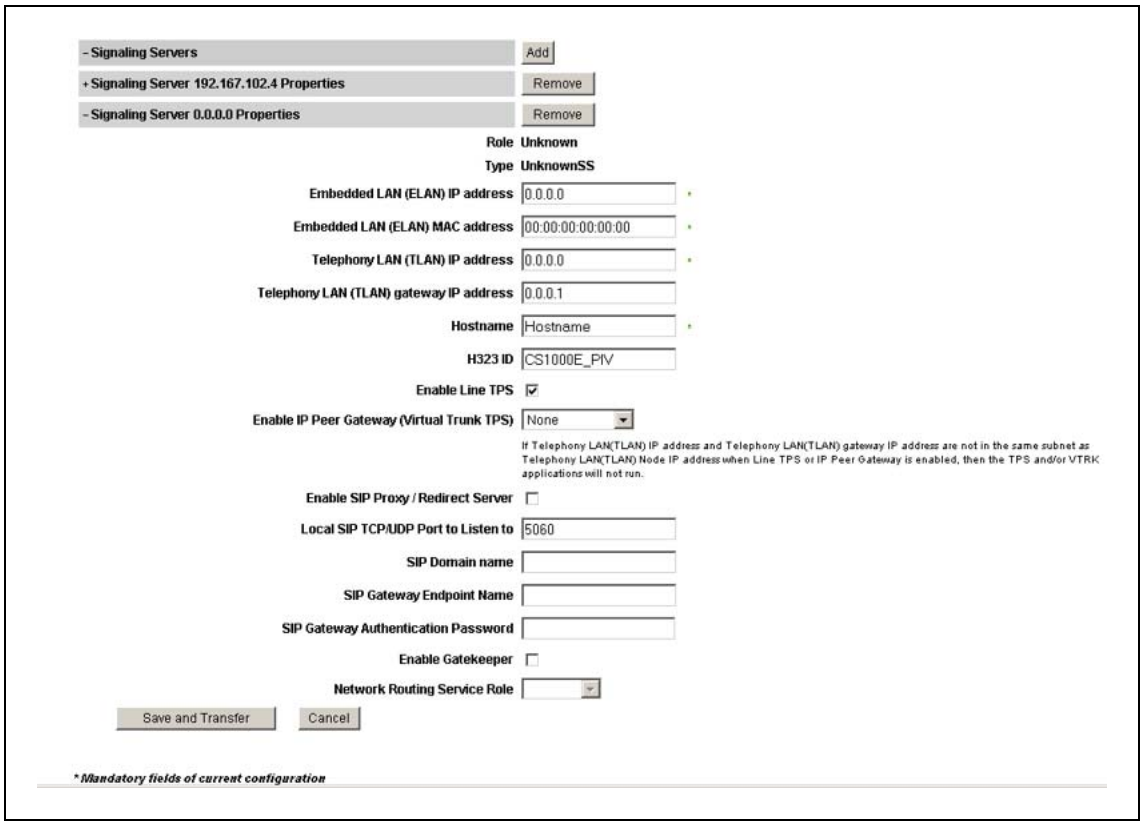
Figure 126
Edit node configuration



4 Click **Add** next to **Signaling Servers**.

The section expands to show a list of Signaling Servers and a blank template for entering **Signaling Server xxx.xxx.xxx.xxx properties** appears.

Figure 127
Signaling Server properties template



5 Enter the information that corresponds to the Follower Signaling Server.

The **Role** field automatically reverts to **Follower** after the Follower Signaling Server is added.

6 Click **Save and Transfer** to transfer the updated IP Telephony node information to the other node elements.

Refer to "Transferring IP Telephony files" (page 251), and *IP Line Fundamentals (NN43001-500)* for detailed instructions to transfer IP Telephony node information.

—End—

Unpack Help files for Virtual Terminal Emulator

Help files for the Virtual Terminal Emulator (VTE) component of Element Manager are copied to the Signaling Server as compressed files during installation of the Signaling Server software.

Unpacking the Help files is optional. However, you can unpack the file any time after you install the Signaling Server software. Use Procedure 48 "Unpacking Help files for Virtual Terminal Emulator" (page 247) to unpack the files.

ATTENTION

IMPORTANT!

Unpacking the Help files takes approximately 20 to 30 minutes. Nortel recommends that you unpack the files during a service outage.

Refer to *Element Manager: System Administration (NN43001-632)* for more information about Element Manager and the Virtual Terminal Emulator.

Log on to the Signaling Server

Use Procedure 22 "Logging on to the Signaling Server" (page 147) to log on to the VxWorks™ shell to access the Signaling Server from a maintenance terminal.

Before you begin, make sure the Signaling Server is properly connected to the maintenance terminal. See "Hardware connection" (page 77) for instructions to connect a maintenance terminal to each type of Signaling Server.

- Nortel ISP1100, IBM X306m, and HP DL320-G4 Signaling Servers connect to the maintenance terminal using a DTE–DTE null modem cable that connects between the serial port on the Signaling Server and the serial port on the maintenance terminal.
- Nortel CP PM Signaling Servers connect to the maintenance terminal using a special cable (NTAK19EC) that is connected to the 50-pin MDF connector on the back of the shelf. This cable converts the 50-pin MDF connector to a 25-pin DB connector. A DTE-DTE null modem cable connects the 25-pin DB connector on the end of the NTAK19EC cable and the serial port on the maintenance terminal.

Procedure 22

Logging on to the Signaling Server

Step	Action
1	Make sure the Signaling Server is powered up and connected to the maintenance terminal. The Signaling Server must boot successfully before you can log on.
2	Press **<CR>** to invoke the logon prompt.
3	Enter the logon credentials by performing one of the following tasks:

- If the Signaling Server has connected to the Call Server (the startup messages indicate if the PBX link is up), use the PWD1 logon to access the Signaling Server.
- If the Signaling Server is not connected to the Call Server:
  1. Enter the default Signaling Server CLI logon **admin** .

     The system immediately prompts you to change the default password.
  2. Enter the Signaling Server CLI password.
     - If this Signaling Server is newly installed and you are logging on for the first time, enter the default password **cseadmin**.
     - If this is not the first logon to the Signaling Server, enter the appropriate password.

       If you forget the password, reset it from the Tools Menu (see "Signaling Server Tools Menu" (page 296).

To log off of the Signaling Server, enter exit at the command line.

—End—

Verify a successful configuration

To ensure that you have successfully configured the Signaling Server Ethernet connections (for the ELAN and TLAN subnets), perform a ping test to one or more of the other devices connected to the network, particularly the Call Server.

Procedure 23
Verifying the Signaling Server Ethernet connection

Step	Action
1	Log on to the Signaling Server, using Procedure 22 "Logging on to the Signaling Server" (page 147).
2	Ping the IP address of the Signaling Server. Enter the command: **ping x.x.x.x** where **x.x.x.x** is the Signaling Server ELAN network interface IP address.
3	Ping the IP address of the Call Server. Enter the command:

ping x.x.x.x ,3

where

x.x.x.x is the Call Server ELAN network interface IP address.

4 If desired, repeat step 3 for other devices connected to the network.

—End—

Test the Leader Signaling Server

Configure two IP Phones to register to the Signaling Server on the temporary IP telephony node. You must provision these IP Phones on the Call Server. See *Communication Server 1000E Installation and Commissioning (NN43041-310)*, *Communication Server 1000M and Meridian 1: Small System Installation and Commissioning (NN43011-310)* or *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning (NN43021-310)* for the procedure appropriate to the system. After provisioning, the IP Phones can call each other.

Software upgrade from Succession 3.0

Contents

This chapter contains the following information:

Introduction

Communication Server 1000 Release 5.0 (CS 1000 Release 5.0) introduces 3 new servers that can host Signaling Server functionality, in addition to the legacy Nortel ISP1100 server:

- Nortel CP PM server
- IBM X306m server
- HP DL320-G4 server

These three new servers can not run any Signaling Server software prior to CS 1000 Release 5.0, and therefore are not subject to software upgrades in CS 1000 Release 5.0. The CS 1000 Release 5.0 Signaling Server software

must be installed on these servers (see "Software installation" (page 111)). Only legacy Nortel ISP1100 Signaling Servers are subject to in-place Signaling Server software upgrades in CS 1000 Release 5.0.

If you want to migrate your legacy Nortel ISP1100 Signaling Server to one of the three new servers introduced in CS 1000 Release 5.0, see "Signaling Server migration" (page 215)

This chapter contains instructions for upgrading the Signaling Server software on a legacy Nortel ISP1100 server (NTDU27AA) from Succession 1000 Release 3.0 to Communication Server 1000 Release 5.0.

CS 1000 Release 5.0 software requires a server to have at least 1 GB of RAM configured. Some Nortel customers may need to upgrade the RAM on their legacy Nortel ISP1100 server before upgrading the Signaling Server software to CS 1000 Release 5.0. To enable customers to configure 1 GB of RAM on their legacy Nortel ISP1100 servers, a Nortel ISP1100 RAM Upgrade Kit (NTDU80CA) is available. Two NTDU80CA RAM Upgrade Kits are required to configure 1 GB of RAM on any Nortel ISP1100 server. See "Upgrade the RAM on a Nortel ISP1100 Signaling Server" (page 304) for instructions on using the NTDU80CA RAM Upgrade kit to upgrade the RAM of a Nortel ISP1100 server.

Note: You can contact Nortel Global Professional Services to assist you with the upgrade.

Network Routing Service

Communication Server 1000 Release 4.0 and later support both H.323 and Session Initiation Protocol (SIP) on the same Signaling Server. You can use Network Routing Service (NRS) to manage a single network dialing plan for H.323, SIP, and mixed H.323/SIP networks.

The NRS combines the following into a single application for network-based routing:

- The SIP Redirect Server provides central dialing plan management and routing for SIP-based solutions. The Redirect Server is a software component of the NRS.
- The H.323 Gatekeeper provides central dialing plan management and routing for H.323-based solutions. The H.323 Gatekeeper is a software component of the NRS.
- The NRS includes the Network Connection Service (NCS). The NCS is used for Branch Office, IP Line Virtual Office, and Geographic Redundancy solutions. With NCS, the Line TPS (LTPS) can query the NRS using the UNIStim protocol.

The NRS provides routing services to both H.323-compliant and SIP-compliant devices. You can configure the H.323 Gatekeeper application for routing services for H.323 endpoints and the SIP Redirect Server application for SIP routing services for SIP endpoints.

The H.323 Gatekeeper and the SIP Redirect Server can coexist on the same Signaling Server. The NRS database resides on the Signaling Server with the NRS applications. Both the H.323 Gatekeeper and SIP Redirect Server have access to this endpoint or location database, and both use its data.

For more information about NRS configuration and management, see *Network Routing Service Installation and Commissioning NN43001-564)*.

Browser configuration

You must properly configure your web browser before you use NRS Manager. Refer to "Configuring the Internet Explorer browser" (page 240) for instructions to configure your web browser.

NRS server configuration

You must enable and properly configure the NRS server before you configure any NRS data.

You can configure the NRS server in two modes:

- Standalone mode: The host Signaling Server is not attached to a Call Server. When you configure the Signaling Server, ensure that the Call Server IP address is configured to 0.0.0.0 (see Procedure 24 "Enabling and configuring the NRS server in Standalone mode" (page 154)).

  Note: When you configure the Signaling Server in Standalone mode (using the Signaling Server Software Installation Tool), you are not prompted to enter the Call Server IP address. Instead, the Call Server IP address defaults to 0.0.0.0.

- Coresident mode: The NRS is Coresident on the Signaling Server that is attached to the Call Server. The Signaling Server can run other applications including Line TPS and Virtual Trunk (see Procedure 25 "Enabling and configuring the NRS server in Coresident mode" (page 155).

Enable and configure the NRS server in Standalone mode

Use the following procedure to enable and configure the NRS server in Standalone mode:

Procedure 24
Enabling and configuring the NRS server in Standalone mode

Step	Action
1	Enable the NRS using the Signaling Server Software Installation Tool. The following summarizes the tasks required to install and configure a Standalone Signaling Server - NRS only. Follow the detailed procedures in "Software installation" (page 111)or "Signaling Server reconfiguration" (page 199) for complete instructions. • Perform the introductory steps for the Signaling Server installation. • Configure the Signaling Server as a Leader, when you are prompted. • Select Standalone mode (NCS only, no Call Server) for the Signaling Server. • Select whether the NRS supports the H.323 Gatekeeper, the SIP Redirect Server, or both. • Select the type of NRS (Primary or Alternate). • Enter the host name, the ELAN network interface parameters, and the TLAN network interface parameters. The ELAN and TLAN network interface parameters include the IP address, subnet mask, and gateway IP address. • The Call Server IP address defaults to 0.0.0.0. for a Standalone Signaling Server - NRS only. • Enter the IP address of the NRS (Primary or Alternate NRS IP address).
2	Reboot the Signaling Server after proper configuration or reconfiguration. If the Signaling Server reboots successfully, the NRS is configured with the default settings.
3	Log on to NRS Manager using the default user ID and password (see Procedure 27 "Logging on to NRS Manager" (page 169)).
4	Configure the NRS Server Settings in NRS Manager. See *Network Routing Service Installation and Commissioning NN43001-564)*.
5	Log off of NRS Manager. See Procedure 32 "Logging off of NRS Manager" (page 182).

6 Reboot the Signaling Server.

If the Signaling Server boots successfully, the NRS server is properly configured.

—End—

Enable and configure the NRS server in Coresident mode

Use the following procedure to enable and configure the NRS server in Coresident mode.

Procedure 25
Enabling and configuring the NRS server in Coresident mode

Step	Action

If the Signaling Server is configured in Coresident mode, proceed directly to step 3.

1 Enable the NRS using the Signaling Server Software Installation Tool.

The following summarizes the tasks required to install a Coresident Signaling Server. Follow the detailed procedures in "Software installation" (page 111) or "Signaling Server reconfiguration" (page 199) for complete instructions.

- Perform the introductory steps for the Signaling Server installation.
- Configure the Signaling Server as a Leader, when you are prompted.
- Select Coresident mode (LTPS + VTRK + NRS) for the Signaling Server.
- Select whether the NRS supports the H.323 Gatekeeper, the SIP Redirect Server, or both.
- Select the type of NRS (Primary, Alternate, or Failsafe).
- Enter the node ID, host name, ELAN network interface parameters, TLAN network interface parameters, node IP address, and the Call Server IP address.

  The ELAN and TLAN network interface parameters include the IP address, subnet mask, and gateway IP address.
- Enter the IP address of the NRS (Primary NRS IP address, Alternate IP address, or both).

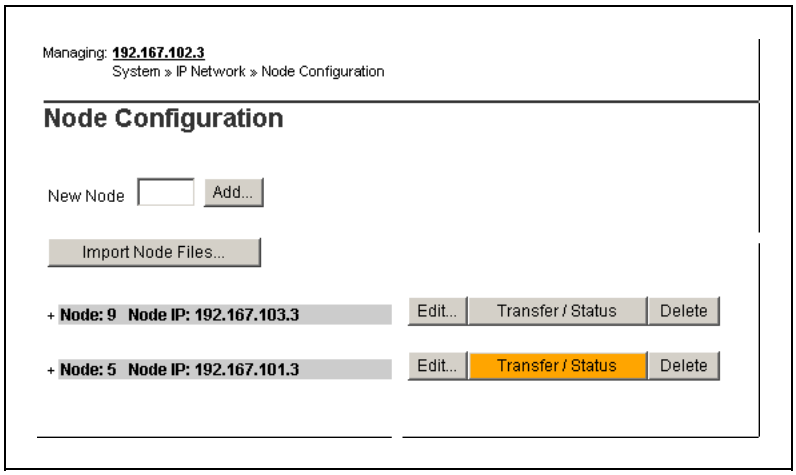
2 Reboot the Signaling Server, after proper configuration or reconfiguration of the Signaling Server.

3 Log on to Element Manager.

4 From the navigation tree, select **IP Network > Nodes: Servers, Media Cards** .

The **Node Configuration** web page appears.

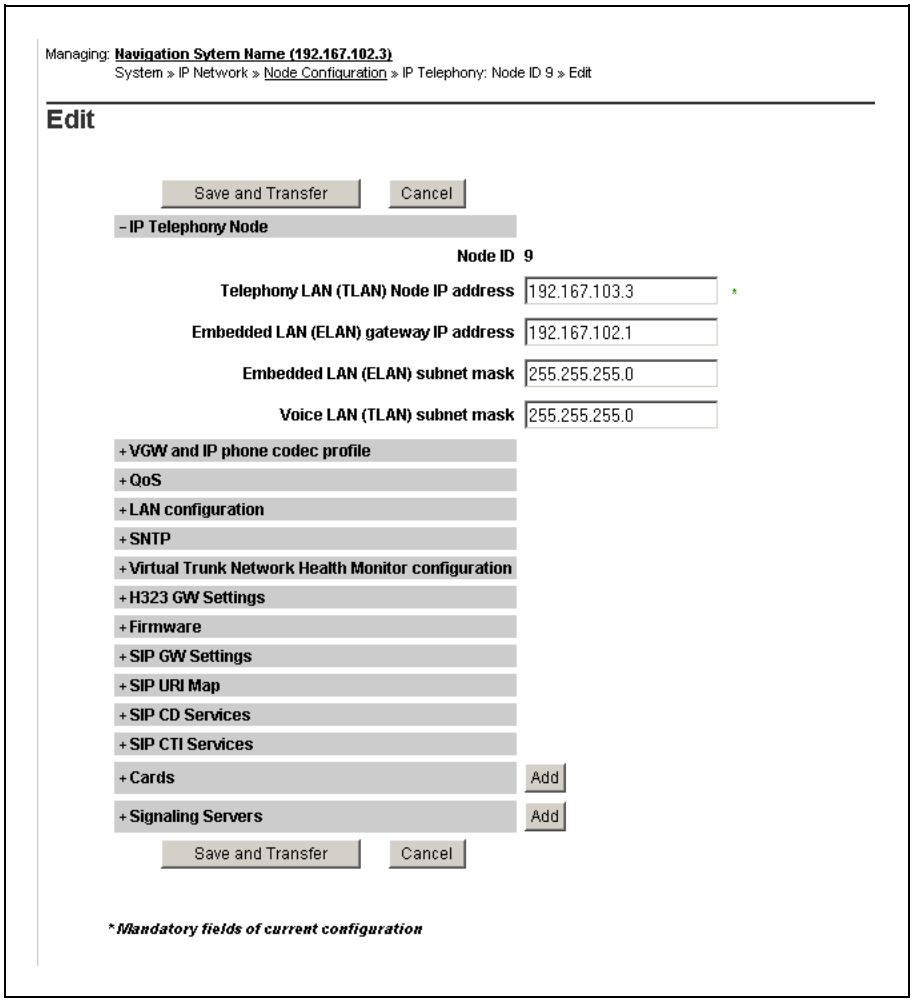
Figure 128
Node configuration



5 Select **Edit** on the appropriate node.

The Edit node configuration web page appears.

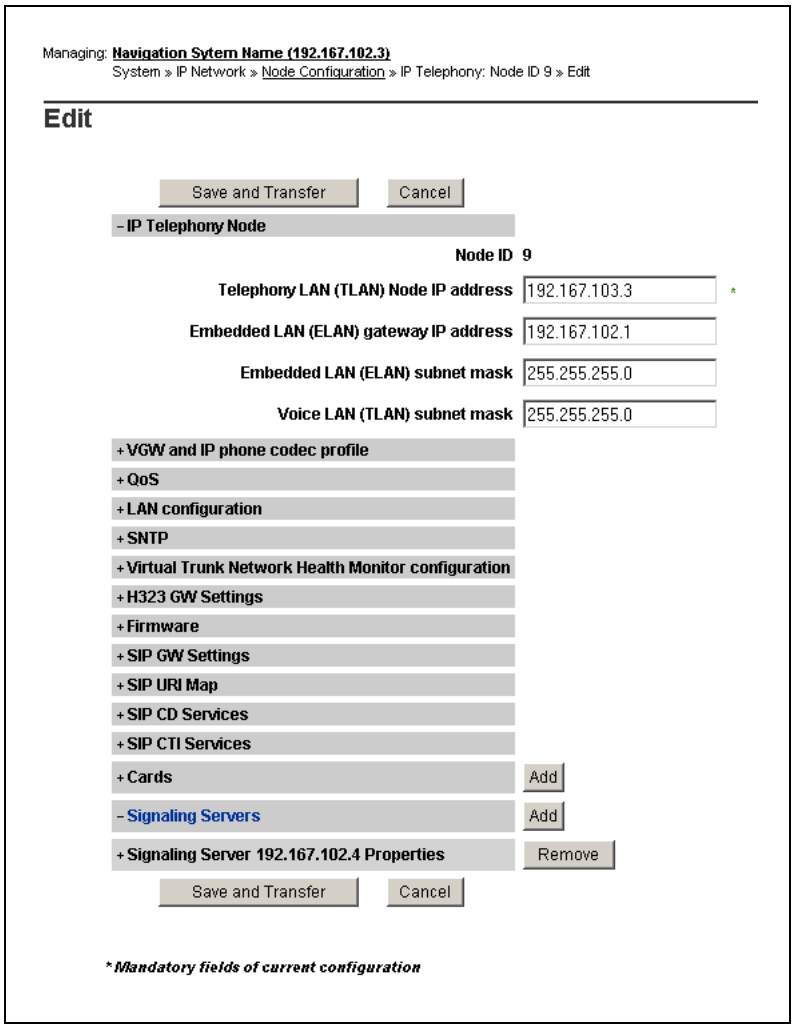
Figure 129
Edit node configuration



6 Click **Signaling Servers** to expand the section and show a list of the Signaling Servers on the node.

The Signaling Server section expands and lists all Signaling Servers on the node.

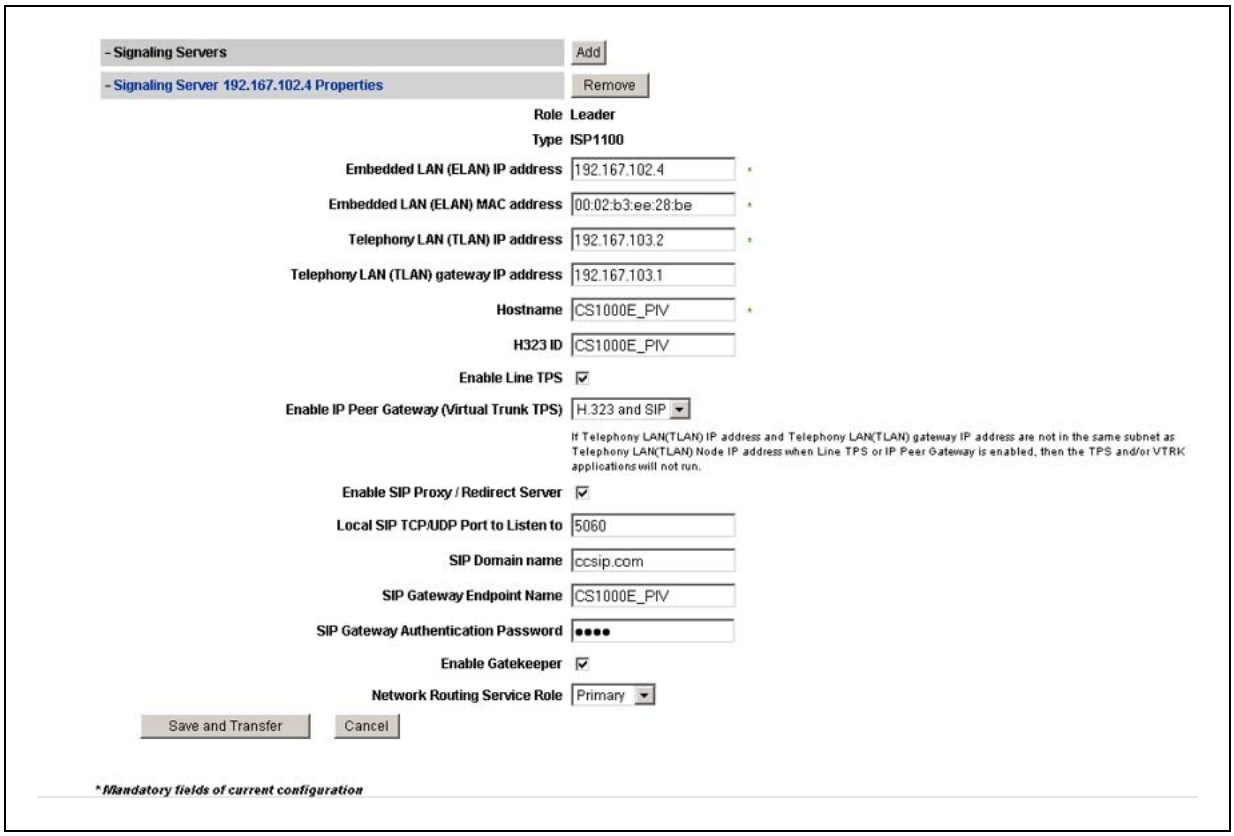
Figure 130
Signaling Server list for node



7 Select the appropriate **Signaling Server xxx.xxx.xxx.xxx Properties** from the list to view the properties of the identified Signaling Server.

The Signaling Server xxx.xxx.xxx.xxx properties web page appears.

Figure 131
Signaling Server xxx.xxx.xxx.xxx properties



8 To enable the NRS, perform the following tasks:

- Enable the SIP Proxy/Redirect Server or the H.323 Gatekeeper or both:
  - — To enable the SIP Proxy Server, the SIP Redirect Server, or both, perform step a.
  - — To enable the H.323 Gatekeeper, perform step b.
  - — To enable the H.323 Gatekeeper, the SIP Proxy Server, and the SIP Redirect Server, perform step a and step b.
- Select the NRS role (see step c).
- Ensure that you correctly configure the remaining Signaling Server properties.

a. Click the **Enable SIP Proxy / Redirect Server** check box to enable the SIP Proxy / Redirect Server. A check mark appears in the check box.

Figure 132
Enabling the SIP Proxy / Redirect Server

Note: You must also configure the SIP Gateway. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.

b. Click the **Enable Gatekeeper** check box to enable the H.323 Gatekeeper. A check mark appears in the check box.

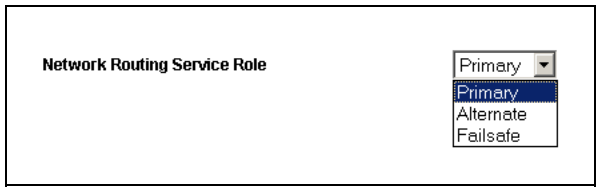
Figure 133
Enabling the H.323 Gatekeeper

Note: You must also configure the H.323 Gateway. See *IP Peer Networking Installation and Commissioning (NN43001-313)* .

c. Select the NRS role from the **Network Routing Service Role** list.

The three options are Primary, Alternate, and Failsafe.

Figure 134
Network Routing Service Role



9 Click **Save and Transfer** to save the changes and transfer the properties to all nodes.

10 Click **Logout** in the top right corner of the Edit page to log off of Element Manager.

11 Reboot the Signaling Server.

12 After you successfully reboot of the Signaling Server, log on to NRS Manager using the default user ID and password. See Procedure 27 "Logging on to NRS Manager" (page 169).

13 Configure the NRS Server Settings in NRS Manager (see *Network Routing Service Installation and Commissioning NN43001-564)*).

14 Log off the NRS. See Procedure 32 "Logging off of NRS Manager" (page 182).

15 Reboot the Signaling Server.

If the Signaling Server boots successfully, the NRS server is properly configured.

—End—

Changing a Coresident NRS server to a Standalone NRS server Use the Signaling Server Software Installation Tool to reconfigure a Coresident NRS server as a Standalone NRS server.

Overview

The following summarizes the tasks required to upgrade a Succession 1000 Release 3.0 Signaling Server to a CS 1000 Release 5.0 Signaling Server:

- "Back up the Succession 3.0 H.323 Gatekeeper database" (page 163)
- "Upgrade the Signaling Server software" (page 168)
- "Reconfigure the Signaling Server" (page 168)
- "Convert the Succession 3.0 H.323 Gatekeeper database to a CS 1000 Release 5.0 NRS database" (page 169)
- "Activate the NRS database" (page 180)

WARNING
Complete each of these tasks in the order specified. Failure to complete all of these tasks in the specified order causes problems (see "Upgrade problems and consequences" (page 182)).

Three types of Signaling Servers can provide redundancy in a Succession 3.0 network:

- Primary Signaling Server
- Alternate Signaling Server
- Failsafe Signaling Server

If these Signaling Servers exist in your Succession 3.0 network, you must upgrade each to CS 1000 Release 5.0 and convert the associated H.323 Gatekeeper databases (if present) to NRS databases, because NRS cannot use an H.323 Gatekeeper database directly.

Note: Nortel Networks recommends that you upgrade the Alternate Signaling Server before you upgrade the Primary Signaling Server.

The Primary and Alternate Signaling Servers can coexist with mixed Signaling Server software releases. However, when a mixture exists, the Alternate and Primary Signaling Servers cannot synchronize their H.323 Gatekeeper databases. For example, if the Primary Signaling Server is running CS 1000 Release 5.0 software while the Alternate Signaling Server is running Succession 3.0 software, no H.323 Gatekeeper database synchronization occurs between the databases. In this situation, synchronization of the H.323 Gatekeeper databases requires manual provisioning.

Nortel provides a 45-day period where a Failsafe Signaling Server that isn't running CS 1000 Release 5.0 software can coexist with Primary and Alternate Signaling Servers that are running CS 1000 Release 5.0 software. The CS 1000 Release 5.0 NRS database responds to Keep-alive messages from the Succession 3.0 Failsafe Signaling Server to facilitate a smooth upgrade path. You can upgrade the Primary and Alternate H.323 Gatekeepers to CS 1000 Release 5.0 without upgrading the Failsafe Signaling Server right away. You can upgrade the Failsafe Signaling Server as time permits over the 45-day period. After 45 days, the Alternate Signaling Server (running CS 1000 Release 5.0) does not recognize the Failsafe Signaling Server (running Succession 3.0).

If you do not upgrade the Failsafe Signaling Server to CS 1000 Release 5.0, it cannot synchronize its H.323 database with the NRS database (the NRS database contains registration information essential for its operation). In this situation, the Failsafe Signaling Server maintains the old H.323 Gatekeeper database to resolve queries (if the Failsafe becomes active).

ATTENTION

IMPORTANT!

Nortel recommends that you convert the H.323 Gatekeeper database to an NRS database as soon as possible after you upgrade the software.

WARNING

IMPORTANT!

Failing to upgrade the Failsafe Signaling Server within 45 days jeopardizes the redundancy in your network.

Before you begin

Before upgrading the software, you must do the following:

- Connect the Signaling Server — see Procedure 13 "Connecting a Nortel ISP1100 server" (page 94)
- Obtain the CS 1000 Release 5.0 version of the Signaling Server Software Install CD-ROM — see "Signaling Server Software" (page 100)
- Ensure there is 1 GB of RAM configured on your legacy Nortel ISP1100 server. If necessary, refer to "Upgrade the RAM on a Nortel ISP1100 Signaling Server" (page 304) to upgrade the RAM before starting the upgrade procedure.

Upgrade the Succession 3.0 Signaling Server

ATTENTION

IMPORTANT!
The Signaling Server is out-of-service during software upgrade.

Back up the Succession 3.0 H.323 Gatekeeper database

You must back up the H.323 Gatekeeper database using the Gatekeeper web pages in the Succession 3.0 version of Element Manager. The Gatekeeper web pages provide two backup options: Manual Backup and Automatic Backup. Use the Manual Backup option to back up the H.323 Gatekeeper database immediately. Use the Automatic option to schedule the database backup at a later date and time.

The H.323 Gatekeeper database is backed up to a specific directory on the Signaling Server. You must also download a copy of the database backup file to your local PC. After you upgrade the Signaling Server to CS 1000 Release 5.0, the backed-up H.323 database must be converted to a CS 1000 Release 5.0 NRS database. The NRS conversion tool accesses the backed-up H.323 Gatekeeper database from your local PC by the CS 1000 Release 5.0 NRS conversion tool during the conversion process.

Use the following procedure to back up the Succession 1000 Release 3.0 H.323 Gatekeeper database.

Procedure 26

Backing up the Succession 3.0 H.323 Gatekeeper database

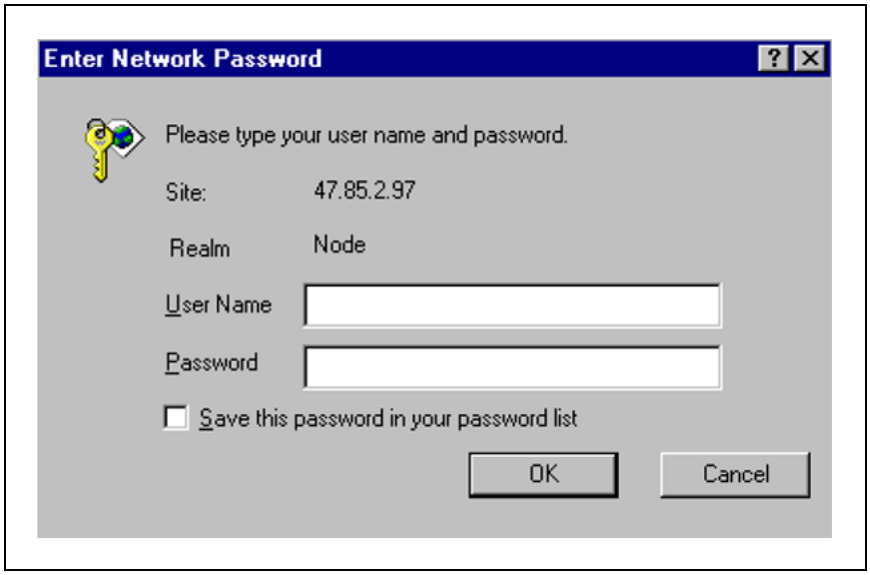
Step	Action
1	Enter the H.323 Gatekeeper URL in the Address Bar of the web browser on the network. The H.323 Gatekeeper address is configured at each H.323 Gateway (that is, each Signaling Server).

The URL is the TLAN network interface IP address of the Signaling Server followed by gk. For example: http://47.39.2.50/gk/

Note: You must include gk as part of the URL because the H.323 Gatekeeper resides on the Signaling Server platform with other applications.

The **Enter Network Password** logon dialog box appears.

Figure 135
Enter Network Password logon dialog box



Note: If you are already logged in to Element Manager, you can access the Gatekeeper web pages as follows:

- Select **Network Numbering Plan > Gatekeeper** from the navigation tree.
- Enter the **Gatekeeper IP Address.**
- Click **Next.**
- When the logon window appears (see Figure 135 "Enter Network Password logon dialog box" (page 164)), enter the **User Name** and **Password.**
- Click **OK.**

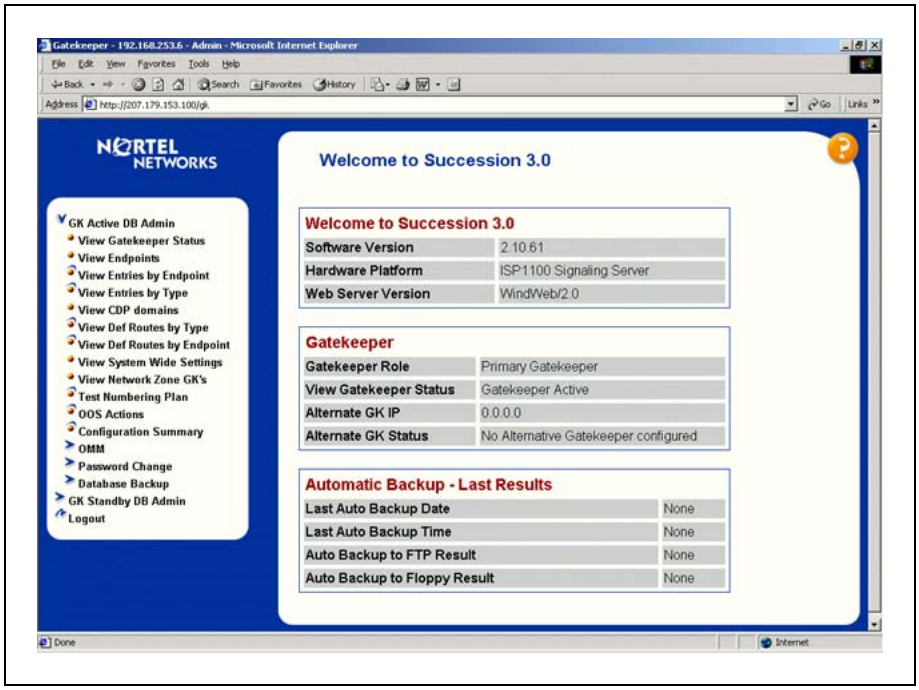
2 Enter your user name in the **User Name** text box (the default username is *gkadmin*).

3 Enter your password in the **Password** text box (the default password is *gkadmin*).

4 Click **OK.**

- If your logon is successful, the **Welcome** web page appears.

Figure 136
Welcome web page

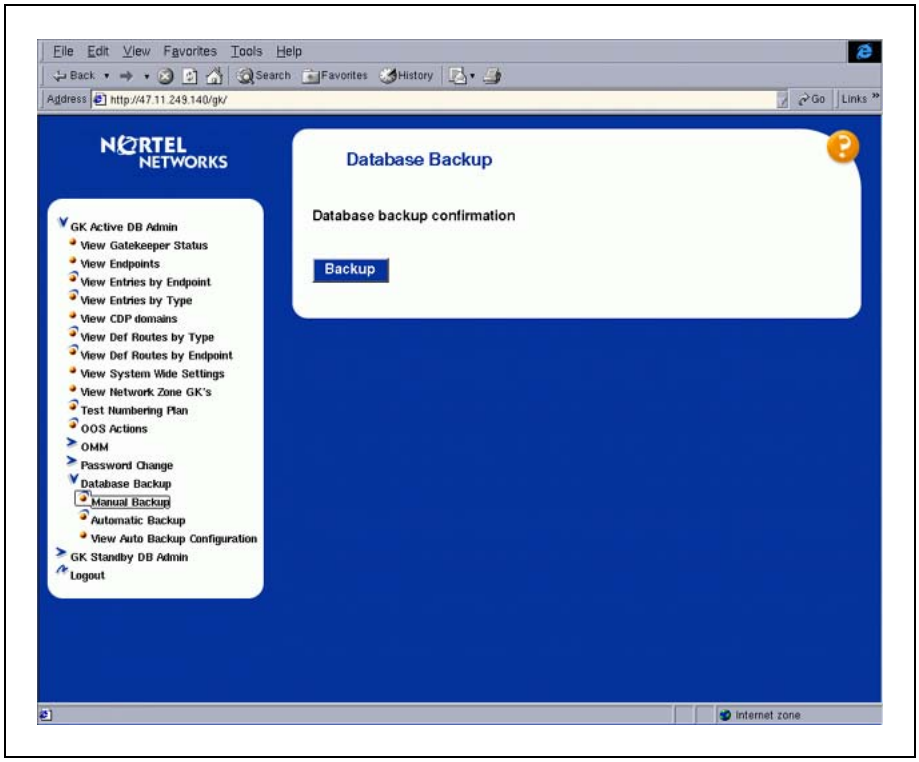


- If your logon is unsuccessful, an error message appears, and then the **Enter Network Password** dialog box reappears.

5 To perform a manual backup of the database, select **GK Active DB Admin > Database Backup > Manual Backup** from the navigation tree.

The Database Backup web page appears.

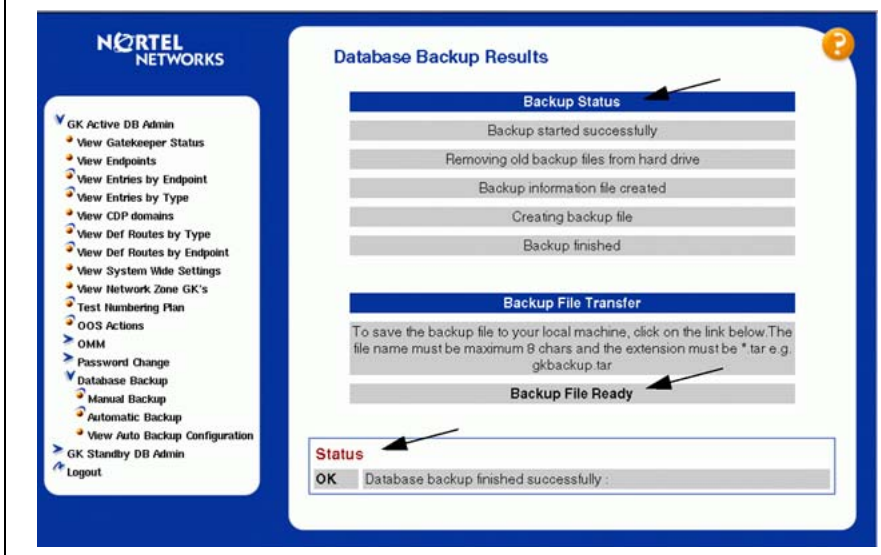
Figure 137
Manual database backup



6 Click **Backup.**

The **Database Backup Results** web page appears.

Figure 138
Manual Database Backup Results



The results appear under the Backup Status area at the top of the web page and in the Status area at the bottom of the web page.

7 Click the **Backup File Ready** link.

A download window appears.

ATTENTION
You must back up the Succession 3.0 H.323 Gatekeeper database to your local PC to ensure a local database migration.

8 Select a folder on your computer as a download target, and save the file.

9 Click **Save.**

10 Ensure that the backup file (gkbackup.tar) was downloaded to the selected folder on your local PC.

11 Check the list of files in the gkbackup.tar file on your local PC.

The files in the gkbackup.tar file consist of some core files (listed below), and possibly others, depending on the configuration of your H.323 Gatekeeper.

Core files:

- bootp.tab
- config.ini
- domain.xml
- 00000001.xml
- backupinfo.inf

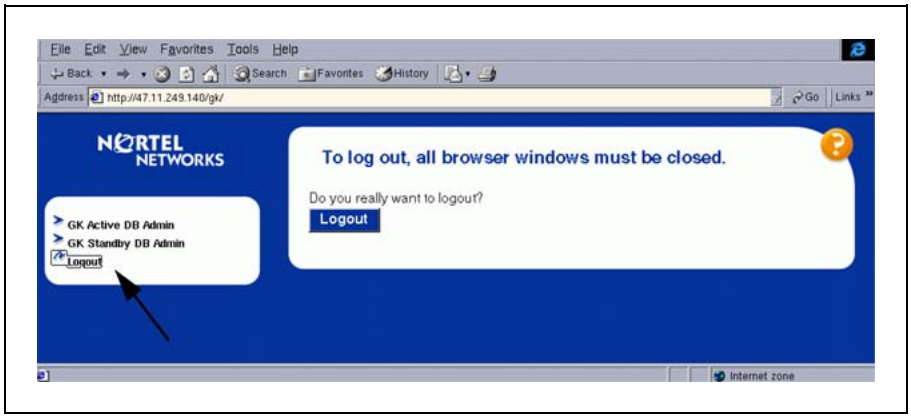
If all core files are present in the gkbackup.tar file, your backup was successful.

If all core files are not present in the gkbackup.tar file, repeat this entire procedure (Procedure 26 "Backing up the Succession 3.0 H.323 Gatekeeper database" (page 163)).

12 Click **Logout** at the bottom of the navigation tree to log off of the H.323 Gatekeeper web pages in Element Manager.

The Logout web page appears.

Figure 139
Logout web page



Note: You must close all browser windows to log off.

13 Click **Logout.**

14 Click **Yes.**

The browser window closes.

—End—

Upgrade the Signaling Server software

Use the Procedure 34 "Upgrading the Signaling Server software" (page 188) procedure to upgrade the Signaling Server from Succession 3.0 software to CS 1000 Release 5.0 software.

ATTENTION

IMPORTANT!
The Signaling Server is out of service during the software upgrade process.

Reconfigure the Signaling Server

Use the "Signaling Server reconfiguration" (page 199) procedure to obtain and configure the NRS.

ATTENTION

IMPORTANT!
If you do not reconfigure the Signaling Server, you cannot use a SIP Proxy/Redirect Server.

Convert the Succession 3.0 H.323 Gatekeeper database to a CS 1000 Release 5.0 NRS database

The Succession 3.0 H.323 Gatekeeper database cannot be directly used by the CS 1000 Release 5.0 NRS. The NRS Manager in CS 1000 Release 5.0 provides a conversion tool called Gatekeeper/NRS Data Upgrade. This tool converts the backed-up Succession 3.0 H.323 Gatekeeper database into a CS 1000 Release 5.0 NRS database.

The first step in the conversion process is to create a Service Domain and a Level 1 Domain on the upgraded Signaling Server. You must select these configured domains in the GK/NRS upgrade tool before conversion can begin. The Succession 3.0 H.323 Gatekeeper conversion process results in an NRS database that is in Standby status. It must be activated before the CS 1000 Release 5.0 NRS can use the data.

The conversion of the H.323 Gatekeeper database involves the following tasks:

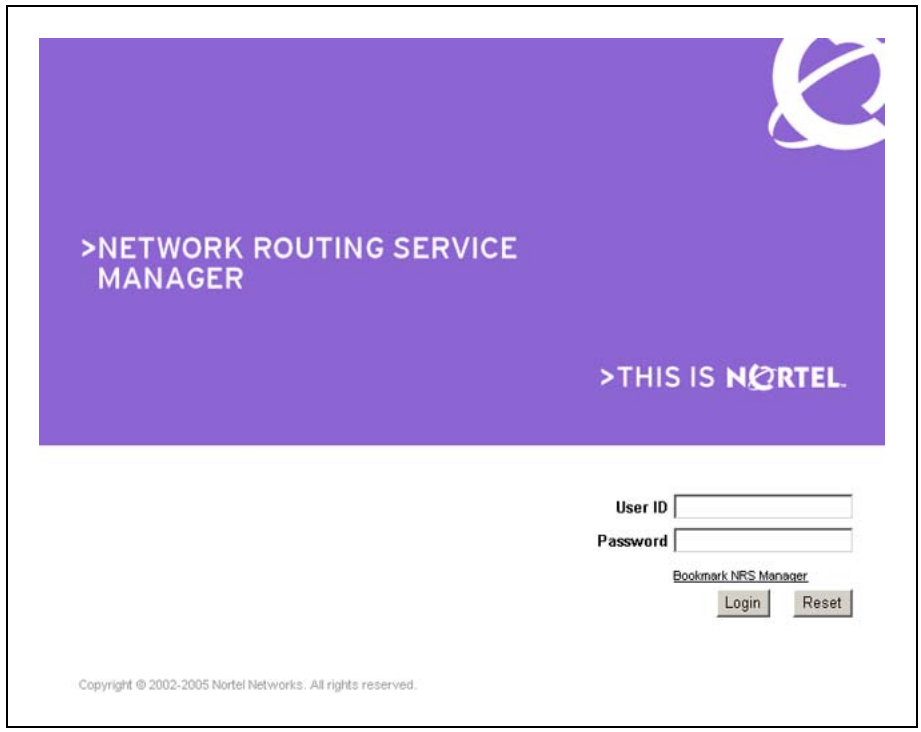
- log on to NRS Manager on the upgraded Signaling Server (see Procedure 27 "Logging on to NRS Manager" (page 169)
- add a Service Domain (see Procedure 28 "Adding a Service Domain" (page 172)
- add a Level 1 Domain (see Procedure 29 "Adding an L1 Domain" (page 175)
- convert the H.323 Gatekeeper database to a "standby" NRS database (see Procedure 30 "Converting the Succession 3.0 H.323 Gatekeeper database to an NRS database" (page 177)

Use the following procedure to log on to NRS Manager.

Procedure 27
Logging on to NRS Manager

Step	Action
1	Open the Microsoft Internet Explorer 6.0 (or later) browser.
2	Type the URL for the NRS into the browser address field. The URL has the following format: **`http://[Signaling_Server_ELAN_IP_address]/nrs/`**. The NRS Manager logon web page appears.

Figure 140
NRS Manager logon



Note: To add a bookmark to your Internet Explorer Favorites list, click the **Bookmark NRS Manager** link.

CS 1000 Release 5.0 provides security through user authentication and database access privileges. A user name and password are required to access the NRS database. User authentication parameters are configurable in Element Manager.

Support exists for two types of access privileges:

- Administrative privileges — Administrative users have full read/write privileges. An administrator can view and modify NRS data.
- Monitor privileges — Observers have read-only privileges. An observer can only view the NRS data.

  Note: When you log on as an administrator, you can create new users. See *Network Routing Service Installation and Commissioning NN43001-564)*.

ATTENTION

IMPORTANT!

Nortel recommends that you use the default User ID and Password to configure the NRS server. After the NRS server configuration is complete, change the User ID and Password for increased system security.

The default values are:

- User ID — **admin**
- password — **admin**

The user name and password are stored (in encrypted format) in the same database as the SIP Redirect Server or SIP Proxy Server data. For that reason, you must enable the H.323 Gatekeeper or SIP Redirect Server before you log on to NRS Manager. To enable the H.323 Gatekeeper or SIP Redirect Server, refer to *IP Peer Networking Installation and Commissioning (NN43001-313)*.

3 Enter the **User ID** and **Password** , and click **login** to log on.

The User ID and Password are securely transferred from the web client to the NRS web server where they are authenticated.

- If user authentication fails, an appropriate error message appears on the NRS Manager logon web page.

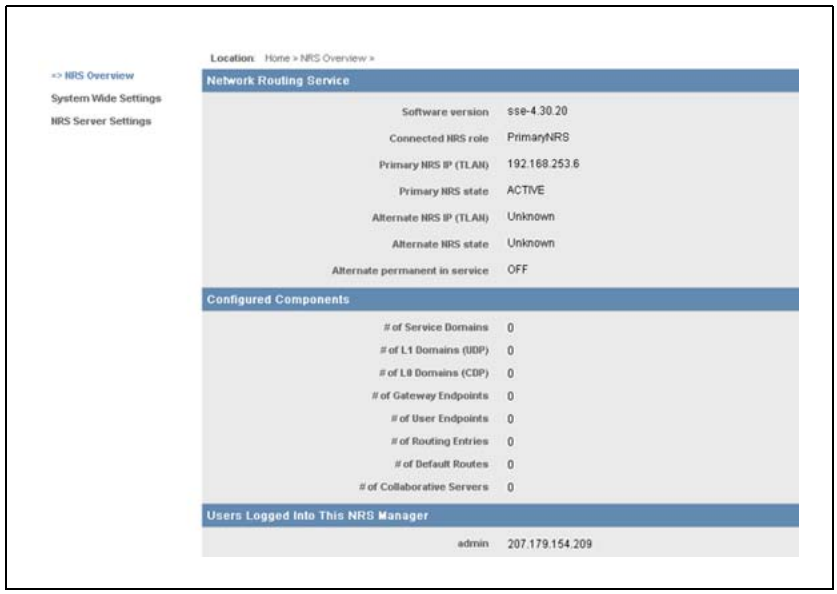
  Note: **Reset** clears the User ID and Password text boxes.

- If you did not enable the H.323 Gatekeeper or the SIP Redirect Server before you logged on to NRS Manager, the NRS Manager logon web page turns white and the following system messages appear:

```
Error code is WC0030:
Error:  Network Routing Service (NRS) Manager is not
accessible when neither Gatekeeper nor SIP Proxy/
Redirect applications are enabled.
Please close the IE window.  Enable the applicatio
n(s).
Reboot the Signaling Server, then access NRS Manager
again.
```

- If user authentication succeeds, the NRS Overview web page appears.

Figure 141
NRS Overview



With NRS Manager, you can navigate to specific components of the NRS for configuration and maintenance.

Note: After 60 minutes of inactivity, your NRS session times out and you are logged out of NRS Manager; the default session timeout is 60 minutes. The default session timeout clock is configurable using the CLI.

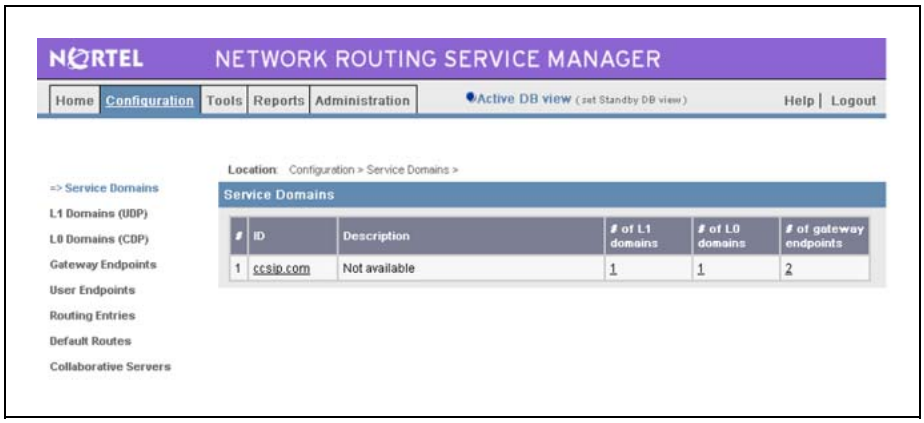
—End—

Use the following procedure to add a Service Domain.

Procedure 28
Adding a Service Domain

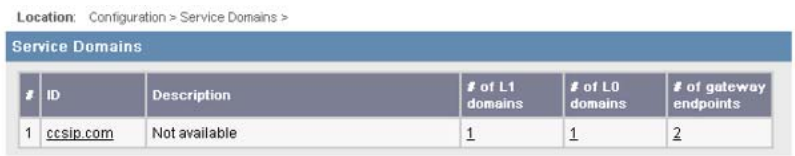
Step	Action
1	Click the **Configuration** navigation tab. The NRS Manager configuration web page appears.

Figure 142
NRS Manager configuration



The **Service Domains** option is highlighted by default on the navigation tree and the Service Domains window shows all configured Service Domains in the active NRS database view.

Figure 143
Service Domains: active DB view



The NRS database has two views: Active and Standby.

- The Active NRS database view is used for run-time queries.
- The Standby NRS database view is used for administrator modifications.

The database is in Active view by default when the NRS is launched.

Figure 144
Active DB view

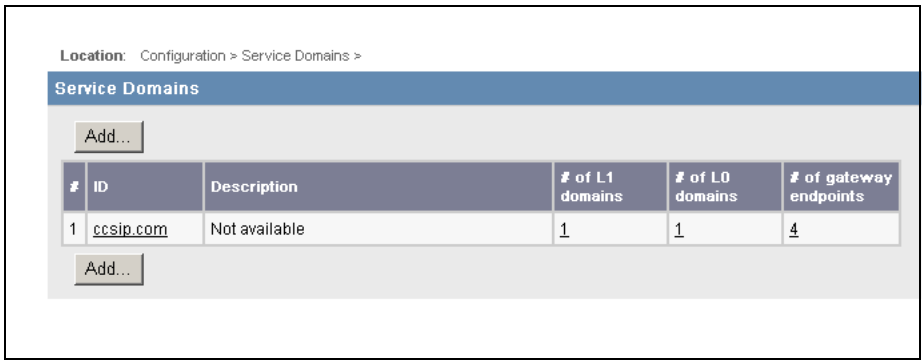
The NRS database must be in Standby view to be modified.

2 Click the **set Standby DB view** switch (to the right of the navigation tabs) to switch from the Active NRS database view to the Standby NRS database view.

This switch is used for toggling between Active and Standby NRS database views.

When you click **set Standby DB view**, the Service Domains web page reappears showing all configured Service Domains and an option to add a new Service Domain.

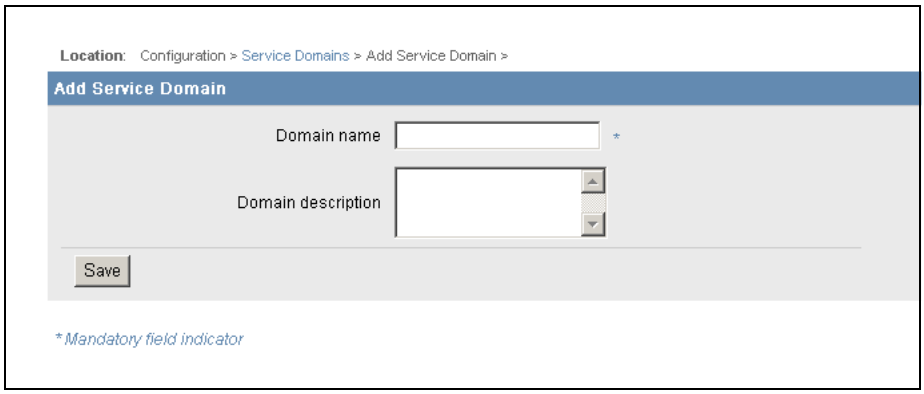
Figure 145
Service Domains: standby DB view



3 Click **Add.**

The **Add Service Domain** web page appears.

Figure 146
Add Service Domain



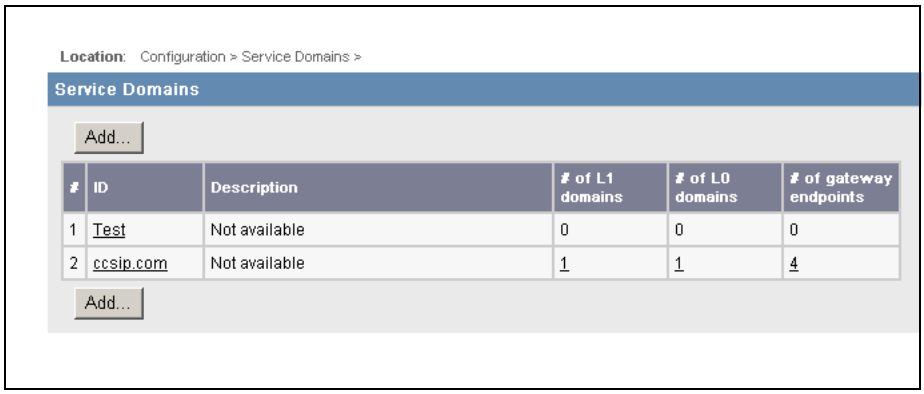
4 Enter a **Domain name** for the Service Domain. This entry must match the SIP Domain name field in the Signaling Server settings in Element Manager.

5 Enter a **Domain description** for the Service Domain.

6 Click **Save** to update the Standby NRS database.

The Service Domains web page reappears showing the newly added Service Domain.

Figure 147
Added Service Domain



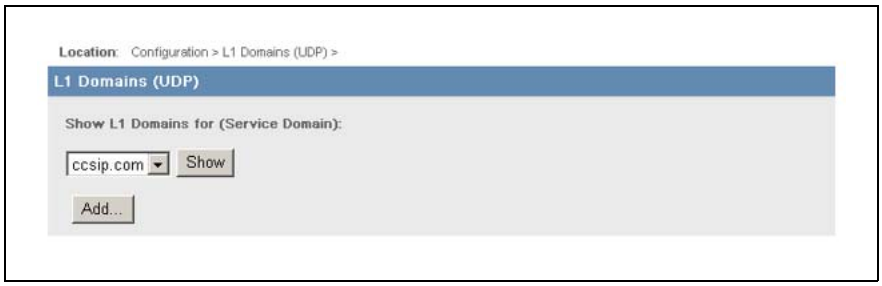
—End—

Use the following procedure to add a Level 1 Domain.

Procedure 29
Adding an L1 Domain

Step	Action
1	Click the **Configuration** tab.
2	Click **set Standby DB view** switch (to the right of the navigation tabs) to switch from the Active NRS database view to the Standby NRS database view.
3	Click **L1 Domains** from the navigation tree. The **L1 Domains** web page appears.

Figure 148
L1 Domains



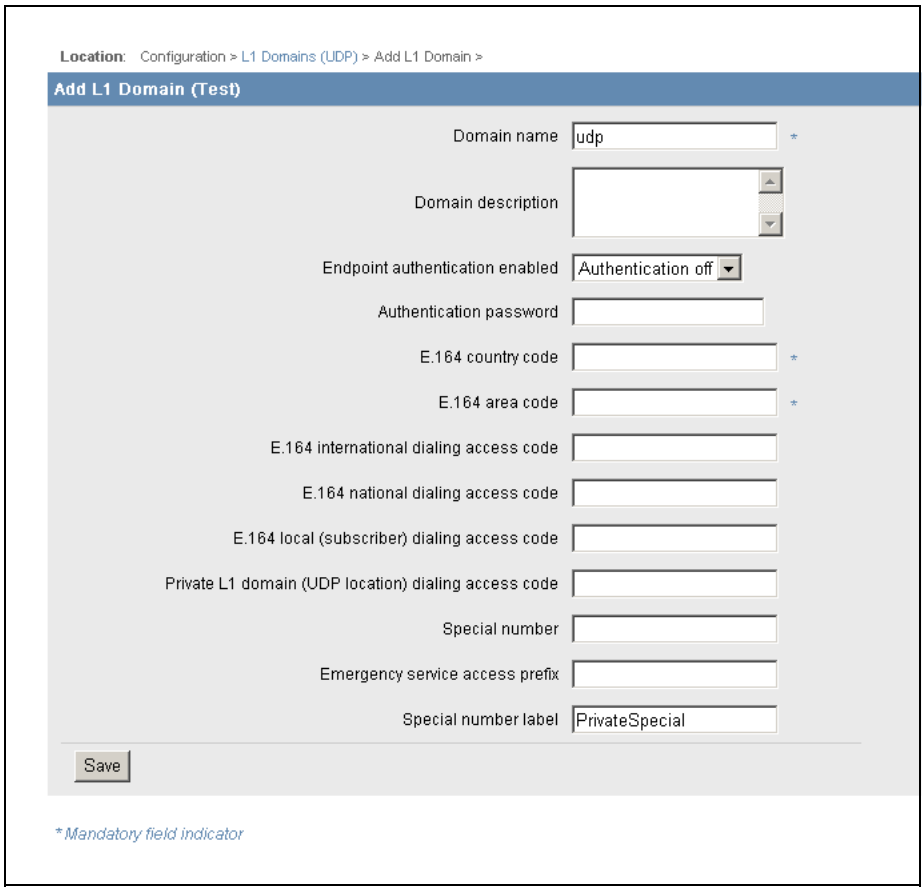
The drop-down list contains all available Service Domains.

4	Select the Service Domain (the one that was just added) for the new L1 domain from the list.

5 Click **Add.**

The **Add L1 Domain** web page appears.

Figure 149
Add L1 Domain



6 Enter the **Domain name** of the L1 Domain.

7 Enter the **Domain description.**

8 Turn authentication on or off from the **End point authentication enabled** list.

If you select **Authentication on**, all endpoints require authentication.

9 Enter the **Authentication password,** if **Authentication on** was selected in step 8.

10 Enter the **E.164 country code.**

11 Enter the **E.164 area code.**

12 Enter the **E.164 international dialing access code.**

13 Enter the **E.164 national dialing access code.**

14 Enter the **E.164 local (subscriber) dialing access code.**

15 Enter the **Private L1 domain (UDP location) dialing access code.**

16 Enter the **Special number.**

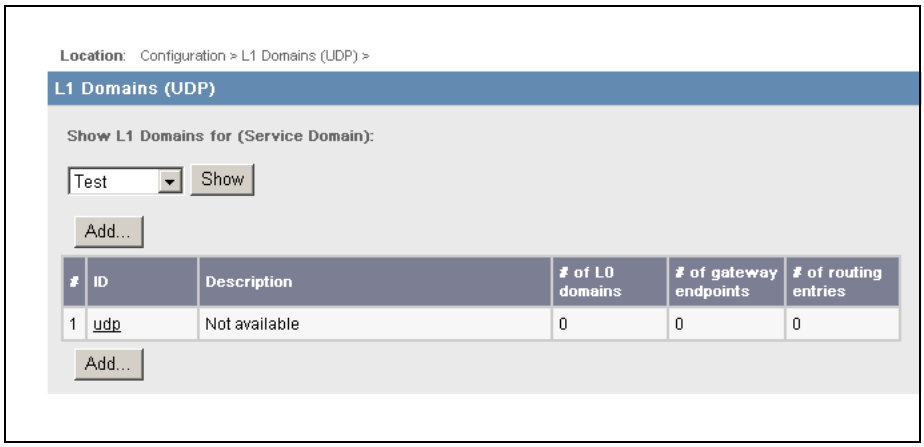
17 Enter the **Emergency service access prefix.**

18 Enter the **Special number label.** The label must be alphanumeric and can be up to 30 characters in length.

19 Click **Save.**

The **L1 Domains** web page appears showing the newly added domain in the Service Domain.

Figure 150
Added L1 Domain



—End—

Use the following procedure to convert the Succession 3.0 H.323 Gatekeeper database to a CS 1000 Release 5.0 NRS database.

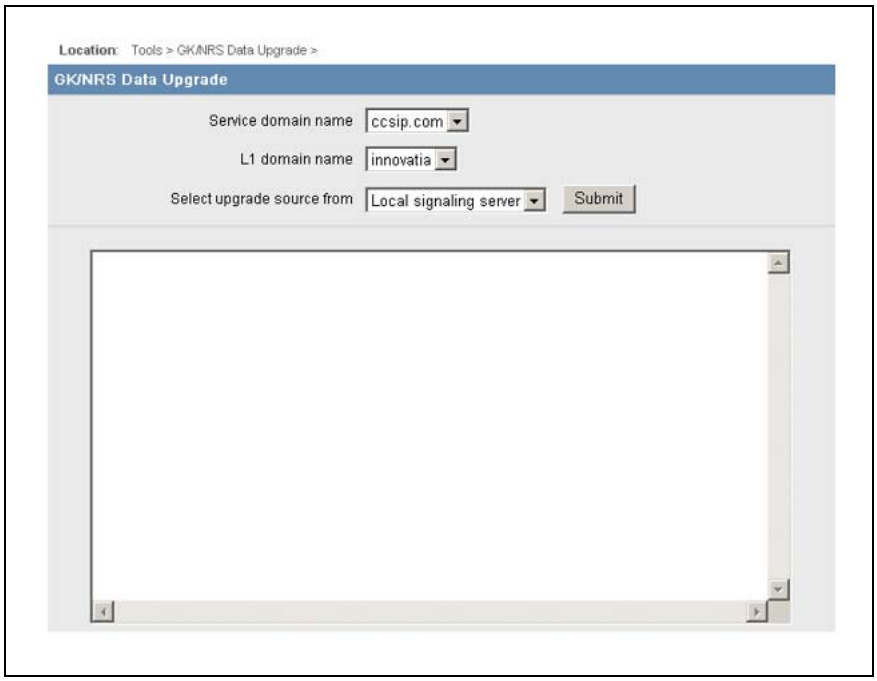
Procedure 30
Converting the Succession 3.0 H.323 Gatekeeper database to an NRS database

Step	Action
1	Click the **Tools** tab.

2 Click the **GK/NRS Data Upgrade** option from the navigation tree.

- If you configured the Service Domain and Level 1 Domain, the GK/NRS Data Upgrade web page appears.

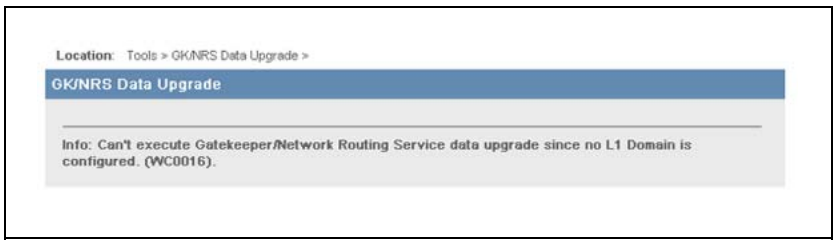
Figure 151
GK/NRS Data Upgrade



Note: The values in the Service Domain name, L1 Domain name in the preceding figure are for illustrative purposes only.

- If you did not configure the Service Domain or Level 1 Domain, a message indicates that the Gatekeeper-to-Networking Routing Service data upgrade cannot execute, because a Level 1 Domain is not configured.

Figure 152
Domains not configured



Ensure that Procedure 28 "Adding a Service Domain" (page 172) and Procedure 29 "Adding an L1 Domain" (page 175) are completed before starting this procedure.

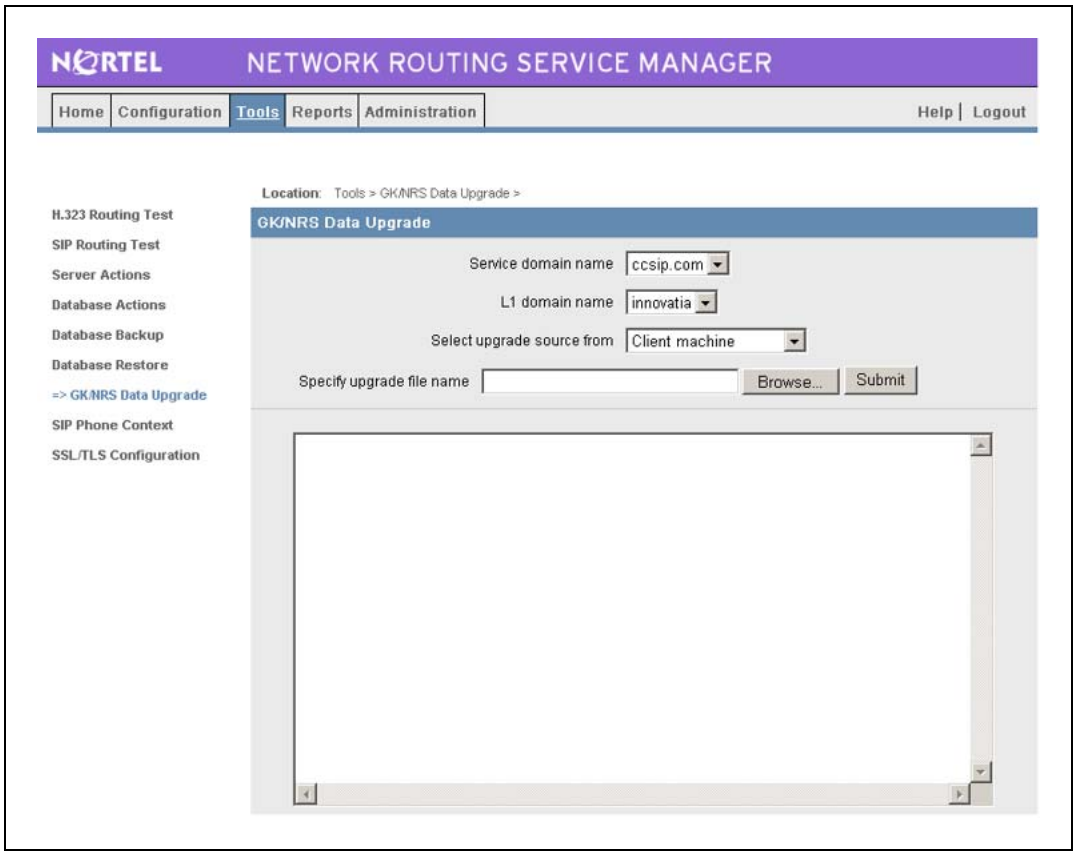
3 Select the Service Domain (configured in Procedure 28 "Adding a Service Domain" (page 172)) from the **Service domain name** list.

4 Select the Level 1 Domain (configured in Procedure 29 "Adding an L1 Domain" (page 175)) from the **L1 domain name** list.

5 Select **Client machine** from the **Select Upgrade source from** list.

A **Specify upgrade file name** window appears on the GK/NRS Data Upgrade web page.

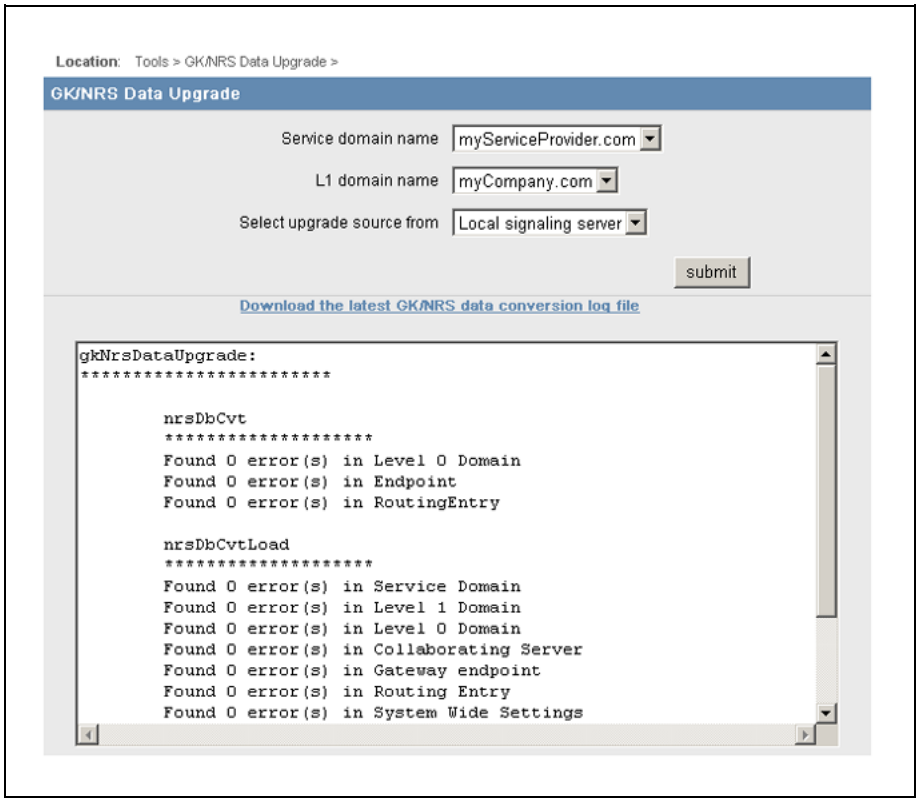
Figure 153
GK/NRS Data Upgrade from client machine



6 Enter the location of the H.323 Gatekeeper database backup file on your local PC and click **Submit.**

The GK/NRS Data Upgrade web page is updated with the conversion results.

Figure 154
GK/NRS Data Upgrade conversion results



Note: The values in the Service Domain name, L1 Domain name in the preceding figure are for illustrative purposes only. Also, the figure identifies the Local signaling server as an upgrade source (as opposed to Client machine); the results are the same regardless of the upgrade source.

—End—

After you convert the H.323 Gatekeeper database to an NRS database, the NRS database is loaded in Standby database view. The NRS database must be activated before the NRS can use its data.

Activate the NRS database

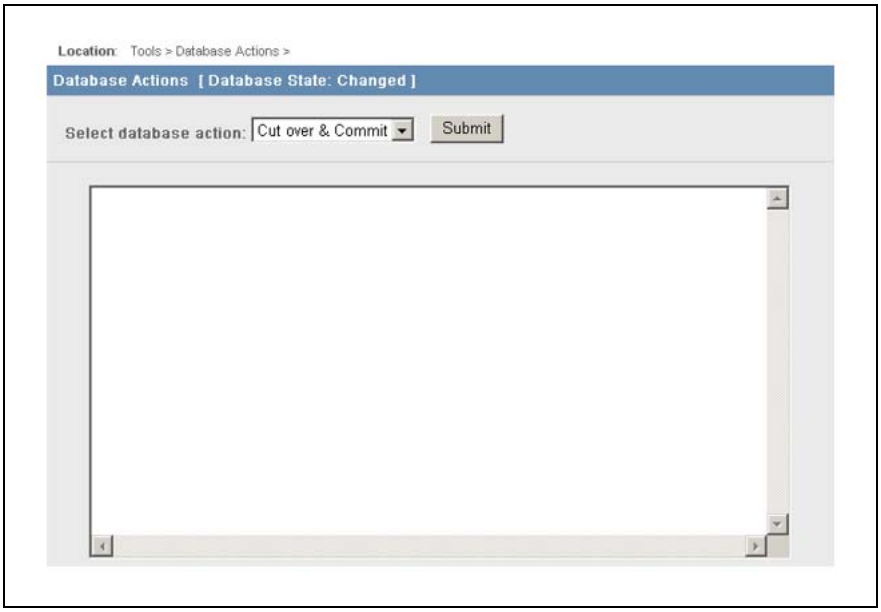
When the Succession 3.0 H.323 Gatekeeper database is converted to a CS 1000 Release 5.0 NRS database, the resulting NRS database is in "Standby" database view. NRS cannot use an NRS database in "Standby" database view. The NRS database must be activated before the NRS can use its data.

Use the following procedure to activate the "Standby" NRS database.

Procedure 31
Activating the NRS database

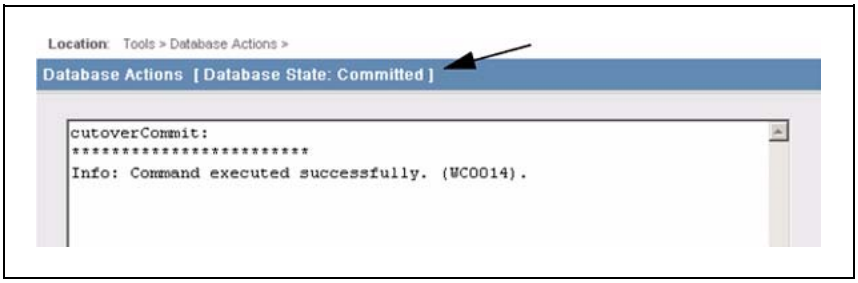
Step	Action
1	Click the **Tools** tab.
2	Select **Database Actions** from the navigation tree. The Database Actions web page appears.

Figure 155
Database actions



Step	Action
3	Select **Cut over & Commit** from the **Select database action** list.
4	Click **Submit**. A message in the text box indicates that the cut over and commit operation succeeded.

Figure 156
Database Actions: cutover and commit (successful)



The NRS database is saved and is in Active DB view.

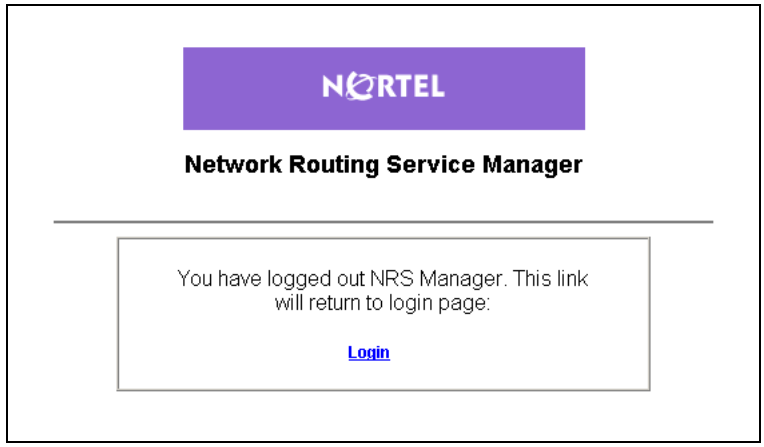
—End—

Use the following procedure to log off of NRS Manager.

Procedure 32
Logging off of NRS Manager

Step	Action
1	Click **Logout** in the top right hand corner of any NRS Manager web page. The Networking Routing Service Manager logout web page appears.

Figure 157
NRS logout



Step	Action
2	Close the browser window.

—End—

Upgrade problems and consequences

Scenario 1

You fail to back up your Succession 3.0 H.323 Gatekeeper database and you are unsuccessful at upgrading the Signaling Server software.

Impact: Severe

You must downgrade the system to the previous software release, which is a complex and time-consuming process.

Scenario 2

Errors occur during the database conversion.

Impact: Severe

One of two possible events can occur:

1. You do not realize that part of the database conversion process did not proceed smoothly. If you place the converted database into active service, the performance can degrade.
2. You start the conversion process, but do not monitor it. It is possible to miss informative error information.

Scenario 3

You enter the wrong name for the Service Domain and/or Level 1 Domain.

Impact: Minor

Your can access the Standby database and edit the names.

Scenario 4

You upgrade the Signaling Server to CS 1000 Release 5.0 software, but do not convert the Succession 3.0 H.323 Gatekeeper database to an NRS database.

Impact: Minor

The existing Succession 3.0 H.323 Gatekeeper database is not responding. The user interface is also upgraded from the old H.323 Gatekeeper web pages (in Succession 3.0) to the new NRS interface (in CS 1000 Release 5.0). Therefore, if you try to access the active database through the H.323 Gatekeeper interface, you can not see the active database because the interface no longer exists. Also, if you try to use the NRS interface to access the active database, you can read no data because the database is not converted.

Scenario 5

You do not enter the Service Domain and Level 1 Domain, and proceed directly to H.323 Gatekeeper database conversion.

Impact: None

The NRS interface prevents you from converting the database if the Service Domain and Level 1 Domain names are not entered. You are informed that you missed steps in the database conversion process.

Software upgrade from Communication Server 4.0 or 4.5

Contents

This chapter contains information on the following topics:

Introduction

Communication Server 1000 Release 5.0 (CS 1000 Release 5.0) introduces 3 new servers that can host Signaling Server functionality, in addition to the legacy Nortel ISP1100 server:

- Nortel CP PM server
- IBM X306m server
- HP DL320-G4 server

These three new servers can not run any Signaling Server software prior to CS 1000 Release 5.0, and therefore are not subject to software upgrades. The CS 1000 Release 5.0 Signaling Server software must be *installed* on these servers (see "Software installation" (page 111)). Only the legacy Nortel ISP1100 server is subject to Signaling Server software upgrades.

This chapter contains instructions for upgrading the Signaling Server software on a legacy Nortel ISP1100 server (NTDU27AA) from Communication Server 1000 Release 4.0 or Communication Server 1000 Release 4.5 to Communication Server 1000 Release 5.0.

CS 1000 Release 5.0 software requires a server to have at least 1 GB of RAM configured. Some Nortel customers may need to upgrade the RAM on their legacy Nortel ISP1100 server before upgrading the Signaling Server software to CS 1000 Release 5.0. To enable customers to configure 1 GB of RAM on their legacy Nortel ISP1100 server , a Nortel ISP1100 RAM Upgrade Kit (NTDU80CA) is available. Two NTDU80CA RAM Upgrade Kits are required to configure 1 GB of RAM on any Nortel ISP1100 server. See "Upgrade the RAM on a Nortel ISP1100 Signaling Server" (page 304) for instructions on using the NTDU80CA RAM Upgrade kit to upgrade the RAM of a Nortel ISP1100 server.

Overview

The upgrade process recognizes the existence of IP configuration data and application databases on the Signaling Server and does not impact on them during the upgrade. However, Nortel recommends that you back up the application databases prior to the upgrade as a precautionary measure. The application databases consist of the IP Phone database and the NRS database.

If you don't know whether the Signaling Server being upgraded has an NRS, use the Procedure 33 "Verifying the presence of an NRS" (page 186) procedure to make this determination.

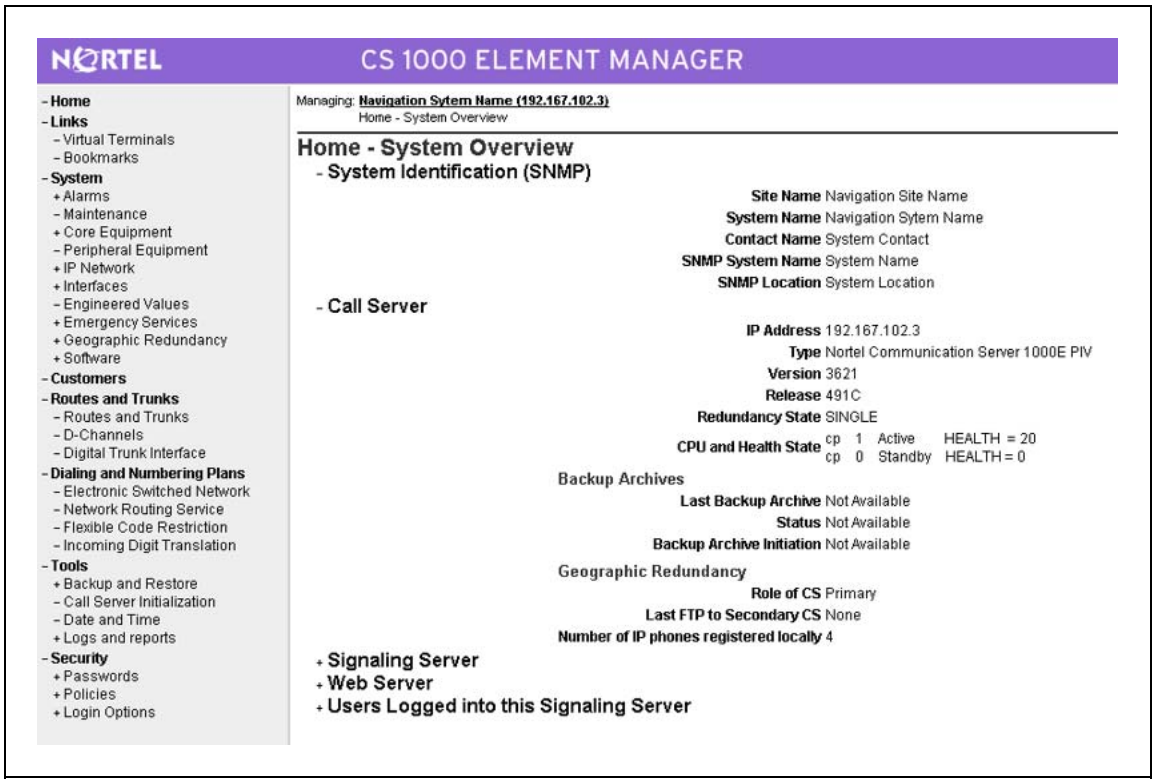
If you have an NRS database on the Signaling Server and wish to back it up prior to the upgrade, you must use the back up tool in NRS Manager. It is recommended that you download the backup file to your local PC after the back up. After the Signaling Server is upgraded, NRS Manager is used to restore the NRS database (from your local PC) and activate it for use by the NRS. For instructions on backing up and restoring an NRS database, refer to "Migrate an NRS database" (page 231).

For instructions on backing up and restoring the IP Phone database, refer to *IP Line Fundamentals (NN43001-500)* .

Procedure 33
Verifying the presence of an NRS

Step	Action
1	Log on to Element Manager on the Signaling Server (see Procedure 46 "Logging on to Element Manager" (page 243)). • The "Home - System Overview" screen appears.

Figure 158
Element manager: Home - System Overview

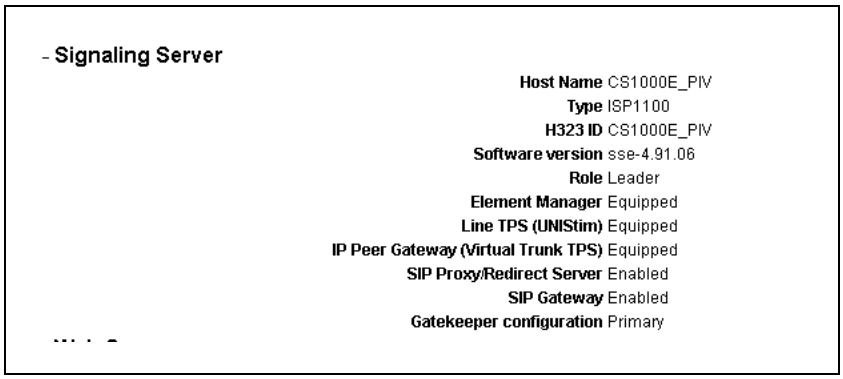


This screen identifies the components of your CS 1000 system.

2 Click the **+** symbol in front of the Signaling Server component.

The Signaling Server component expands to display the properties of the Signaling Server.

Figure 159
Signaling Server properties



3 View the contents of the "Gatekeeper configuration" property.

Figure 160
Gatekeeper configuration property

If the Gatekeeper configuration property indicates Primary (as is the case here), Alternate or Failsafe, the Signaling Server hosts an NRS. If the property indicates nothing, the Signaling Server does not host an NRS.

—End—

Before you begin

Before upgrading the software, you must do the following:

- Connect the Signaling Server — see Procedure 13 "Connecting a Nortel ISP1100 server" (page 94)
- Take a precautionary backup of the IP Phones application database — see *IP Line Fundamentals (NN43001-500)* for instructions
- Take a precautionary backup of the NRS database.
- Obtain the CS 1000 Release 5.0 version of the Signaling Server Software Install CD-ROM — see "Signaling Server Software" (page 100)
- Ensure that there is 1 GB of RAM configured on your legacy Nortel ISP1100 server. If necessary, refer to "Upgrade the RAM on a Nortel ISP1100 Signaling Server" (page 304) to upgrade the RAM before starting the upgrade procedure.

Upgrade the CS 1000 Release 4.0 or CS 1000 Release 4.5 Signaling Server

ATTENTION

IMPORTANT!
The Signaling Server is out-of-service during software upgrade.

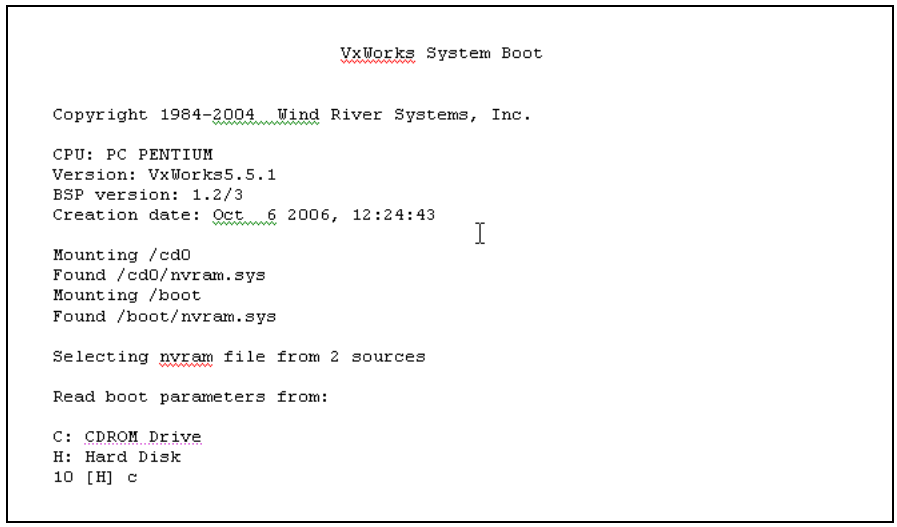
Use the following procedure to upgrade the Signaling Server software on a legacy Nortel ISP1100 server.

Procedure 34
Upgrading the Signaling Server software

Step	Action
1	Insert the Signaling Server Software CD into the CD drive, and press the **RST** button on the front panel to cold boot the Signaling Server.

The VxWorks™ system boot screen appears.

Figure 161
VxWorks system boot

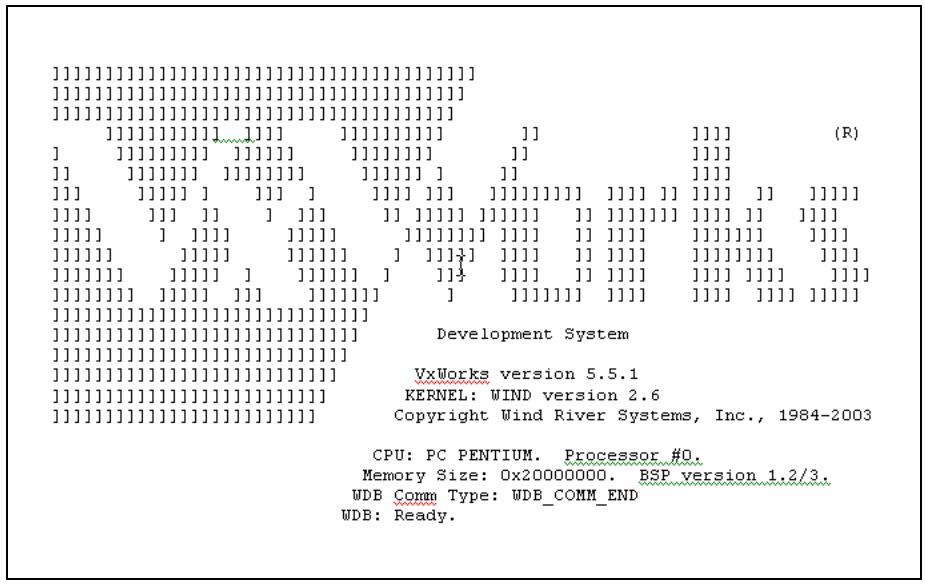


2 Enter **c** at the prompt to force the Signaling Server to boot from the Signaling Server Software CD.

Note: Enter **c** within ten seconds to ensure that the Signaling Server boots from the CD drive.

The VxWorks™ banner screen appears.

Figure 162
VxWorks banner

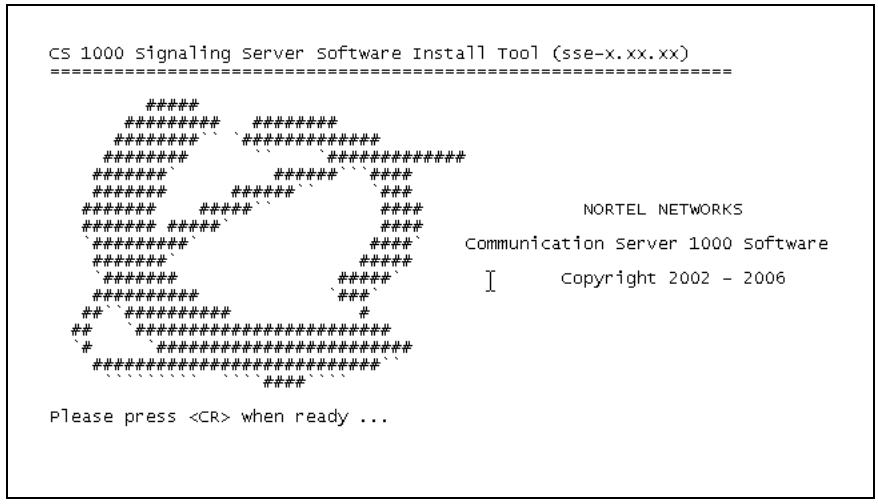


The following system messages appear:

```
/boot/ - Volume is OK
/p/ - Volume is OK
/u/ - Volume is OK
/e/ - Volume is OK
Loading /cd0/load/inst.out
```

The Signaling Server Software Installation Tool banner screen appears.

Figure 163
Installation Tool banner



3 Press**<CR>** to perform system checks and begin software installation.

The system verifies the file systems.

The following messages appear:

```
Verifying filesystems ...
Filesystems verification succeeded.

Copying "/cd0/disk.sys" to "/u/disk.sys".
```

The System Information screen appears.

Figure 164
System information

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

            ------------------------------------------
                        SYSTEM INFORMATION
            ------------------------------------------

+================================================================+
|  Hostname: CS1000E_PIV              S/W Ver: 4.50.88           |
|  Location: N/A                                                 |
|                                                                |
|      Role: Leader                    Set TPS: Enabled          |
|   Node ID: 9                        Vtrk TPS: Enabled          |
|   Node IP: 192.167.103.3           MRS Config: Primary GK + SIP|
|  H.323 ID: CS1000E_PIV                CS IP: 192.167.102.3     |
|                                                                |
|   ELAN IP: 192.167.102.4             TLAN IP: 192.167.103.2    |
|   ELAN SM: 255.255.255.0             TLAN SM: 255.255.255.0    |
|   ELAN GW: 192.167.102.1             TLAN GW: 192.167.103.1    |
|  ELAN MAC: 00:02:b3:ee:28:be        TLAN MAC: 00:02:b3:ee:28:bf|
+================================================================+

        Please enter:
<CR> -> <a> - Continue with Install Tool.
        <q> - Quit.

        Enter Choice>
```

4 Do one of the following:

- If you want to quit the upgrade and restore the previous release of software, enter **q** at the prompt. The Installation Tool Main Menu appears.

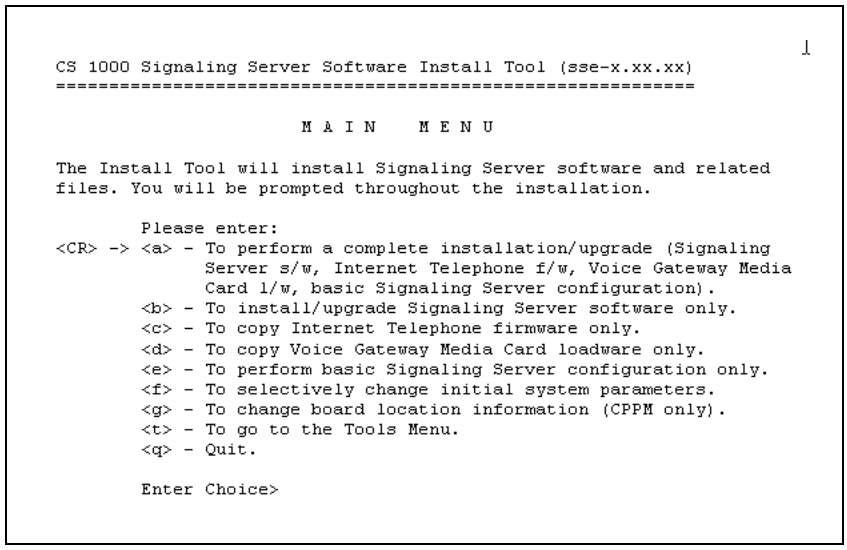
  Figure 165
  Installation Tool Main Menu

  ```
  CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
  ============================================================

                          M A I N    M E N U

  The Install Tool will install Signaling Server software and related
  files. You will be prompted throughout the installation.

          Please enter:
  <CR> -> <a> - To perform a complete installation/upgrade (Signaling
                Server s/w, Internet Telephone f/w, Voice Gateway Media
                Card l/w, basic Signaling Server configuration).
          <b> - To install/upgrade Signaling Server software only.
          <c> - To copy Internet Telephone firmware only.
          <d> - To copy Voice Gateway Media Card loadware only.
          <e> - To perform basic Signaling Server configuration only.
          <f> - To selectively change initial system parameters.
          <g> - To change board location information (CPPM only).
          <t> - To go to the Tools Menu.
          <q> - Quit.

          Enter Choice>
  ```

  Go to step 9.

- If you want to continue the upgrade, press **<CR>** or enter **a** at the prompt. The Installation Tool Main Menu appears.

Figure 166
Installation Tool Main Menu



5 Do one of the following:

- Enter **a** to upgrade the Signaling Server software, IP Phone firmware, and Voice Gateway Media Card loadware.

  Note: The upgrade process does not include Signaling Server configuration steps. If the Signaling Server is being upgraded, IP configuration data already exists on the server.

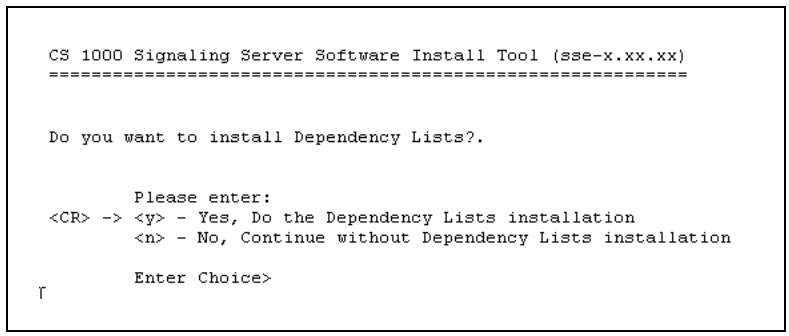
- Enter **b** to upgrade only the Signaling Server software.

  The following sample lines appear:

  ```
  Copying "/cd0/ssexxxxx.p3/disk.sys" to
  "/u/disk.sys".
  "/cd0/sse30047.p3/install.dat" parsed.

  Processing the install control file ...
  "/cd0/ssexxxxx.p3/install.dat" parsed.
  ```

Regardless of the option chosen, the Dependency list installation screen appears.

Figure 167
Dependency list installation

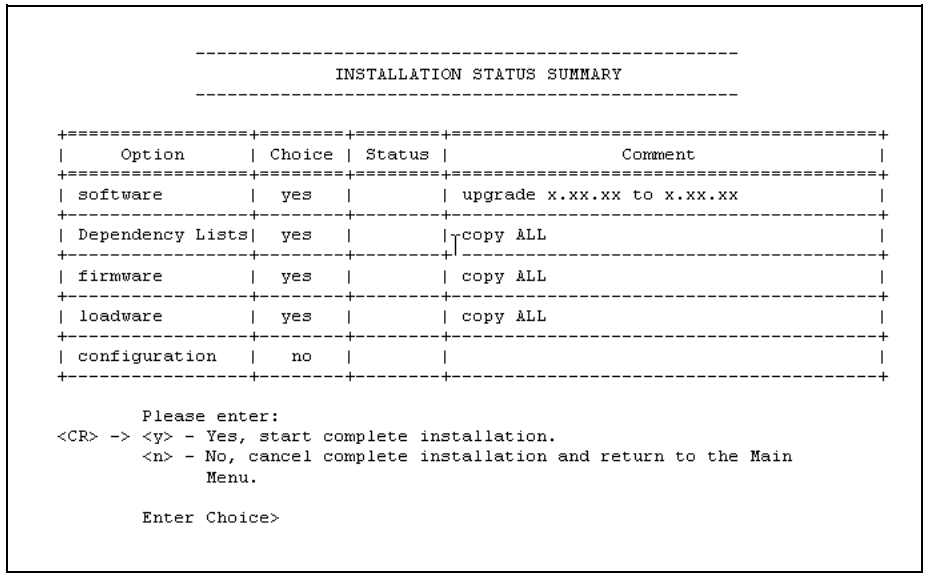


6 Do one of the following:

- Press **CR** or enter **y** to install dependency lists and continue with the upgrade.
- Enter **n** to continue the upgrade without installing the dependency lists.

Regardless of the option chosen, the Installation Status Summary screen appears.

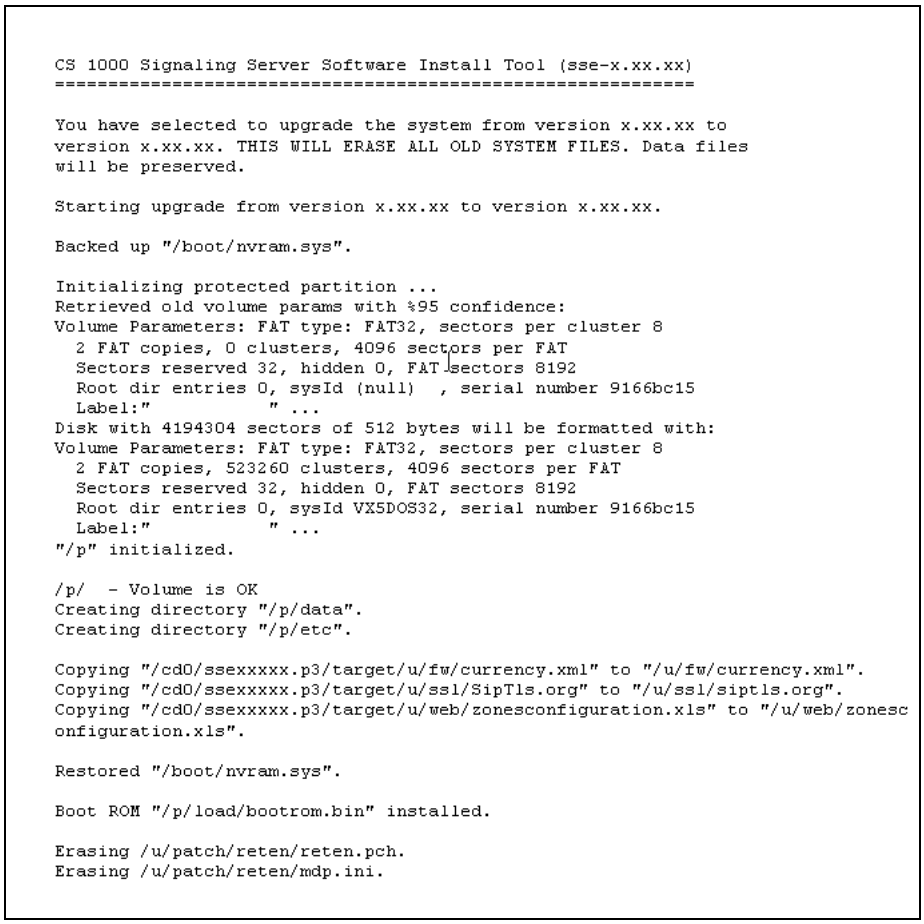
Figure 168
Installation Status Summary



7 Press **<CR>** or enter **y** to start the upgrade.

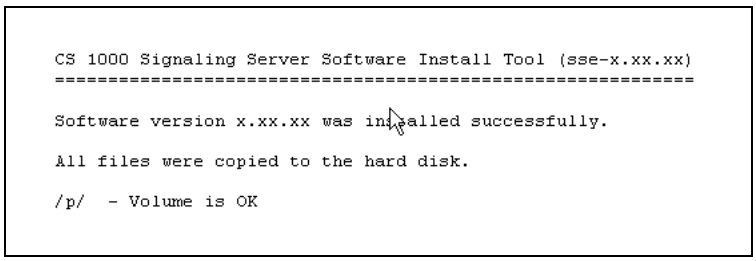
The following screens and messages appear in succession.

Figure 169
Software upgrade start



```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

You have selected to upgrade the system from version x.xx.xx to
version x.xx.xx. THIS WILL ERASE ALL OLD SYSTEM FILES. Data files
will be preserved.

Starting upgrade from version x.xx.xx to version x.xx.xx.

Backed up "/boot/nvram.sys".

Initializing protected partition ...
Retrieved old volume params with %95 confidence:
Volume Parameters: FAT type: FAT32, sectors per cluster 8
  2 FAT copies, 0 clusters, 4096 sectors per FAT
  Sectors reserved 32, hidden 0, FAT sectors 8192
  Root dir entries 0, sysId (null)   , serial number 9166bc15
  Label:"           " ...
Disk with 4194304 sectors of 512 bytes will be formatted with:
Volume Parameters: FAT type: FAT32, sectors per cluster 8
  2 FAT copies, 523260 clusters, 4096 sectors per FAT
  Sectors reserved 32, hidden 0, FAT sectors 8192
  Root dir entries 0, sysId VX5DOS32, serial number 9166bc15
  Label:"           " ...
"/p" initialized.

/p/  - Volume is OK
Creating directory "/p/data".
Creating directory "/p/etc".

Copying "/cd0/ssexxxxx.p3/target/u/fw/currency.xml" to "/u/fw/currency.xml".
Copying "/cd0/ssexxxxx.p3/target/u/ssl/SipTls.org" to "/u/ssl/siptls.org".
Copying "/cd0/ssexxxxx.p3/target/u/web/zonesconfiguration.xls" to "/u/web/zonesc
onfiguration.xls".

Restored "/boot/nvram.sys".

Boot ROM "/p/load/bootrom.bin" installed.

Erasing /u/patch/reten/reten.pch.
Erasing /u/patch/reten/mdp.ini.
```

Figure 170
Software upgrade success



```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

Software version x.xx.xx was installed successfully.

All files were copied to the hard disk.

/p/  - Volume is OK
```

Figure 171
IP Phone firmware upgrade

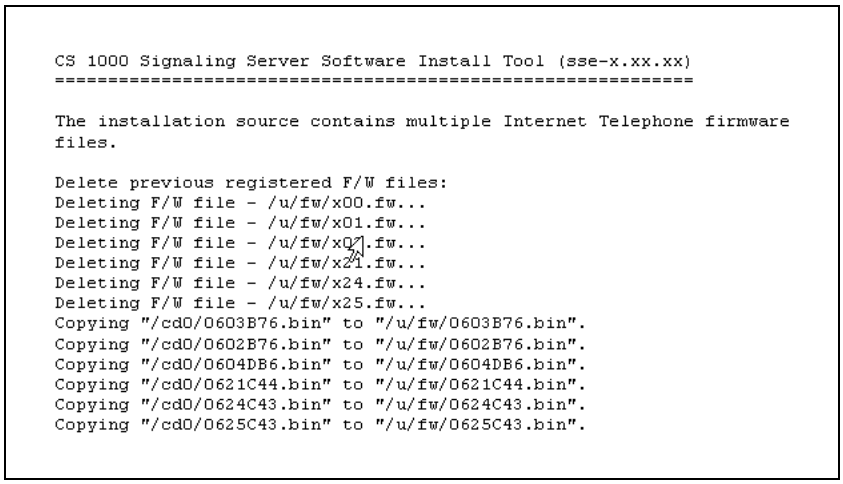


Figure 172
Voice Gateway Media Card loadware upgrade

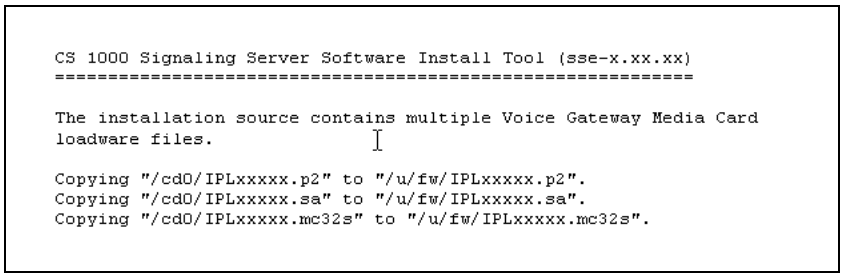


Figure 173
Retain existing IP configuration

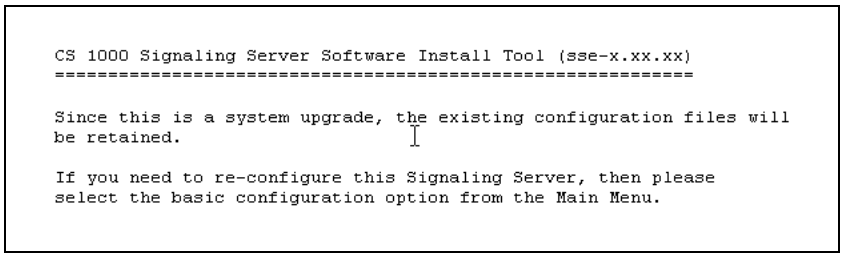
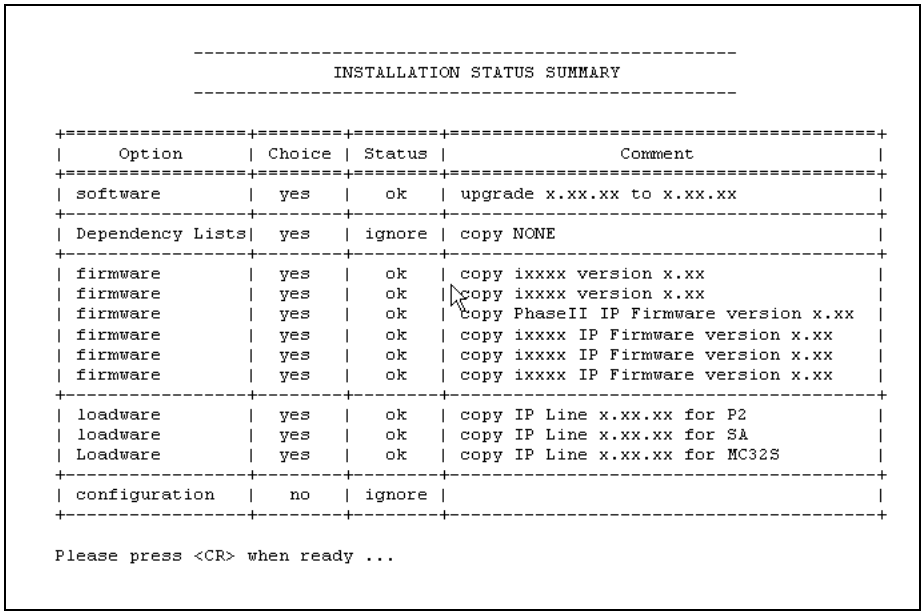


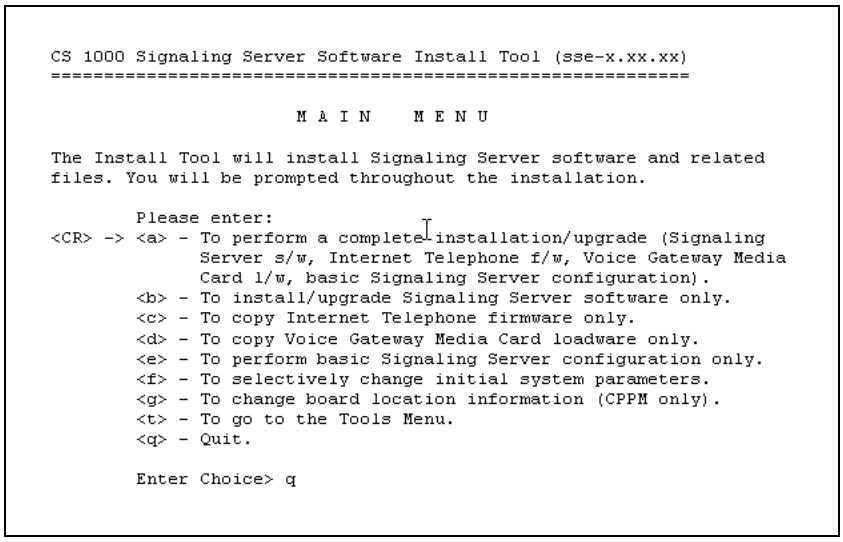
Figure 174
Installation Status Summary



```
                    ------------------------------------------------
                                INSTALLATION STATUS SUMMARY
                    ------------------------------------------------

+=================+========+========+=======================================+
|     Option      | Choice | Status |                Comment                |
+=================+========+========+=======================================+
| software        |  yes   |   ok   | upgrade x.xx.xx to x.xx.xx            |
+-----------------+--------+--------+---------------------------------------+
| Dependency Lists|  yes   | ignore | copy NONE                             |
+-----------------+--------+--------+---------------------------------------+
| firmware        |  yes   |   ok   | copy ixxxx version x.xx               |
| firmware        |  yes   |   ok   | copy ixxxx version x.xx               |
| firmware        |  yes   |   ok   | copy PhaseII IP Firmware version x.xx |
| firmware        |  yes   |   ok   | copy ixxxx IP Firmware version x.xx   |
| firmware        |  yes   |   ok   | copy ixxxx IP Firmware version x.xx   |
| firmware        |  yes   |   ok   | copy ixxxx IP Firmware version x.xx   |
+-----------------+--------+--------+---------------------------------------+
| loadware        |  yes   |   ok   | copy IP Line x.xx.xx for P2           |
| loadware        |  yes   |   ok   | copy IP Line x.xx.xx for SA           |
| Loadware        |  yes   |   ok   | copy IP Line x.xx.xx for MC32S        |
+-----------------+--------+--------+---------------------------------------+
| configuration   |   no   | ignore |                                       |
+-----------------+--------+--------+---------------------------------------+

Please press <CR> when ready ...
```

8 Press **<CR>** and the Installation Tool Main Menu screen appears.

Figure 175
Installation Tool Main Menu

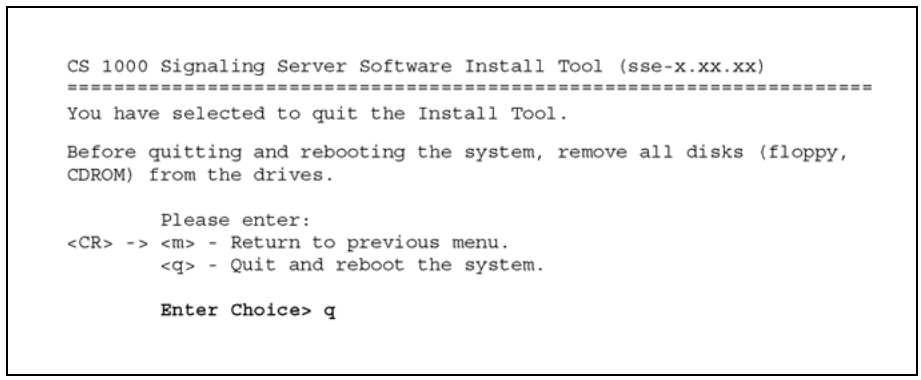


```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

                        M A I N    M E N U

The Install Tool will install Signaling Server software and related
files. You will be prompted throughout the installation.

        Please enter:
<CR> -> <a> - To perform a complete installation/upgrade (Signaling
              Server s/w, Internet Telephone f/w, Voice Gateway Media
              Card l/w, basic Signaling Server configuration).
        <b> - To install/upgrade Signaling Server software only.
        <c> - To copy Internet Telephone firmware only.
        <d> - To copy Voice Gateway Media Card loadware only.
        <e> - To perform basic Signaling Server configuration only.
        <f> - To selectively change initial system parameters.
        <g> - To change board location information (CPPM only).
        <t> - To go to the Tools Menu.
        <q> - Quit.

        Enter Choice> q
```

9 Enter **q** to exit the Installation Tool.

The Installation Tool quit confirmation screen (Figure 176 "Installation Tool quit confirmation" (page 197)) appears.

Figure 176
Installation Tool quit confirmation



10 Remove the Signaling Server Software CD from the CD drive and enter **q** to quit the Installation Tool and reboot the system.

The following system messages appear:

```
Removing temporary file "/u/disk.sys".
Rebooting system ...
```

—End—

If you are upgrading from Succession 3.0, you must reconfigure the Signaling Server to obtain and configure the NRS. If you do not reconfigure the Signaling Server, you cannot use a SIP Redirect Server. Refer to Procedure 36 "Reconfiguring the Signaling Server" (page 199) for instructions on reconfiguring a Signaling Server.

Re-install the previous software release

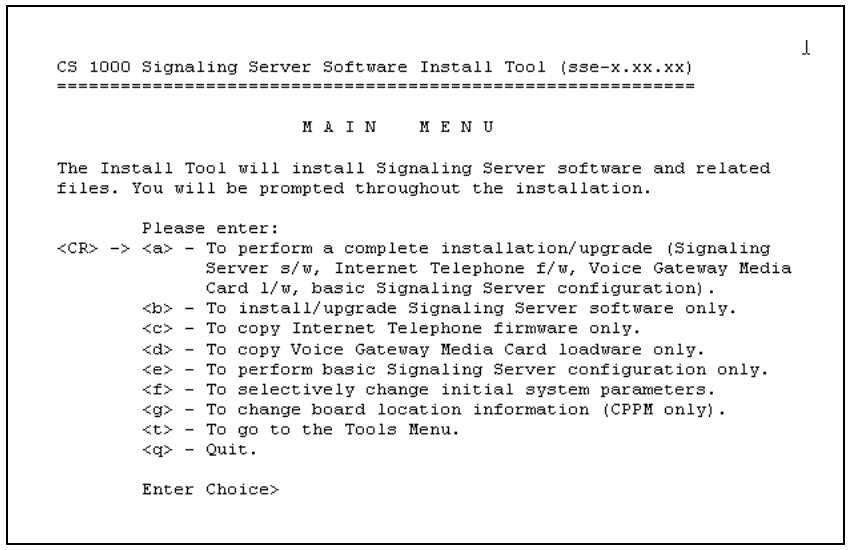
This section is only relevant to a Nortel ISP1100 Signaling Server. The Nortel CP PM, IBM X306m and HP DL320-G4 Signaling Servers only run CS 1000 Release 5.0 Signaling Server software. Earlier releases of the Signaling Server software cannot be installed on these Signaling Servers.

Use the following procedure to reinstall the previous release of software on a Nortel ISP1100 Signaling Server.

Procedure 35
Re-installing the previous software release

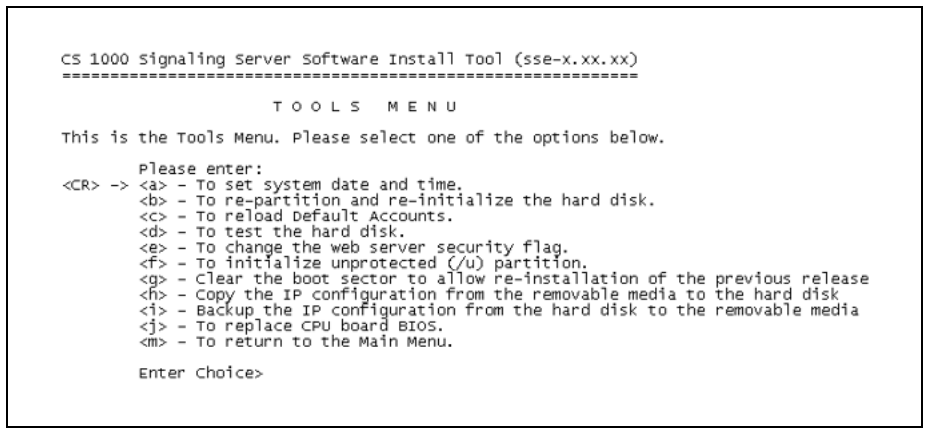
Step	Action
1	Enter **t** at the Installation Tool Main Menu screen.

Figure 177
Installation Tool Main Menu



The **Tools Menu** appears.

Figure 178
Tools Menu



2 Enter **g** to **Clear the boot sector to allow the re-installation of the previous release**.

After the boot sector is cleared, the following system messages appear:

```
The boot sector is cleared.
Insert the installation CD and restart the system.
```

3 Insert the Signaling Server Softwarel CD for the previous release, and install the software accordingly.

—End—

Signaling Server reconfiguration

Contents

This section contains information on the following topics:

Introduction

This chapter describes the procedure for reconfiguring an installed Signaling Server. The reconfiguration process consists of updating network and IP telephony data for the Signaling Server. Use the Signaling Server Software Installation Tool to reconfigure the Signaling Server.

Reconfigure the Signaling Server

Procedure 36
Reconfiguring the Signaling Server

Step	Action
1	From your Planning and Engineering group, obtain the appropriate network and IP Telephony data to reconfigure the Signaling Server: • node ID for the IP Telephony node • node IP address for the IP Telephony node • host name for the Signaling Server • ELAN network interface IP address, subnet mask, and gateway • TLAN network interface IP address, subnet mask, and gateway • ELAN network interface IP address of the Call Server • Gatekeeper role (refer to *IP Peer Networking Installation and Commissioning (NN43001-313)* for details on the Gatekeeper)

- primary and alternate Gatekeeper IP addresses for this networked system (refer to *IP Peer Networking Installation and Commissioning (NN43001-313)*)
- NRS role (refer to *Network Routing Service Installation and Commissioning NN43001-564)* for details on NRS

2 Trigger the Signaling Server Software Installation Tool on the Signaling Server.

- For IBM X306m, HP DL320-G4, and Nortel ISP1100 Signaling Servers:
  - — insert the Signaling Server Software CD into the CD drive
  - — press the **RST** button on the front of the Signaling Server or enter the **`reboot -l`** command on the CLI of the Signaling Server to trigger a cold boot. The VxWorks™ system boot banner screen appears.

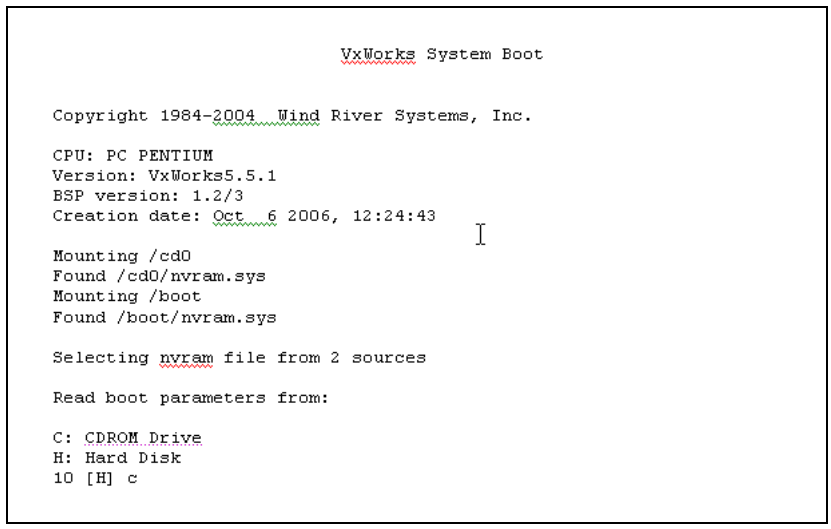
Figure 179
VxWorks system boot banner

```
                        VxWorks System Boot

Copyright 1984-2004  Wind River Systems, Inc.

CPU: PC PENTIUM
Version: VxWorks5.5.1
BSP version: 1.2/3
Creation date: Oct  6 2006, 12:24:43

Mounting /cd0
Found /cd0/nvram.sys
Mounting /boot
Found /boot/nvram.sys

Selecting nvram file from 2 sources

Read boot parameters from:

C: CDROM Drive
H: Hard Disk
10 [H] c
```

  - — enter **`c`** at the countdown prompt to trigger the Signaling Server to boot from the CD drive

- For Nortel CP PM Signaling Servers:
  - — press the **RST** button on the faceplate of the Signaling Server to trigger a cold-re-boot. The VxWorks™ boot banner screen appears.

Figure 180
VxWorks system boot banner



— enter **Ctrl+B** at the countdown prompt to stop the boot sequence

— enter **c** to change the boot parameters

— press **<CR>** until you reach the "flags" parameter

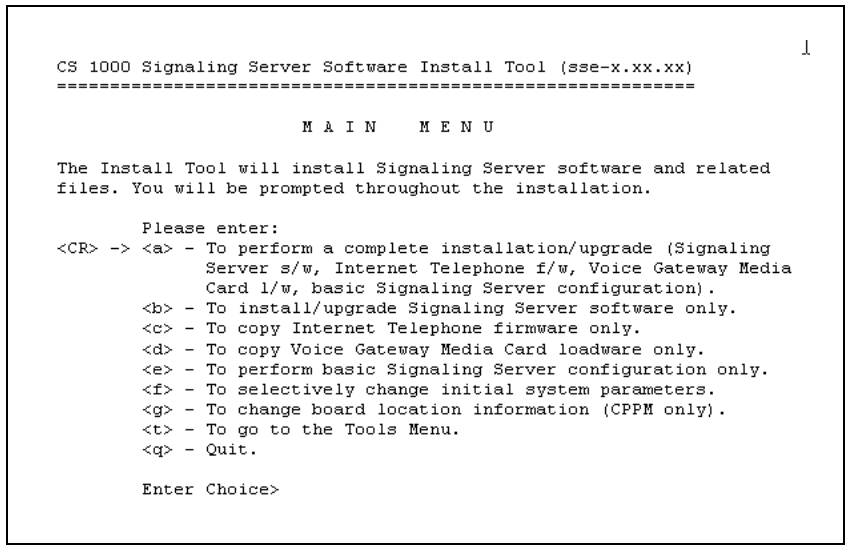
— update the contents of the "flags" parameter with the value **0x40000**

— press **<CR>** until the VxWorks™ system boot banner screen re-appears.

— enter **@** to continue the boot sequence

The Installation Tool Main Menu appears.

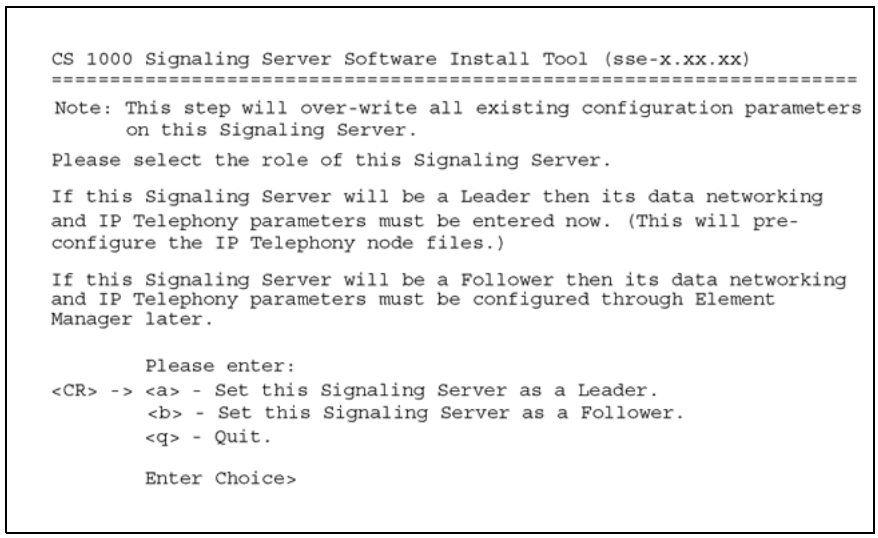
Figure 181
Installation Tool Main Menu



3 Enter **e** to reconfigure the Signaling Server.

- If an nrsconf.xml file exists already, the Leader/Follower configuration screen appears.

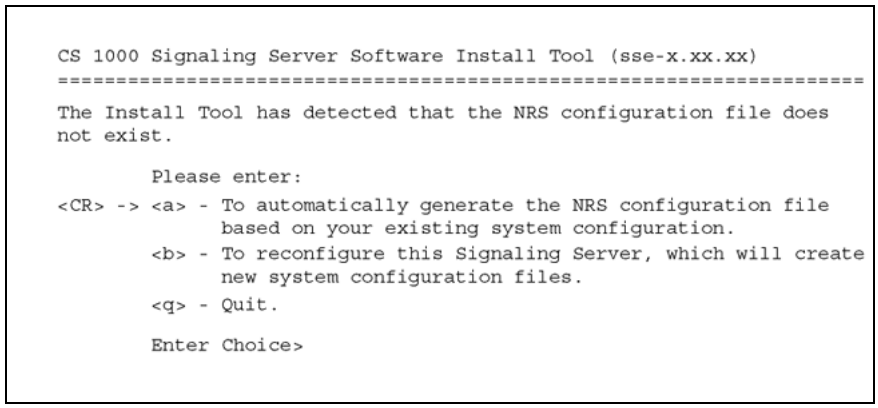
  Figure 182
  Leader/Follower configuration

  Go to step 5.

- If the nrsconf.xml file does not exist (and the nrsdflt.xml file does exist), the NRS configuration screen appears.

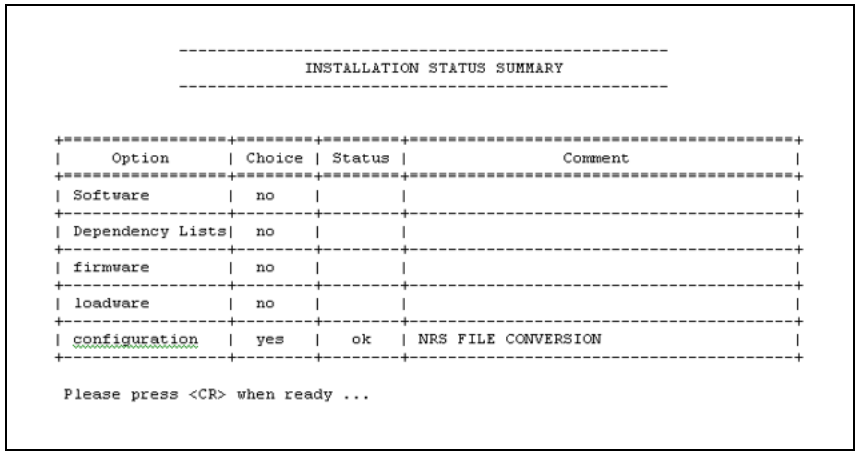
Figure 183
NRS configuration file



4 Choose the appropriate NRS configuration option.

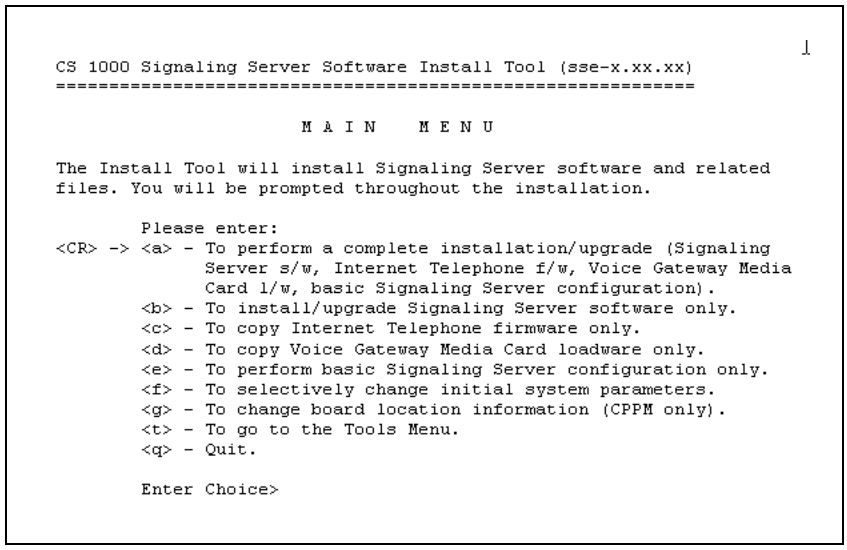
- select **a** to have the system automatically generate the NRS configuration file (nrsconf.xml) based on the existing configuration of the Signaling Server. The Installation Status Summary screen appears.

Figure 184
Installation status summary



Press **<CR>**. The Installation Tool Main Menu appears.

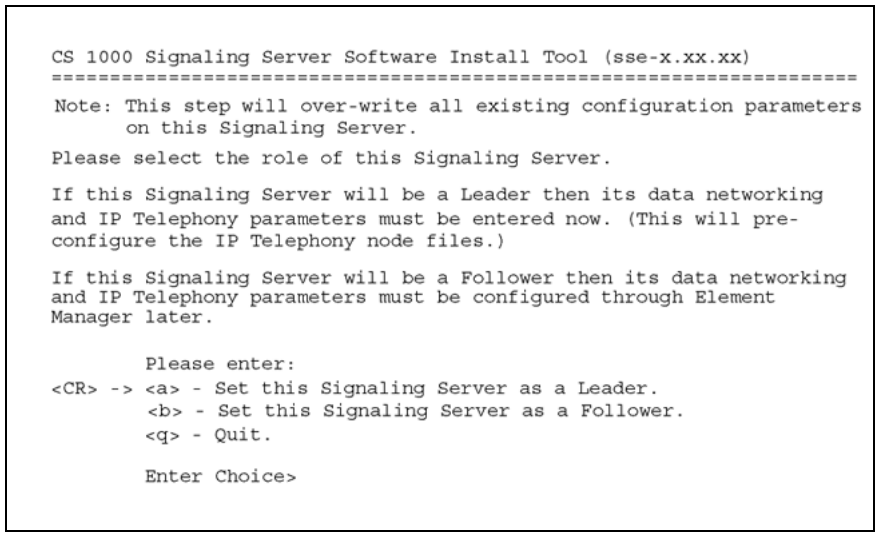
Figure 185
Installation Tool Main Menu



Go to step 13.

- Select **b** to create the new configuration file by re-configuring the Signaling Server. The Leader/Follower configuration screen appears.

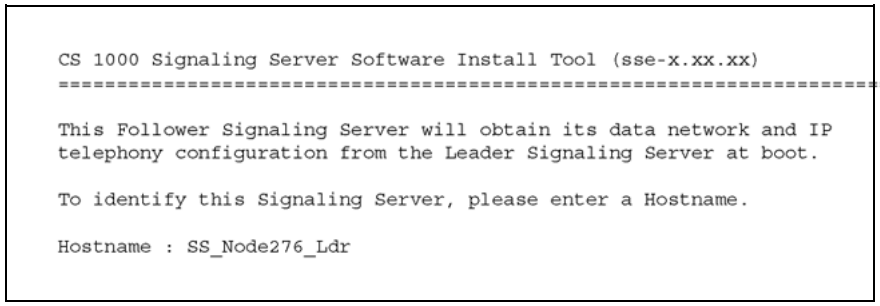
Figure 186
Leader/Follower configuration



5 Configure the Signaling Server as Leader or Follower.

- Enter **b** at the prompt to configure this Signaling Server as Follower. The Follower Signaling Server configuration screen appears.

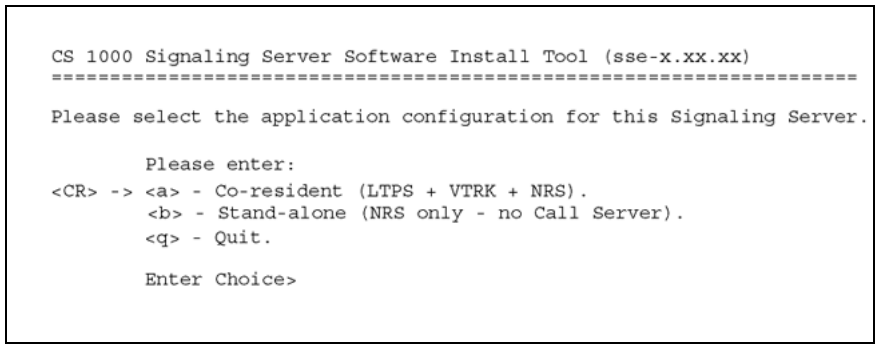
Figure 187
Follower Signaling Server configuration



Go to step 9.

- Enter **a** at the prompt to configure this Signaling Server as Leader. The Application configuration screen appears.

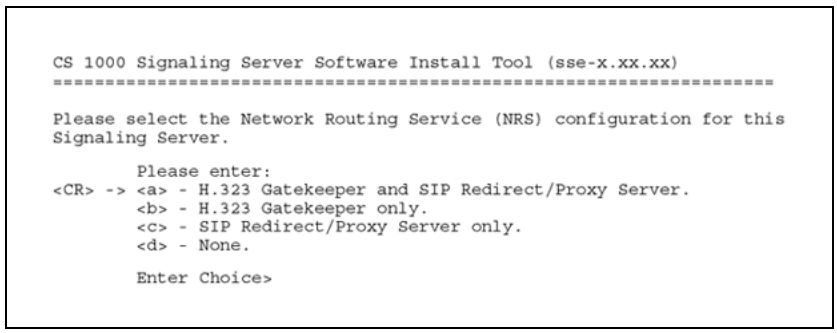
Figure 188
Application configuration



6 Select the application configuration for this Signaling Server.

- If the IP Telephone TPS, Virtual Trunk TPS, and optional Network Routing Service (NRS) applications are required on this Signaling Server, enter **a** at the prompt to configure this Signaling Server as a Coresident Signaling Server. The NRS configuration: Coresident Signaling Server screen appears.

Figure 189
NRS configuration: Coresident Signaling Server



- If only the NRS is to be enabled on this Signaling Server:
  - If this Signaling Server is to be associated with a Call Server, enter **a** at the prompt to configure this Signaling Server as a Coresident Signaling Server. The NRS configuration: Coresident Signaling Server screen appears.

Figure 190
NRS configuration: Coresident Signaling Server

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
======================================================================

Please select the Network Routing Service (NRS) configuration for this
Signaling Server.

        Please enter:
<CR> -> <a> - H.323 Gatekeeper and SIP Redirect/Proxy Server.
        <b> - H.323 Gatekeeper only.
        <c> - SIP Redirect/Proxy Server only.
        <d> - None.

        Enter Choice>
```

After you finish installing the Signaling Server software, you can disable the Line TPS and Virtual Trunk TPS in Element Manager (refer to *Element Manager: System Administration (NN43001-632)*).

  - If this Signaling Server is not to be associated with a Call Server, enter **b** at the prompt to configure this Signaling Server as a Standalone Signaling Server - NRS only. The NRS configuration: Standalone Signaling Server screen appears.

Figure 191
NRS configuration: Standalone Signaling Server

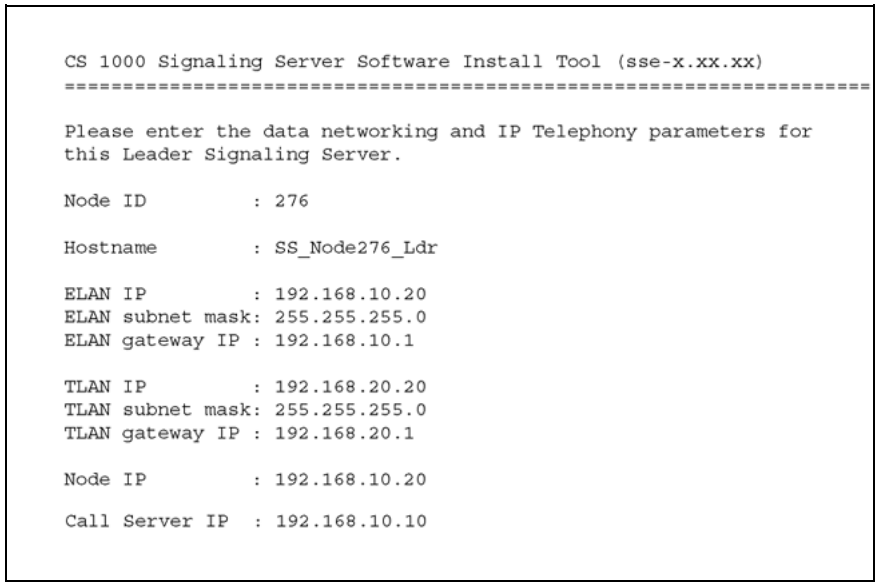
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
======================================================================

Please select the Network Routing Service (NRS) configuration for this
Signaling Server.

        Please enter:
<CR> -> <a> - H.323 Gatekeeper and SIP Redirect/Proxy Server.
        <b> - H.323 Gatekeeper only.
        <c> - SIP Redirect/Proxy Server only.

        Enter Choice>
```

7 Select the NRS configuration for the Signaling Server.

Refer to *Network Routing Service Installation and Commissioning NN43001-564)* for more information on the NRS.

- Enter **d** if this Signaling Server is configured as Leader, but is not providing an NRS. The Leader Signaling Server configuration screen appears.

Figure 192
Leader Signaling Server



Go to step 9.

- Enter **a** if this Signaling Server is to provide an H.323 Gatekeeper and a SIP Redirect/Proxy Server.
- Enter **b** if this Signaling Server is to provide only an H.323 Gatekeeper.
- Enter **c** if this Signaling Server is to provide only a SIP Redirect/Proxy Server.

Depending on the option chosen in step 6, either the "NRS type - Coresident Signaling Server" screen or the "NRS type - Standalone Signaling Server" screen appear.

Figure 193
NRS type: Coresident Signaling Server

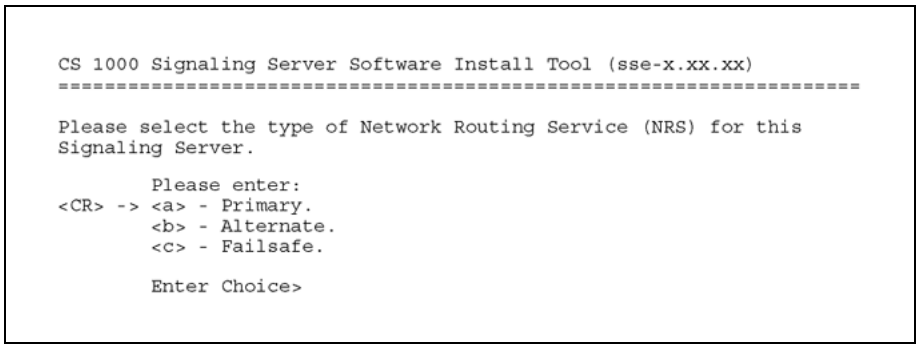
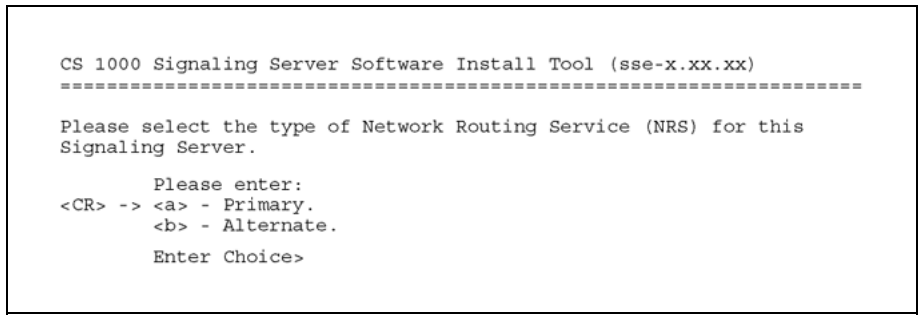


Figure 194
NRS type: Standalone Signaling Server



8 Select the type of NRS to be provided by this Signaling Server.

Refer to *Network Routing Service Installation and Commissioning NN43001-564)* for more information on the NRS.

- If this Signaling Server is to be the Primary NRS, enter **a**.
- If this Signaling Server is to be the Alternate NRS, enter **b**.
- If this Signaling Server is not a Standalone Signaling Server - NRS only and is to be the Failsafe NRS, enter **c**.

Depending on whether this Signaling Server is configured as a "Coresident" or "Standalone" Leader, either the Leader Signaling Server IP telephony screen or the Standalone IP telephony screen appears.

Figure 195
Leader Signaling Server - IP telephony parameters

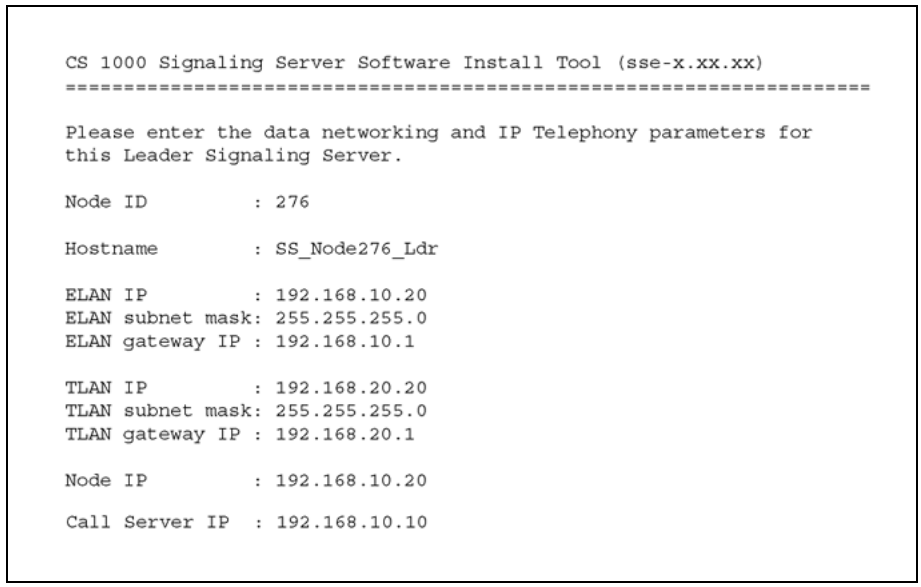


Figure 196
Standalone Signaling Server - NRS only - IP telephony parameters

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=============================================================================

Please define the data networking parameters for this Standalone
Signaling Server. Note that the ELAN parameters are necessary for
management access (e.g. SNMP).

Hostname        : SS_SA

ELAN IP         : 192.168.10.20
ELAN subnet mask: 255.255.255.0
ELAN gateway IP : 192.168.10.1

TLAN IP         : 192.168.20.20
TLAN subnet mask: 255.255.255.0
TLAN gateway IP : 192.168.20.1
```

9 Enter the data networking and IP telephony parameters for the Signaling Server.

The IP information applies to a temporary IP Telephony node. This ensures that the existing node is not impacted. This also pre-configures the IP Telephony node files. In "Importing IP Telephony nodes" (page 251), the node files are imported to Element Manager for further configuration.

- For a Follower Signaling Server, enter the host name of the Leader Signaling Server. The IP telephony parameter confirmation screen appears.

Figure 197
IP telephony parameter confirmation

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

You have entered the following parameters for this Leader SS :
(Press <a>-<l> to correct, <y> to proceed, <n> to reconfigure all.)

        Please enter:
<CR> -> <y> - Yes, these parameters are correct.
        <n> - Re-enter all of the parameters

        <a> - Node ID           : 9
        <b> - Hostname          : CS1000E_PIV
        <c> - ELAN IP           : 192.167.102.4
        <d> - ELAN subnet mask  : 255.255.255.0
        <e> - ELAN gateway IP   : 192.167.102.1
        <f> - TLAN IP           : 192.167.103.2
        <g> - TLAN subnet mask  : 255.255.255.0
        <h> - TLAN gateway IP   : 192.167.103.1
        <i> - Node IP           : 192.167.103.3
        <j> - Call Server IP    : 192.167.102.3
              NRS configuration : Primary GK + SIP
        <k> - Primary NRS IP    : 192.167.103.2
        <l> - Alternate NRS IP  :

        Enter Choice>
```

Go to step step 11.

- For a Leader Signaling Server, enter the parameters for the Node, ELAN network interface, TLAN network interface, and Call Server as required. For the Call Server:
  - If installing the Signaling Server at an office that is not a branch office, enter the ELAN network interface IP address of the Call Server.
  - If installing the Signaling Server at a branch office, enter the ELAN network interface IP address of the MG 1000B Core.
- For a Standalone Signaling Server - NRS only not associated with a Call Server (that is, **b** was selected in step 6, enter the TLAN network interface parameters as required. The Call Server IP address is automatically configured to 0.0.0.0.

Depending on the option chosen in step 7: select NRS configuration or step 8: select NRS type, either the Primary NRS IP address screen or the Alternate NRS IP address screen, or both (in succession), appear.

Figure 198
Primary NRS IP address

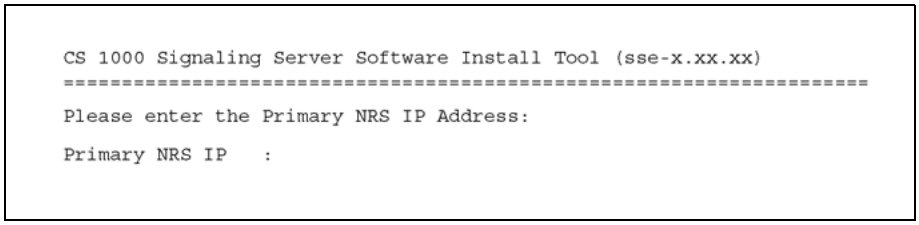
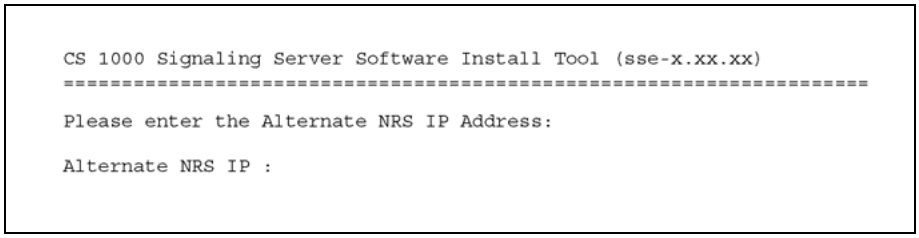


Figure 199
Alternate NRS IP address



10 Enter the Primary NRS IP address or the Alternate NRS IP address, depending on the option entered in step 7: select NRS configuration or step 8: select NRS type.

The Gatekeeper configuration can be updated later using Element Manager.

- If **a** was entered in step 8: select NRS type, you can enter the address of the Alternate NRS if you know it, but it is not required.

- If **b** was entered in step 8: select NRS type, enter the address of the Primary NRS.
- If **c** was entered in step 8: select NRS type:
  - Enter the address of the Primary NRS.
  - Enter the address of the Alternate NRS.
- If **d** was entered in step 7: select NRS configuration:
  - Enter the address of the Primary NRS (optional).
  - If you did enter the address of the Primary NRS, enter the address of the Alternate NRS (also optional).

The IP telephony parameter confirmation screen appears.

Figure 200
IP telephony parameter confirmation

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

You have entered the following parameters for this Leader SS :
(Press <a>-<l> to correct, <y> to proceed, <n> to reconfigure all.)

        Please enter:
<CR> -> <y> - Yes, these parameters are correct.
        <n> - Re-enter all of the parameters

        <a> - Node ID           : 9
        <b> - Hostname          : CS1000E_PIV
        <c> - ELAN IP           : 192.167.102.4
        <d> - ELAN subnet mask  : 255.255.255.0
        <e> - ELAN gateway IP   : 192.167.102.1
        <f> - TLAN IP           : 192.167.103.2
        <g> - TLAN subnet mask  : 255.255.255.0
        <h> - TLAN gateway IP   : 192.167.103.1
        <i> - Node IP           : 192.167.103.3
        <j> - Call Server IP    : 192.167.102.3
              NRS configuration : Primary GK + SIP
        <k> - Primary NRS IP    : 192.167.103.2
        <l> - Alternate NRS IP  :

        Enter Choice>
```

11 Press]**<CR>** or enter **y** to confirm all parameters entered, or enter the letter preceding any parameter to change its value.

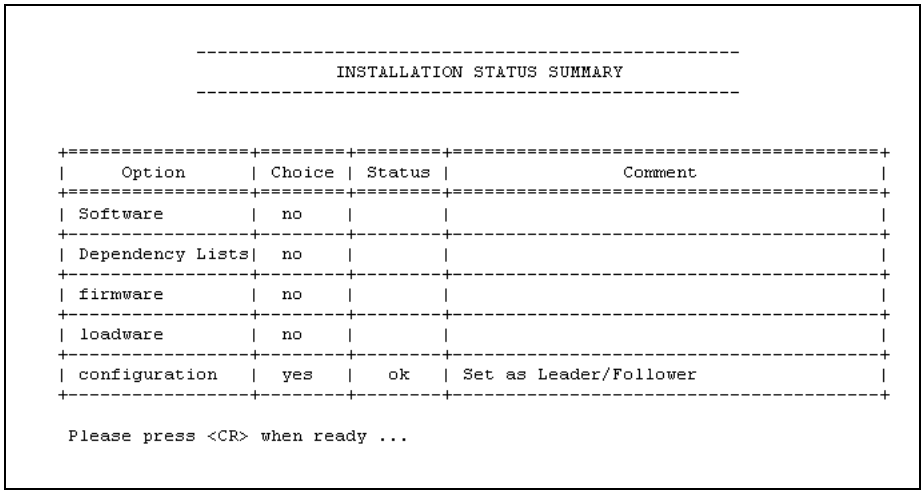
The example in Figure 200 "IP telephony parameter confirmation" (page 211)is for a Leader Signaling Server configured with an Alternate H.323 and SIP NRS. The confirmation screens for a Follower and Standalone Signaling Server - NRS only are similar, showing the same list of parameters, specifically:

- The configuration screen for a Follower Signaling Server only contains a value for the host name parameter; all other values are blank.

- The configuration screen for a Standalone Signaling Server - NRS only contains values for the host name, ELAN network interface, TLAN network interface, and NRS parameters. The Node ID parameter is configured to 0. The Call Server IP parameter is configured to 0.0.0.0.

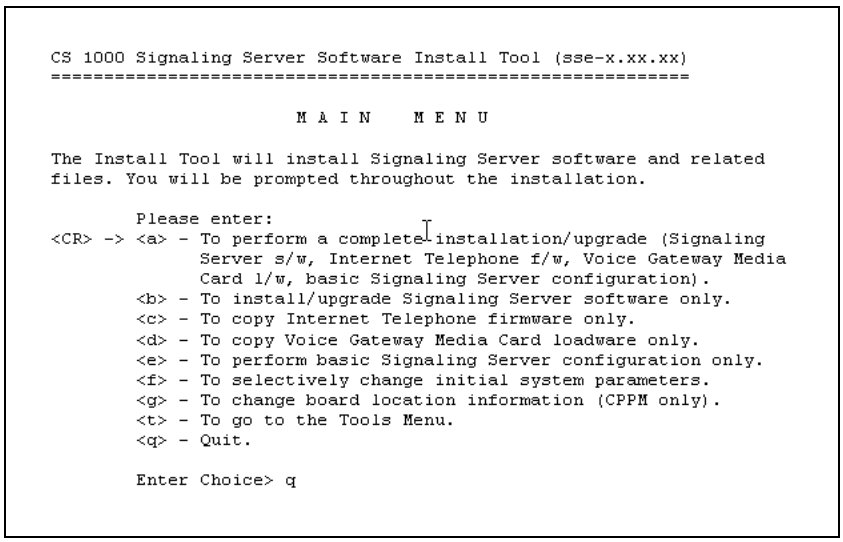
After the IP telephony parameters are confirmed, the Installation Status Summary screen appears.

Figure 201
Installation Status Summary



12 Press **<CR>** to return to the Installation Tool Main Menu.

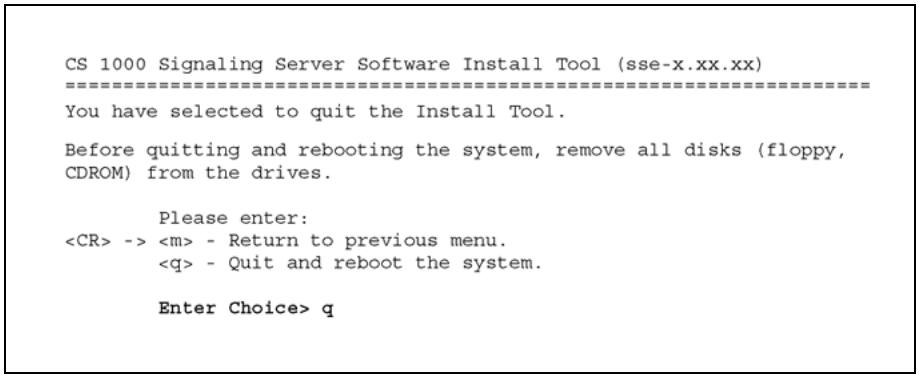
Figure 202
Installation Tool Main Menu



13 Enter **q** to quit the Installation Tool.

The Installation Tool quit confirmation screen appears.

Figure 203
Installation Tool quit confirmation



14 Remove the Signaling Server Software CD-ROM from the CD-ROM drive of your IBM X306m, HP DL320-G4 or Nortel ISP1100 Signaling Server, and enter **q** to Quit the Installation Tool and reboot the system.

—End—

Signaling Server migration

Contents

This chapter contains information on the following topics:

Introduction

CS 1000 Release 5.0 introduces three new Signaling Servers:

- Nortel CP PM Signaling Server
- IBM X306m Signaling Server
- HP DL320-G4 Signaling Server

This chapter describes the processes for migrating your legacy Nortel ISP1100 Signaling Server to any of the three new CS 1000 Release 5.0 Signaling Servers.

Overview

ATTENTION

IMPORTANT!
This migration process assumes that the connected Call Server has already been upgraded to CS 1000 Release 5.0.

The process for migrating your legacy Nortel ISP1100 Signaling Server (source) to any of the three new CS 1000 Release 5.0 Signaling Servers (target) is dependent on the version of Signaling Server software currently running on your legacy Nortel ISP1100 Signaling Server:

- Succession 1000 Release 3.0

- Communication Server 1000 Release 4.0
- Communication Server 1000 Release 4.5

In Succession 3.0, the Signaling Server only supported H.323 signaling. The Signaling Server maintained an H.323 Gatekeeper database to support the requirements of the H.323 signaling protocol. Session Initiation Protocol (SIP) signaling was introduced in CS 1000 Release 4.0, along with Network Routing Service (NRS) to support the requirements of both H.323 and SIP signaling protocols. NRS uses an NRS database to support these signaling requirements.

When migrating your Signaling Server from a Nortel ISP1100 server running Succession 1000 Release 3.0 to a server running CS 1000 Release 5.0 (Nortel CP PM, IBM X306m, HP DL320-G4), the Succession 3.0 H.323 Gatekeeper database must be converted to an NRS database using a conversion tool during the migration process. When migrating your Signaling Server from a Nortel ISP1100 server running CS 1000 Release 4.0 or CS 1000 Release 4.5, the structural changes to the NRS database are implemented automatically when the database is restored to the target server during the migration process.

The migration process consists of the migration of the IP Phones Application database (if applicable), the conversion and migration of the H.323 Gatekeeper database (if applicable), and the migration of the Network Routing Service (NRS) database (if applicable) from the source Signaling Server to the target Signaling Server. It also includes the installation of CS 1000 Release 5.0 Signaling Server software on the target Signaling Server and the exchange of IP telephony node data with the Call Server.

The migration process does not include the migration of base IP configuration data. You can not back up the base IP configuration data from the source Signaling Server and restore it on the target Signaling Server when migrating your legacy Nortel ISP1100 Signaling Server to one of the three new CS 1000 Release 5.0 Signaling Server platforms. You must take note of the base IP configuration data for the source Signaling Server prior to its physical removal from the system. You must then enter this IP configuration data on the target Signaling Server during the Signaling Server software installation step of the migration process.

The purpose of the migration process is to have the target Signaling Server assume the role of the source Signaling Server in the CS 1000 system.

ATTENTION

IMPORTANT!

You can not back up the IP configuration data from the source Signaling Server and restore it on the target Signaling Server when migrating your legacy Nortel ISP1100 Signaling Server to one of the three new CS 1000 Release 5.0 Signaling Server platforms. IP configuration data (from the source Signaling Server) must be entered during the Signaling Server software installation step for the target Signaling Server.

WARNING

Before starting the Signaling Server migration process, the IP telephony node database files on the source Signaling Server must be backed up (refer to "IP Telephony node configuration procedures" (page 250)).

Migrate a Succession 3.0 Signaling Server

Use the following procedure to migrate your Succession 3.0 Nortel ISP1100 Signaling Server (source) to any of the three new CS 1000 Release 5.0 Signaling Servers (target).

Procedure 37
Migrating a Succession 3.0 Signaling Server

Step	Action
1	Log on to Element Manager (EM) on the source Signaling Server.
2	Back up the Succession 3.0 H.323 Gatekeeper database (if applicable). For instructions, see "Back up the Succession 3.0 H.323 Gatekeeper database" (page 163).
3	Back up the IP Phone Application Server database (if applicable). See *IP Line Fundamentals (NN43001-500)* for instructions.
4	Take note of the following IP Telephony and data networking data: • node ID for the IP Telephony node • node IP address for the IP Telephony node • host name for the Signaling Server • ELAN network interface IP address, Subnet mask, and Gateway • TLAN network interface IP address, Subnet mask, and Gateway • ELAN network interface IP address of the Call Server

-
- H.323 Gatekeeper role, if applicable (see *IP Peer Networking Installation and Commissioning (NN43001-313)*)

5 Obtain the Primary and Alternate NRS IP addresses for your networked CS 1000 Release 5.0 system from your Planning and Engineering group (see *IP Peer Networking Installation and Commissioning (NN43001-313)*)

6 Log off of EM on the source Signaling Server.

7 Remove the source Signaling Server from the system.

a. Turn off the power.

b. Disconnect all cables from the unit, including the power cord.

Note: Add labels to the cables so that they can be easily and properly reinstalled.

c. Loosen the screws through the faceplate of the Signaling Server to the rack-mount bracket and slide the unit out of the rack.

8 Install the target Signaling Server hardware (see "Hardware installation and connection" (page 59) for instructions.

9 Do one of the following:

- If the source Signaling Server is a Leader:
  - — if you are migrating to an IBM X306m or HP DL320-G4 Signaling Server, install CS 1000 Release 5.0 software on the target Signaling Server and configure the Signaling Server with the IP Telephony and data networking data that you collected from the source Signaling Server and your Planning and Engineering group (see "Software installation" (page 111) for instructions.
  - — if you are migrating to a Nortel CP PM Signaling Server (CS 1000 Release 5.0 Signaling Server software is preloaded), configure the Signaling Server with the IP Telephony and data networking data that you collected from the source Signaling Server and your Planning and Engineering group (see Procedure 20 "Entering basic system configuration parameters" (page 131) for instructions.
- If the source Signaling Server is a Follower, proceed to next step.

10 Transfer IP telephony node information to the target Signaling Server.

- If migrating a Leader Signaling Server, see Procedure 39 "Migrating a Leader Signaling Server" (page 222) for instructions.
- If migrating a Follower Signaling Server, see Procedure 40 "Migrating a Follower Signaling Server" (page 225) for instructions.

11 Log on to EM on the target Signaling Server.

Note: This step is only necessary if the source Signaling Server hosted an IP Phones Application Server.

If the source Signaling Server did not host an IP Phones Application server, go to step 14.

12 Restore the IP Phone Application database.

For instructions, see *IP Line Fundamentals (NN43001-500)*.

13 Log off of EM on the target Signaling Server.

14 Log on to the Network Routing Service (NRS) Manager on the target Signaling Server.

Note: This step is only necessary if the source Signaling Server hosted an H.323 Gatekeeper.

If the source Signaling Server did not host an H.323 Gatekeeper, go to step 17.

15 Convert the H.323 Gatekeeper database to an NRS database.

For instructions, see "Convert the Succession 3.0 H.323 Gatekeeper database to a CS 1000 Release 5.0 NRS database" (page 169).

16 Log off of NRS Manager.

17 Re-boot the new Signaling Server for the changes to take effect.

- For a Nortel CP PM Signaling Server, press the **INI** button on the faceplate to warm-reboot the Signaling Server.
- For an IBM X306m or HP DL320-G4 Signaling Server, press the **RST** button to cold-reboot the Signaling Server.

—End—

Migrate a CS 1000 Release 4.0 or 4.5 Signaling Server

Use the following procedure to migrate your CS 1000 Release 4.0 or CS 1000 Release 4.5 Signaling Server (source) to any of the three new CS 1000 Release 5.0 Signaling Servers (target).

Procedure 38
Migrating a CS 1000 Release 4.0 or 4.5 Signaling Server

Step	Action
1	Log on to Element Manager (EM) on the source Signaling Server.
2	Back up the IP Phone Application database (if applicable). See *IP Line Fundamentals (NN43001-500)* for instructions.
3	Take note of the following IP Telephony and data networking data for the source Signaling Server: • node ID for the IP Telephony node • node IP address for the IP Telephony node • host name for the Signaling Server • ELAN network interface IP address, Subnet mask, and Gateway • TLAN network interface IP address, Subnet mask, and Gateway • ELAN network interface IP address of the Call Server • Primary and Alternate NRS IP addresses for this networked system (see *IP Peer Networking Installation and Commissioning (NN43001-313)*) • NRS role, if applicable (see *IP Peer Networking Installation and Commissioning (NN43001-313)*)
4	Log off of EM on the source Signaling Server.
5	Log on to the Network Routing Service (NRS) Manager on the source Signaling Server. ***Note:*** This step is only necessary if the source Signaling Server hosts an NRS. If the source Signaling Server does not host an NRS, go to STEP 8.
6	Back up the NRS database. For instructions, see Procedure 42 "Backing up the NRS database" (page 231).
7	Log off of NRS Manager on the source Signaling Server.

8 Remove the source Signaling Server from the system.

a. Turn off the power.

b. Disconnect all cables from the unit, including the power cord.

Note: Add labels to the cables so that they can be easily and properly reinstalled.

c. Loosen the screws through the faceplate of the Signaling Server to the rack-mount bracket and slide the unit out of the rack.

9 Install the target Signaling Server hardware (see "Hardware installation and connection" (page 59) for instructions.

10 Do one of the following:

- If the source Signaling Server is a Leader:
  - — if you are migrating to an IBM X306m or HP DL320-G4 Signaling Server, install CS 1000 Release 5.0 software on the target Signaling Server and configure the Signaling Server with the IP Telephony and data networking data that you collected from the source Signaling Server (see "Software installation" (page 111) for instructions.
  - — if you are migrating to a Nortel CP PM Signaling Server (CS 1000 Release 5.0 Signaling Server software is preloaded), configure the Signaling Server with the IP Telephony and data networking data that you collected from the source Signaling Server (see Procedure 20 "Entering basic system configuration parameters" (page 131) for instructions.
- If the source Signaling Server is a Follower or Standalone Signaling Server - NRS only, proceed to next step.

11 Transfer IP telephony node information to the target Signaling Server.

- If you are migrating a Leader Signaling Server, see Procedure 39 "Migrating a Leader Signaling Server" (page 222)
- If you are migrating a Follower Signaling Server, see Procedure 40 "Migrating a Follower Signaling Server" (page 225)
- If you are migrating a Standalone Signaling Server - NRS only, see Procedure 41 "Migrating a Standalone Signaling Server - NRS only with no Call Server association" (page 231)

  Go to STEP 15.

12 Log on to EM on the target Signaling Server.

Note: This step is only necessary if the source Signaling Server hosted an IP Phones Application Server.

If the source Signaling Server did not host an IP Phones Application server, go to step 15.

13 Restore the IP Phone Application database.

For instructions, see *IP Line Fundamentals (NN43001-500)*.

14 Log off of EM on the target Signaling Server.

15 Log on to NRS Manager on the target Signaling Server.

Note: This step is only necessary if the source Signaling Server hosted an NRS.

If the source Signaling Server did not host an NRS, go to step 19.

16 Restore the NRS database.

For instructions, see Procedure 43 "Restoring the NRS database" (page 235).

17 Activate the NRS database.

For instructions, see Procedure 44 "Activating the NRS database" (page 237).

18 Log off of NRS Manager.

19 Re-boot the target Signaling Server for the changes to take effect.

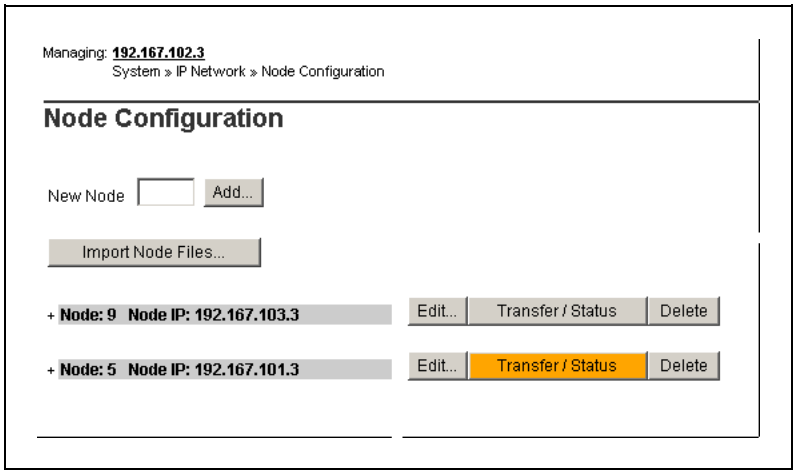
- For a Nortel CP PM Signaling Server, press the **INI** button on the faceplate to warm-reboot the Signaling Server.
- For an IBM X306m or HP DL320-G4 Signaling Server, press the **RST** button to cold-reboot the Signaling Server.

—End—

Procedure 39
Migrating a Leader Signaling Server

Step	Action
1	Log on to EM on the target Signaling Server.
2	Select **IP Network > Nodes: Servers, Media Cards** from the navigator. The **Node Configuration** web page appears.

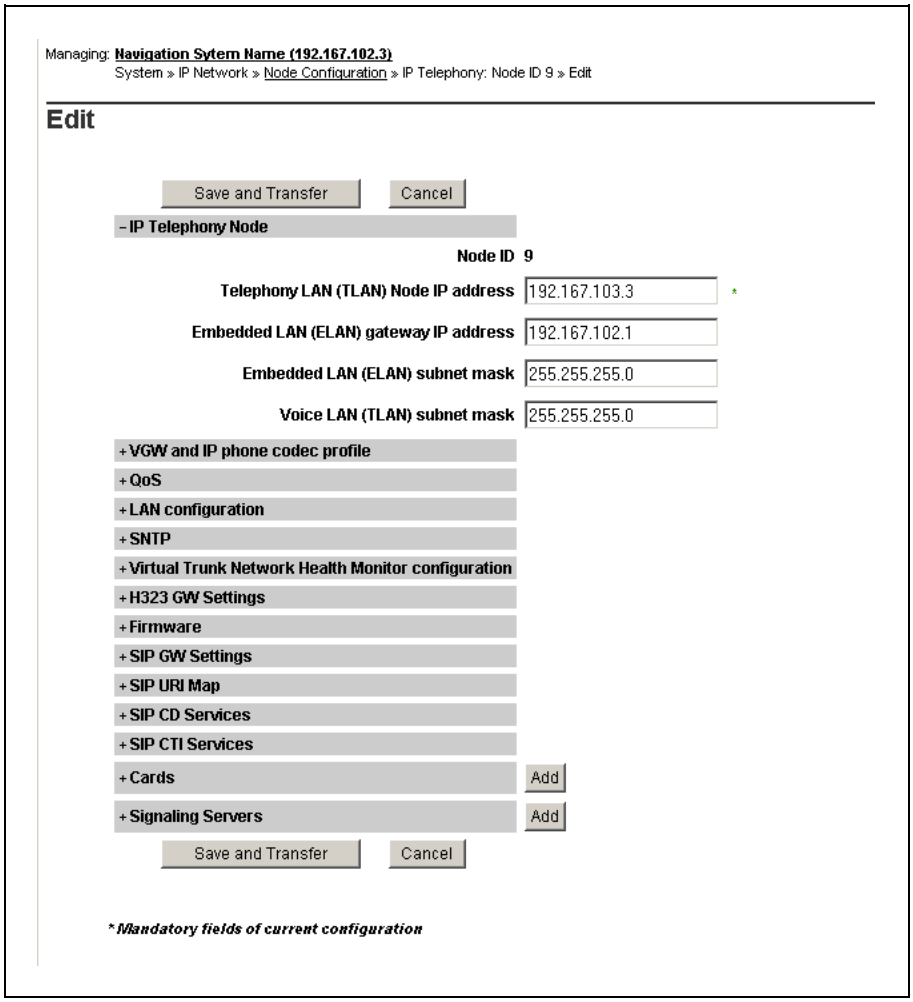
Figure 204
Node configuration



3 Click **Edit** next to the node where the Leader Signaling Server is located.

The Edit node web page appears.

Figure 205
Edit node configuration



Note: The information that is being edited is the node configuration that resides on the Call Server, not the Signaling Server.

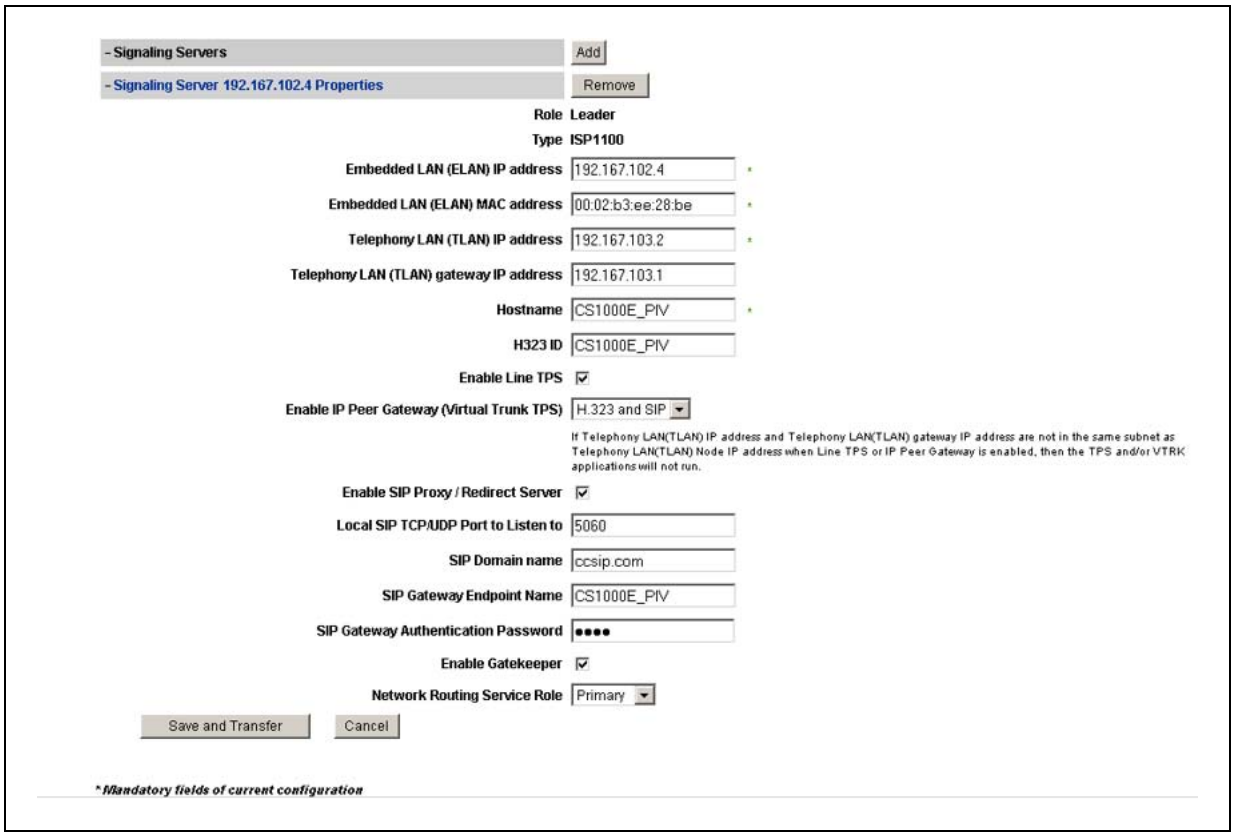
4 Click the **Signaling Servers** component.

The section expands to show a list of Signaling Servers on the node.

5 Click on the Leader Signaling Server.

The **Signaling Server xxx.xxx.xxx.xxx properties** web page appears (where xxx.xxx.xxx.xxx is the IP address of the Leader Signaling Server).

Figure 206
Signaling Server properties



6 Enter the MAC address of the target Signaling Server in the **Embedded LAN (ELAN) MAC address** entry field.

7 Click **Save and Transfer** to transfer the node information to the target Signaling Server.

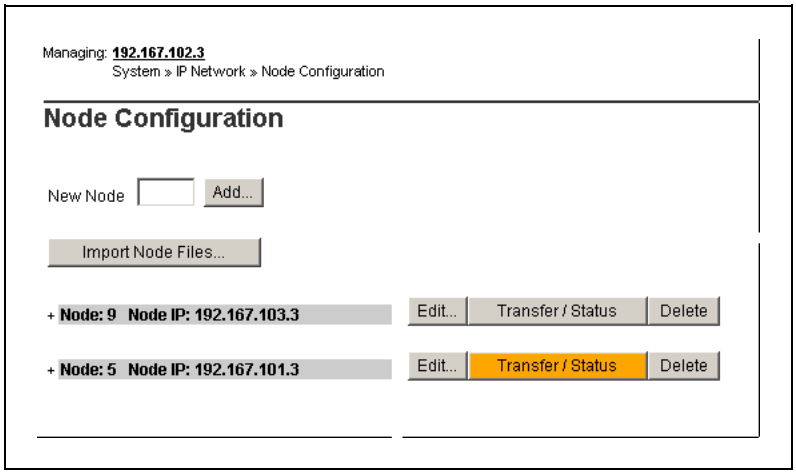
8 Re-boot the target Signaling Server

—End—

Procedure 40
Migrating a Follower Signaling Server

Step	Action
1	Log on to EM on the CS 1000 Release 5.0 Leader Signaling Server.
2	Select **IP Network > Nodes: Servers, Media Cards** from the navigator. The **Node Configuration** web page appears.

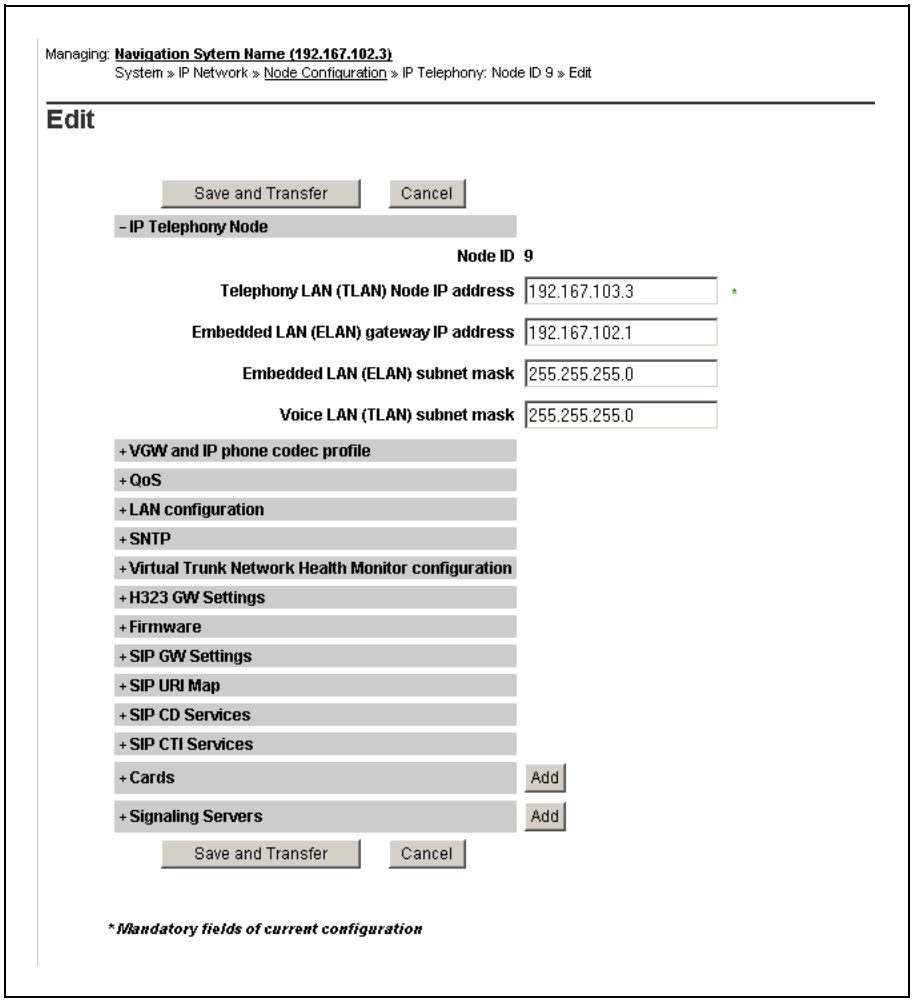
Figure 207
Node configuration



3 Click **Edit** next to the node from which you are migrating the source Signaling Server.

The Edit node web page appears.

Figure 208
Edit node configuration



Note: The information that you are editing is the node configuration that resides on the Call Server, not the Signaling Server.

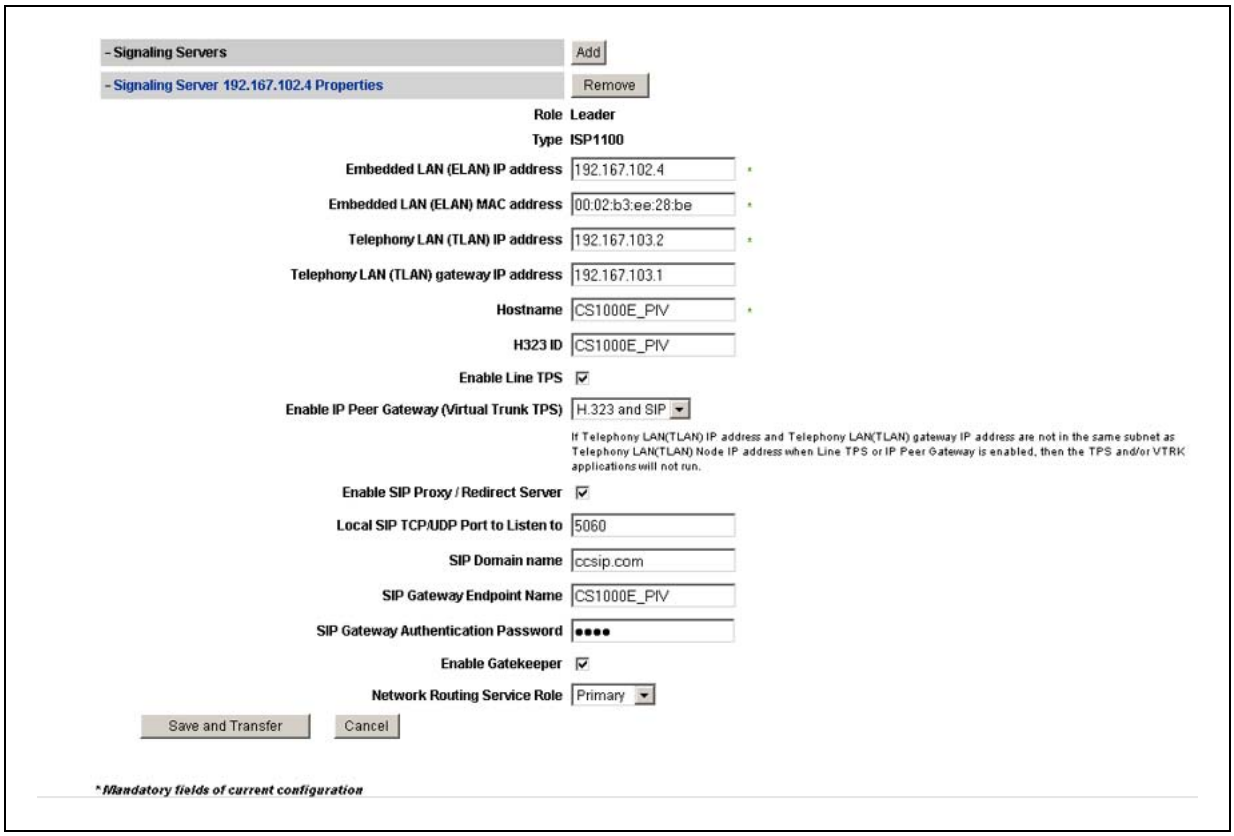
4 Click the **Signaling Servers** component.

The section expands to show you a list of Signaling Servers on this node.

5 Click on the source Signaling Server.

The **Signaling Server xxx.xxx.xxx.xxx properties** web page appears (where xxx.xxx.xxx.xxx is the IP address of the source Signaling Server).

Figure 209
Signaling Server properties



Data in the above sample is for illustrative purposes only.

6 Enter the MAC address of the target Signaling Server in the **Embedded LAN (ELAN) MAC address** entry field.

7 Click **Save and Transfer** to save the MAC address of the target Signaling Server on the Leader Signaling Server.

8 Log off of EM on the Leader Signaling Server.

9 Install CS 1000 Release 5.0 software on the target Signaling Server and configure it with the IP telephony and data networking data that you collected from the source Signaling Server.

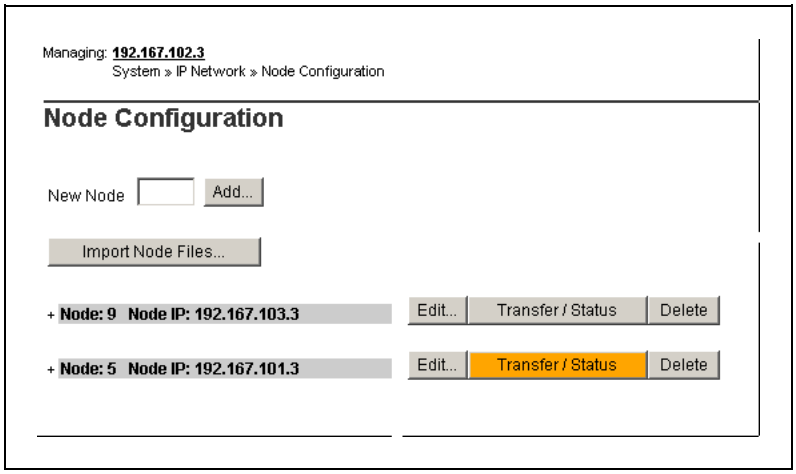
- If you are migrating to an IBM X306m or HP DL320-G4 Signaling Server, see "Software installation" (page 111)for instructions.
- If you are migrating to a Nortel CP PM Signaling Server (CS 1000 Release 5.0 Signaling Server software is preloaded), see Procedure 20 "Entering basic system configuration parameters" (page 131)for instructions.

10 Log on to EM on the target Signaling Server.

11 Select **IP Network > Nodes: Servers, Media Cards** from the navigator.

The **Node Configuration** web page appears.

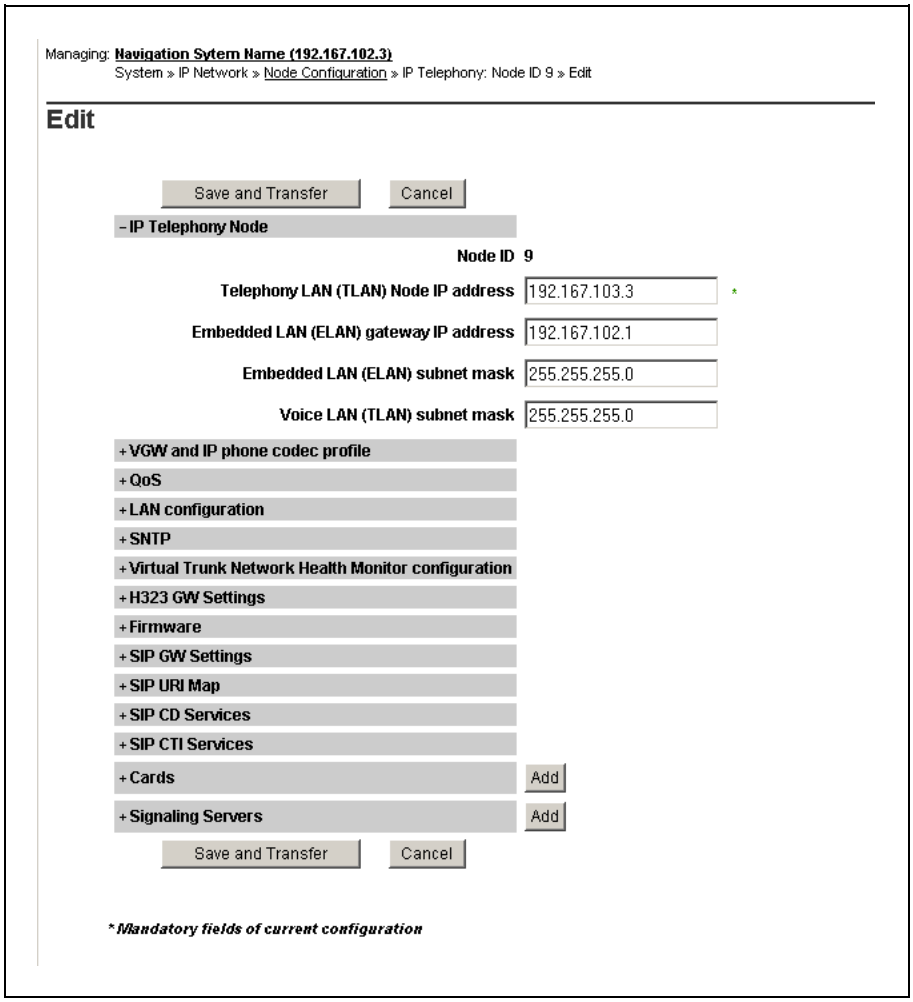
Figure 210
Node configuration



12 Click **Edit** next to the node where the target Signaling Server is located.

The Edit node web page appears.

Figure 211
Edit node configuration



Note: The information that you are editing is the node configuration that resides on the Call Server, not the Signaling Server.

13 Click **Save and Transfer** to transfer the node information to the target Signaling Server.

14 Re-boot the target Signaling Server

—End—

Procedure 41

Migrating a Standalone Signaling Server - NRS only with no Call Server association

Step	Action
1	Install CS 1000 Release 5.0 software on the target Signaling Server and configure the Signaling Server as a Standalone Signaling Server - NRS only with no Call Server association, using the IP Telephony and data networking data that you collected from the source Signaling Server. • If the target Signaling Server is an IBM X306m or HP DL320-G3, see "Software installation" (page 111). • If the target Signaling Server is a Nortel CP PM (CS 1000 Release 5.0 Signaling Server software is preloaded), see Procedure 20 "Entering basic system configuration parameters" (page 131).

—End—

Migrate an NRS database

This section describes the processes for migrating an NRS database from one Signaling Server (source) to another Signaling Server (target).

The following list summarizes the tasks required to perform an NRS database migration:

- "Back up the NRS database" (page 231)
- "Restore the NRS database" (page 235)
- "Activate the NRS database" (page 237)

Back up the NRS database

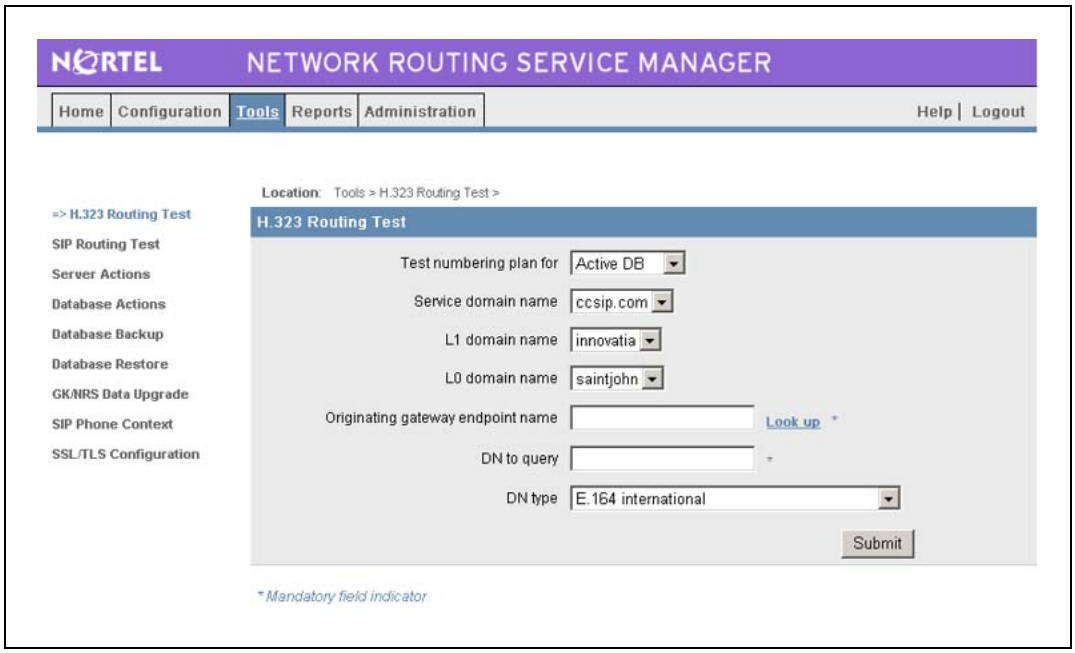
Use the following procedure to back up the NRS database from the source Signaling Server and download it to your local PC.

Procedure 42

Backing up the NRS database

Step	Action
1	Log on to NRS Manager on the source Signaling Server (seeProcedure 27 "Logging on to NRS Manager" (page 169)).
2	Click on the **Tools** tab. The NRS Manager Tools web page appears.

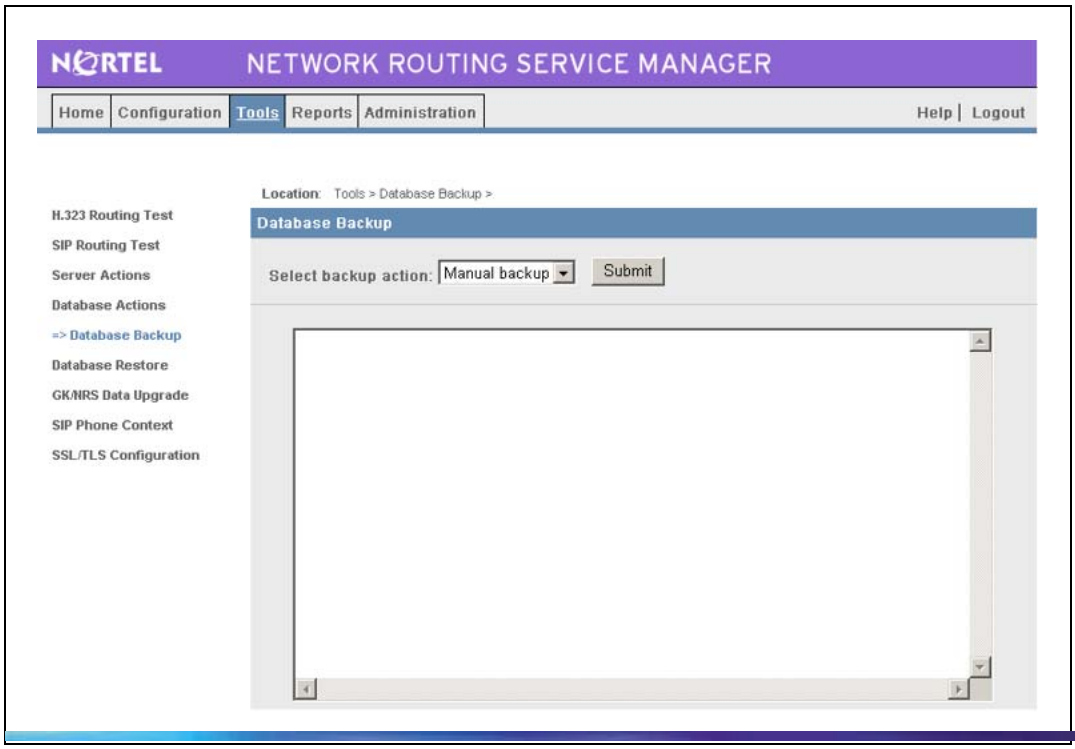
Figure 212
NRS Manager Tools



3 Click on the **Database Backup** option on the navigation tree.

The NRS Database Backup web page appears.

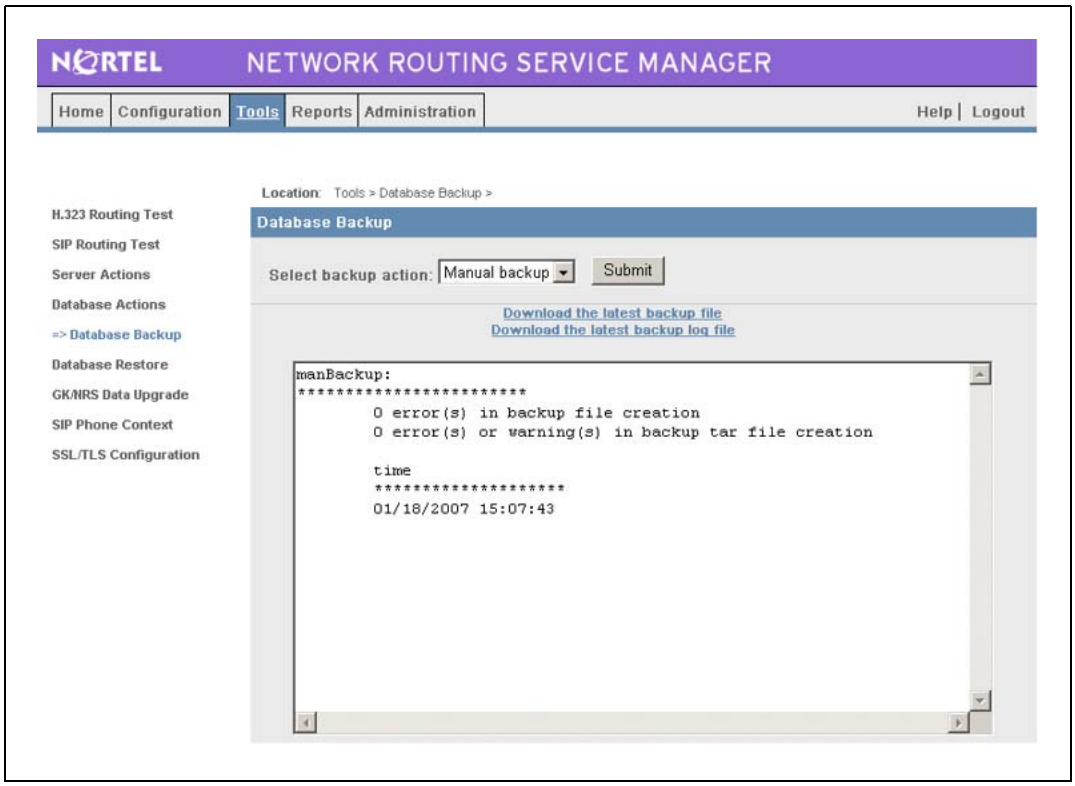
Figure 213
NRS Database Backup



4 Select **Manual backup** from the **Select backup action** drop-down box and click **Submit**.

The Database Backup web page appears again with details about the database backup and offering options to download the latest backup file or the associated backup log file.

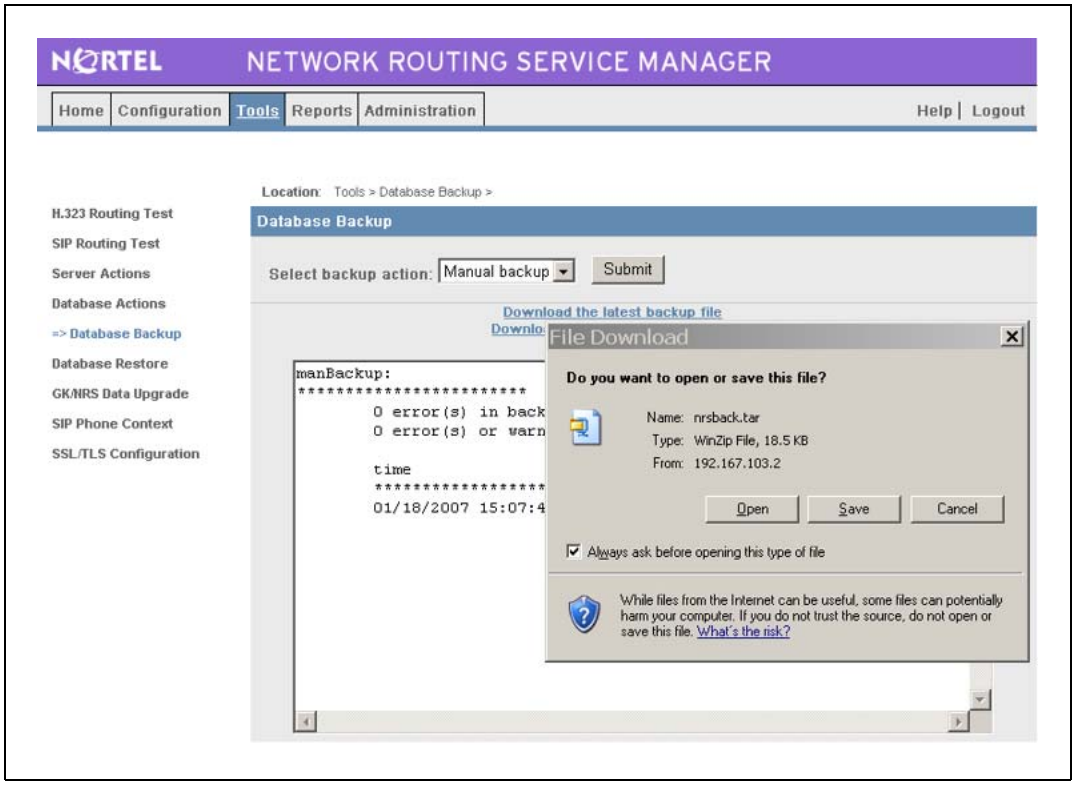
Figure 214
NRS database backup



5 Click on the **Download the latest backup file** option.

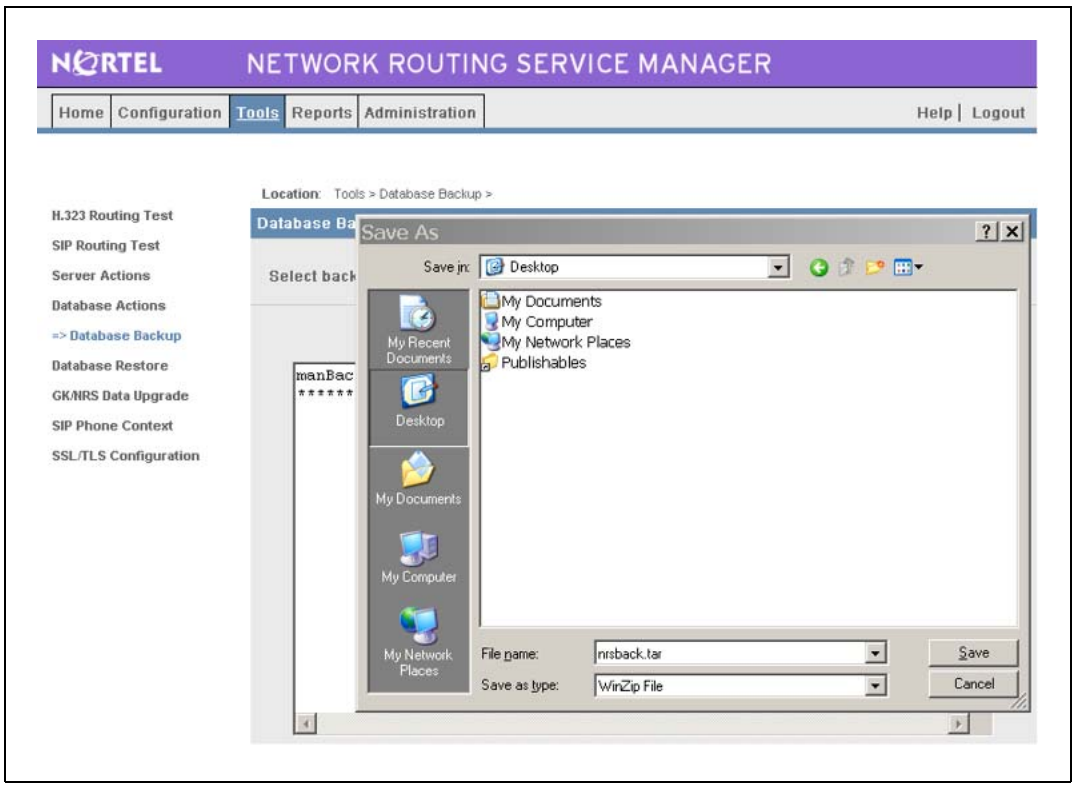
A file download window appears asking if you would like to **Open** or **Save** the file.

Figure 215
Download NRS database backup



6 Click on **Save** and a **Save as** window appears.

Figure 216
Save NRS database backup on local PC



Navigate to a location on your local PC and press the **Save**button. The NRS database backup file is saved to the chosen location on your local PC.

—End—

Restore the NRS database

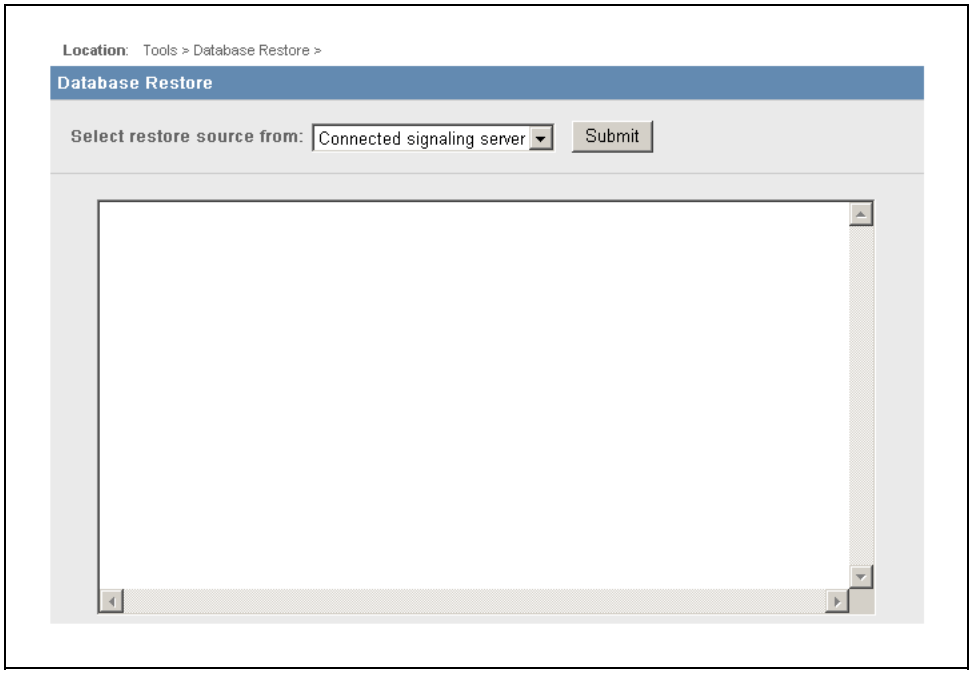
Use the following procedure to restore the backed up NRS database from your local PC to the target Signaling Server.

Procedure 43
Restoring the NRS database

Step	Action
1	Log on to NRS Manager on the target Signaling Server (see Procedure 27 "Logging on to NRS Manager" (page 169)).
2	Click the **Tools** navigation tab.
3	Click the **Database Restore** option on the navigation tree.

The Database Restore web page appears.

Figure 217
Database Restore



4 Select the **Connected Signaling Server** option from the **Select restore source from** drop-down list and click **Submit** to restore the NRS database.

Data from the old StandBy database is replaced with data from the new NRS database.

Monitor the log messages that appear in the browser window. If additional log analysis is necessary, a generated XML file is accessible to the user.

Monitor these key logs:

- Logs indicating that some entries cannot be restored correctly:
  - The particular entry does not exist in the new database, so the user must check and provision it manually.
- Messages indicating corruption of the nrsback.tar file:
  - The nrsback.tar file is not properly formatted or the content is not recognizable to the Restoring tool. The user must check the tar file and possibly regenerate and upload it again.

ATTENTION

The new NRS database is loaded in standby DB view. You must activate the new NRS database to complete the migration process.

—End—

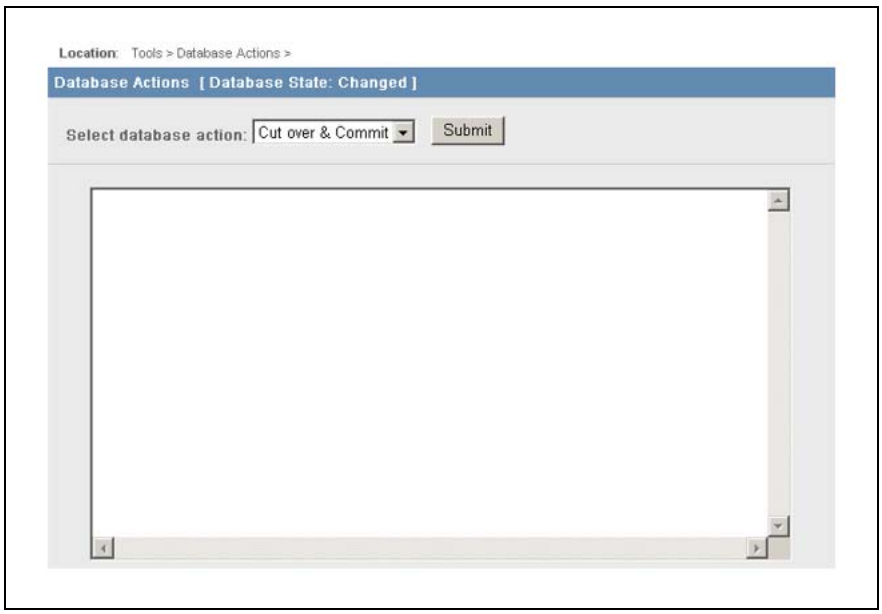
Activate the NRS database

Use the following procedure to activate the new NRS database on the target Signaling Server.

Procedure 44
Activating the NRS database

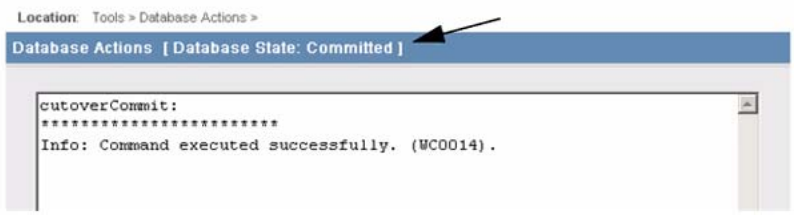
Step	Action
1	Click the **Tools** navigation tab.
2	Click the **Database Actions** option on the navigation tree. The Database Actions web page appears.

Figure 218
Database Actions



Step	Action
3	Select the **Cut over & Commit** option from the **Select database action** drop-down list.
4	Click the **Submit** button to activate the new NRS database. A message appears in the text box indicating that the cut over and commit command was executed successfully.

Figure 219
Database Actions: cutover and commit (successful)



The NRS database is saved and is in Active DB view.

—End—

Element Manager configuration

Contents

This section contains information on the following topics:

Introduction

Element Manager is a simple and user-friendly web-based interface that supports a broad range of system management tasks, including:

- configuration and maintenance of IP Peer and IP telephony features
- configuration and maintenance of traditional routes and trunks
- configuration and maintenance of numbering plans
- configuration of Call Server data blocks (such as configuration data, customer data, Common Equipment data, D-channels)
- maintenance commands, system status inquiries, backup and restore functions
- software download, patch download, patch activation

Element Manager has many features to help administrators manage systems with greater efficiency. Examples are as follows:

- Web pages provide a single point-of-access to parameters that were traditionally available through multiple overlays.

- Parameters are presented in logical groups to increase ease-of-use and speed-of-access.
- The "hide or show information" option enables administrators to see information that relates directly to the task at hand.
- Full-text descriptions of parameters and acronyms help administrators reduce configuration errors.
- Configuration screens offer pre-selected defaults, drop-down lists, checkboxes, and range values to simplify response selection.

The Element Manager web server resides on the Signaling Server and can be accessed directly through a web browser or Telephony Manager (TM). The TM navigator includes integrated links to each network system and their respective instances of Element Manager.

For more information about Element Manager, refer to *Element Manager: System Administration (NN43001-632)*.

Configuring the Internet Explorer browser

System requirements for Element Manager

Element Manager and NRS Manager requires Microsoft Internet Explorer 6.0.2600 or higher with Service Pack 1. Element Manager and NRS Manager are not supported on the Netscape browser.

The Element Manager Virtual Terminal Environment requires the Java Runtime Environment (JRE).

Configuring the browser

Before you can use Element Manager and NRS Manager, you must complete the following tasks:

- Enable pop-ups in the browsers search utility (mandatory)
- Configure the Internet Explorer browser settings (mandatory)
- Configure the Windows Display settings (highly recommended)

Note: The interface for the Internet Explorer browser settings and Windows Display settings can vary by browser version and by operating system.

Enabling pop-ups

If you use a browser search utility (such as the Google™ search engine or the Yahoo!™ search engine), ensure that pop-ups are enabled. Enabling pop-up windows is usually done at the toolbar of the search utility.

ATTENTION

IMPORTANT!
Do not block pop-up windows if you are using a search utility (such as Google or Yahoo! search engines) in your browser.

Configuring the browser settings

Use the following procedure to configure the following Internet Explorer browser settings.

- Turn off Internet Explorer caching.

  Internet Explorer caching interferes with the Element Manager and NRS Manager applications, such that users cannot see real-time changes as they occur.

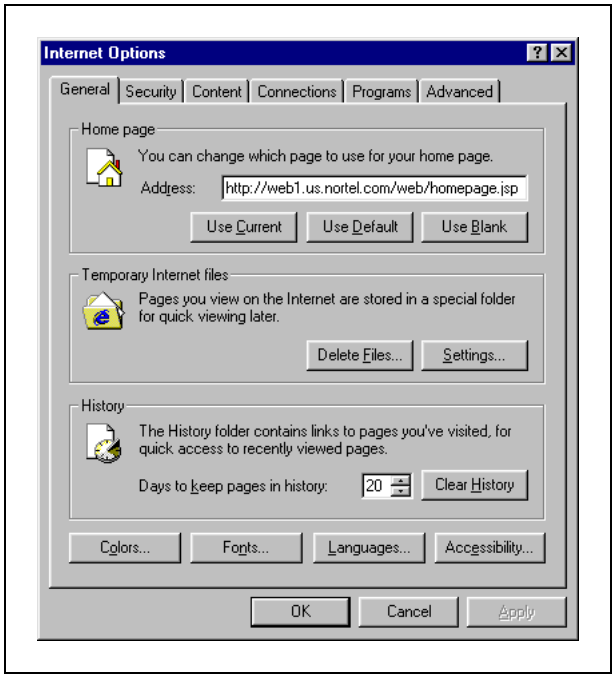
- Configure empty session information.
- Deselect the AutoComplete options.

Procedure 45

Configure the Internet Explorer browser settings

Step	Action
1	Select **View > Text Size > Medium** to configure the text size in the browser.
2	Select **Tools > Internet Options** In the Internet Explorer browser window. The **Internet Options** window appears, as shown in Figure 220 "Internet Options window" (page 242).

Figure 220
Internet Options window



3 Turn off Internet Explorer caching:

a. On the **General** tab under the **Temporary Internet files** section, click **Settings**.

The **Settings** window appears.

b. Under the **Check for newer versions of stored pages** section, select the **Every visit to the page** option.

c. Click **OK**.

4 Configure empty session information:

a. Select the **Advanced** tab.

The Advanced Settings window appears.

b. Under **Security**, select **Empty Temporary Internet Files folder when browser is closed**.

5 Deselect the AutoComplete options.

a. Select the **Content** tab.

b. Under **Personal Information**, click **AutoComplete**.

The **AutoComplete Settings** window appears.

c. Under the **Use AutoComplete for** section, deselect **Forms** and **User names and passwords on forms**.

6 (Optional) Configure the Windows display settings.

a. Select **Start > Settings > Control Panel > Display**.

The **Display Settings** window appears.

b. Select the **Settings** tab.

c. Select **True Color (32 bit)** from the **Colors** drop-down list.

d. Under **Screen area**, select **1280 by 1024 pixels**.

e. Click **OK**.

—End—

Log on to Element Manager

Before logging on to Element Manager, obtain the IP address of:

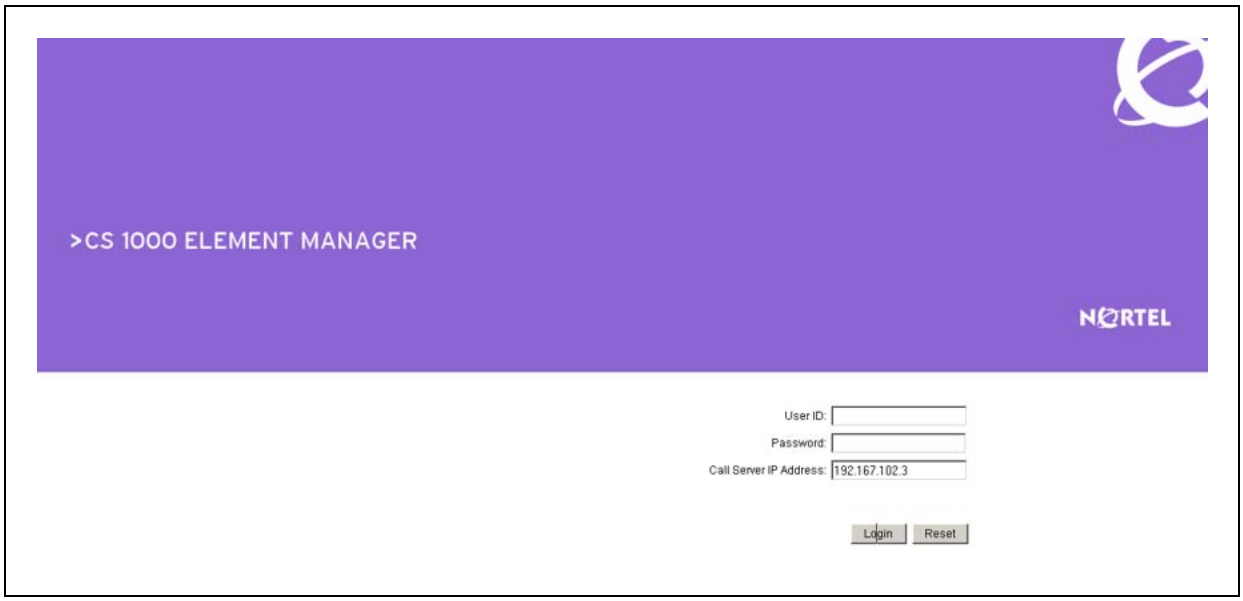
- the Signaling Server
- the Call Server (or MG 1000B Core if at a branch office)

Before beginning this procedure, be sure that you have configured the browsers properly, using Procedure 45 "Configure the Internet Explorer browser settings" (page 241).

Procedure 46
Logging on to Element Manager

Step	Action
1	Open Internet Explorer.
2	Enter the ELAN or TLAN network interface IP Address of the primary Signaling Server as the URL. ***Note:*** Do not assign the same IP address for the Node ID and the TLAN network interface IP address. This must be verified manually. The Node IP address must be on the same subnet as the TLAN network interface IP addresses of the Media Cards. In addition, the TLAN and ELAN network interfaces of the Media Card must reside on separate logical subnets. If additional configuration parameters were entered during installation, the node IP address can also be used as the URL. The Element Manager logon web page appears.

Figure 221
Element Manager logon page



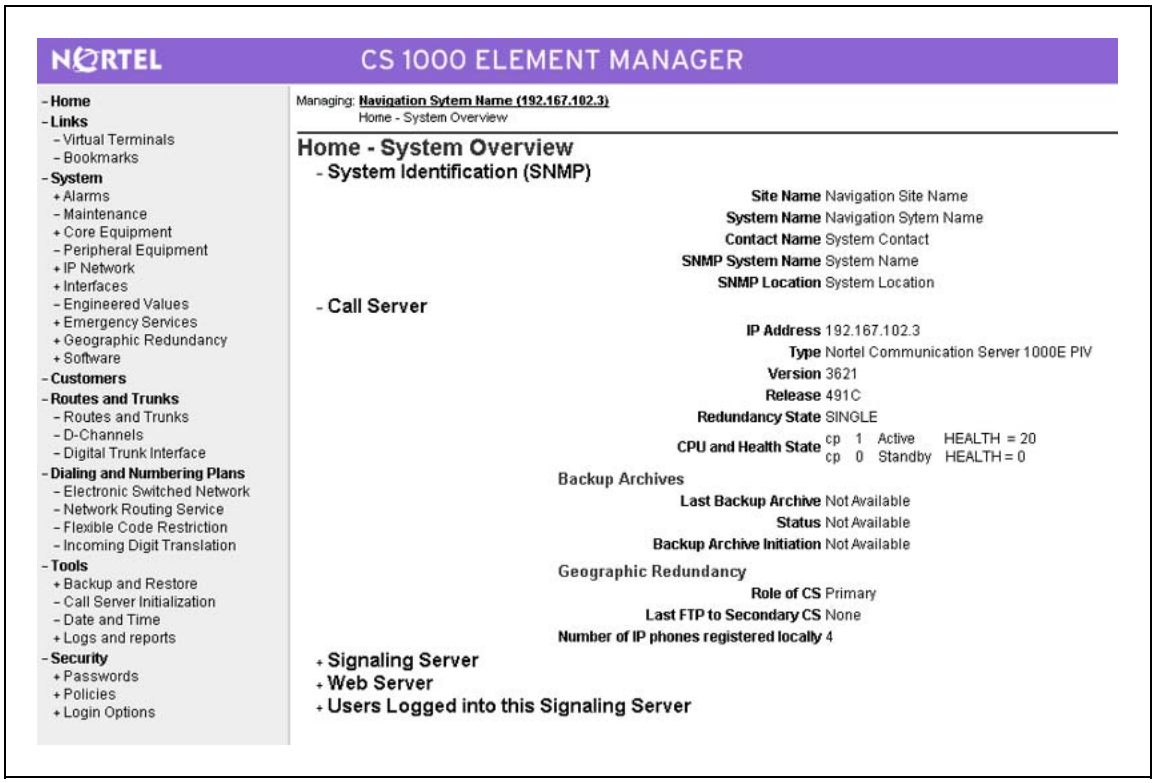
Initially, you can be prompted to enter the Call Server IP address, because the Call Server is used for web logon authorization. The Call Server IP address is a requirement, because unless you entered additional configuration parameters during the Signaling Server installation, the node configuration data file containing the Call Server IP address does not yet exist.

3 Enter a Level 1 or Level 2 user ID and password. If configured, you can also use a Limited Access Password (LAPW) user ID and password.

If this is the first time the Call Server is accessed, the default Level 1 or Level 2 user ID and password must be used.

If the logon is successful, the Element Manager System Overview web page (with the navigator) appears.

Figure 222
Element Manager: System Overview web page with navigator



Now you can begin to configure the Call Server or IP telephony node. For more information, see *IP Line Fundamentals (NN43001-500)* and *Element Manager: System Administration (NN43001-632)*.

—End—

ATTENTION

IMPORTANT!

Nortel discourages the use of the browser's Back, Forward, and Refresh buttons.

Use of the Back button is not recommended while the Element Manager application is launched because Element Manager pages contain dynamic data content. The Element Manager provides a path for navigation purposes on top of every Element Manager page.

Nortel recommends that the user click the navigation path to go back to the previous page (instead of using the Back button).

Restricting web access to the ELAN subnet

By default, Element Manager can be accessed from management workstations (web browsers) on any subnet. A security flag can be enabled to restrict Element Manager access to hosts on the ELAN subnet.

If this Signaling Server's IP Telephony node is already managed using Element Manager, perform a node file transfer to ensure that the Signaling Server has the latest node files before performing this procedure.

Procedure 47
Changing the web server security flag

Step	Action
1	Open the Tools Menu in the Signaling Server Installation Tool (see Procedure 51 "Accessing the Signaling Server Tools Menu" (page 297)).
2	Enter **e** to change the web server security flag. The following system message appears: `Currently, the flag is set to:  DISABLED`
3	Change the flag accordingly: a. To disable the web server security flag, enter **a**. The new flag setting appears. b. To enable the web server security flag, enter **b**. The new flag setting appears. c. To exit this menu without changing the web server security flag, enter **q**.
4	Import the IP Telephony node files for the web security flag change to take effect. Refer to "Importing IP Telephony nodes" (page 251). For a first-time Signaling Server or Node installation, the preconfigured IP Telephony node files are imported. For an upgrade of an existing Signaling Server, the web server security flag change is saved to the master copy of the node files on the Call Server.

—End—

Unpacking Help files for Virtual Terminal Emulator

Help files for the Virtual Terminal Emulator (VTE) are copied to the Signaling Server as compressed files during installation of the Signaling Server software. Unpacking the Help files is optional. They can be unpacked any time after the Signaling Server software is installed.

ATTENTION

IMPORTANT!

Unpacking the Help files takes approximately 20 to 30 minutes. Nortel recommends that you unpack the Help files during a service outage.

Use the following procedure to unpack the Help files.

Procedure 48

Unpacking Help files for Virtual Terminal Emulator

Step	Action
1	Reboot the Signaling Server.
2	Log on to the Signaling Server CLI. Use Procedure 22 "Logging on to the Signaling Server" (page 147).
3	Enter the following command at the prompt: `unpackVTHelp`

—End—

Refer to *Element Manager: System Administration (NN43001-632)* for more information on Element Manager and the Virtual Terminal Emulator.

IP Telephony node configuration

Contents

This section contains information on the following topics:

Introduction

This chapter describes the configuration and management of IP Telephony nodes. The procedures can be carried out in either TM or Element Manager, and are fully described in *IP Line Fundamentals (NN43001-500)*.

IP Telephony nodes

An IP Telephony node is defined as a collection of Signaling Servers and Voice Gateway Media Cards. Each network node has a unique Node ID that is an integer value. A node has only one Leader Signaling Server. All other Signaling Servers and Voice Gateway Media Cards are defined as Followers.

An IP Telephony node must be configured to make a CS 1000 system operational. The IP Telephony node files are BOOTP.TAB and CONFIG.INI. The master copies of the BOOTP.TAB and CONFIG.INI files reside on the Call Server, with an additional copy on each node component (Signaling Server and Voice Gateway Media Cards).

The node database files are backed up, along with the customer database file, by using the EDD command in LD 43. Refer to *Software Input/Output: Maintenance (NN43001-711)* for details about this command. The backup can also be done in Element Manager using the procedure described in "Backing up IP Telephony node configuration files" (page 252).

When a Leader Signaling Server is first installed, the IP Telephony nodes are configured during software installation. After software installation, the node configuration files are imported into Element Manager for further node configuration. These files are saved on the Call Server as the following:

- c:/u/db/node/node*x*.cfg where *x* is the node number
- c:/u/db/node/node*x*.btp where *x* is the node number

ATTENTION

IMPORTANT!

Do not attempt to alter the database files manually or by importing to IP Trunk or IP Telephony management in TM. Use Element Manager.

IP Telephony nodes are configured in Element Manager. Therefore, a Signaling Server that hosts Element Manager must be installed. See "Element Manager configuration" (page 239).

For more information about IP Telephony nodes and their configuration, refer to *IP Line Fundamentals (NN43001-500)*. For more information about Element Manager, refer to *Element Manager: System Administration (NN43001-632)*.

IP Telephony node configuration procedures

This section provides a high-level summary of the procedures used to configure an IP Telephony node using Element Manager (EM) or Telephony Manager (TM).. For detailed procedures and additional information about IP Telephony nodes, refer to *IP Line Fundamentals (NN43001-500)*.

For information about upgrading IP Trunk nodes, refer to *Communication Server 1000E: Upgrade Procedures (NN43041-458)* or *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures (NN43021-458)*.

WARNING

Before and after you make a change to the customer database, perform a datadump. The customer database is not impacted in this chapter. However, the IP Telephony node is, and its files are backed up at the same time as the customer database. Use the EDD command in LD 43, or use Element Manager (refer to "Backing up IP Telephony node configuration files" (page 252)).

Importing IP Telephony nodes

This procedure is used to import existing IP Telephony nodes, including those that are configured during the installation of the Signaling Server software (see "mam commands: MAM module" (page 267)).

Adding a Follower Signaling Server to a node

This procedure is used to add a Follower Signaling Server to an existing IP Telephony node. Refer to Procedure 21 "Adding a Follower Signaling Server to an IP Telephony node" (page 144) for instructions on adding a Follower Signaling Server to an IP Telephony node.

After installing Signaling Server software on a server for the first time, configuring it as a Follower Signaling Server, and then rebooting it, the Follower Signaling Server sends out a BOOTP request using FTP and waits for a successful BOOTP response. Because the Follower Signaling Server has not been booted before and cannot obtain the system logon ID and password or the current CONFIG.INI file with the Call Server IP address, no successful BOOTP response will be received. Do not wait for the successful BOOTP response; perform this procedure immediately.

> ***Note:*** The first time the Follower Signaling Server is installed, configured and booted, the BOOTP request sent using FTP fails. The failure occurs because the Follower does not have the system logon and password or the current CONFIG.INI file with the Call Server IP address. In subsequent Follower installations, the BOOTP request succeeds.

Importing and upgrading an IP Trunk node

To work with IP Trunk nodes, the IP Trunk cards must first be converted to Voice Gateway Media Cards. They can then be added to new and existing IP Telephony nodes. To import and upgrade an IP Trunk node to an IP Telephony Node, refer to *Communication Server 1000E: Upgrade Procedures (NN43041-458)* or *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures (NN43021-458)*.

Reviewing and submitting IP Telephony node configuration

Use this procedure to review IP Telephony node configuration before submitting. If the configuration is correct, the data can be submitted.

Transferring IP Telephony files

Use this procedure whenever you change the IP telephony node configuration. This procedure transfers the node data files to the other nodes in the system. You can transfer the data files to one, many, or all other nodes in the system.

ATTENTION

IMPORTANT!

After completing this procedure, reboot the Signaling Server if you changed its configuration.

Backing up IP Telephony node configuration files

Use this procedure as an alternative to the EDD command in LD 43 to perform a datadump. The datadump backs up new and updated IP Telephony node files on the Call Server at the same time as it backs up the customer database.

Command Line Interface (CLI) commands

Contents

This section contains information on the following topics:

Introduction

The Signaling Server provides a Command Line Interface (CLI) through a serial port or a telnet session. This section contains the CLI commands available for use through that interface.

Signaling Server CLI commands are available at three levels:

- Level One — Operations, Administration, and Maintenance (OAM) shell for basic technician support and general status system checking (`oam>` prompt)
- Level Two — Problem Determination Tool (PDT) shell for expert support; also includes all Level One (OAM) commands (`pdt>` prompt)
- Level Three — Nortel proprietary VxWorks™ shell for advanced debugging and design support (>prompt)

  Note: This section describes the Level One (OAM) and Level Two (PDT) CLI commands. Level Three commands are considered expert support and design level commands, and are not documented here.

You must log on to the Signaling Server to use the CLI. See Procedure 22 "Logging on to the Signaling Server" (page 147).

Platform-specific commands are fully described in this section. Application-specific commands are fully described in the documentation for the particular application. Therefore, they are only briefly described in this section, and a reference is given to the NTP containing the full description.

The information in this chapter is presented in tables, with the commands organized by command groups. Each table gives the command name and a description of the command.

Element Manager

The "Element Manager" column gives the Element Manager command group name if the command is available in Element Manager. If the command is not available in Element Manager, the column entry reads "N/A" for "Not Available".

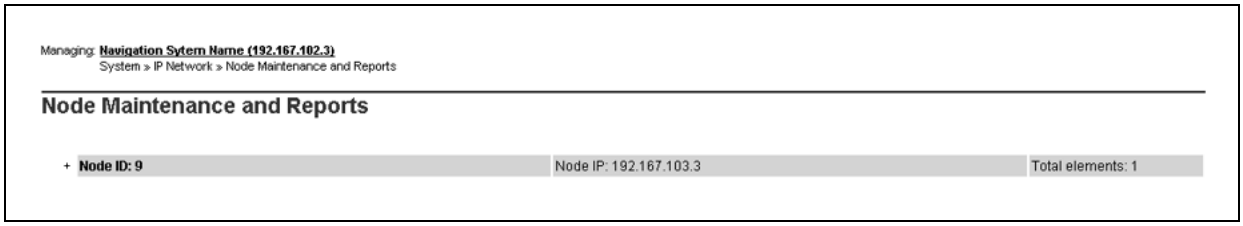
Use the following procedure to access the CLI commands in Element Manager.

Procedure 49

Accessing CLI commands in Element Manager

Step	Action
1	Log on to Element Manager (see Procedure 46 "Logging on to Element Manager" (page 243).
2	Select **IP Network > Maintenance and Reports** from the navigator. The **Node Maintenance and Reports** web page appears.

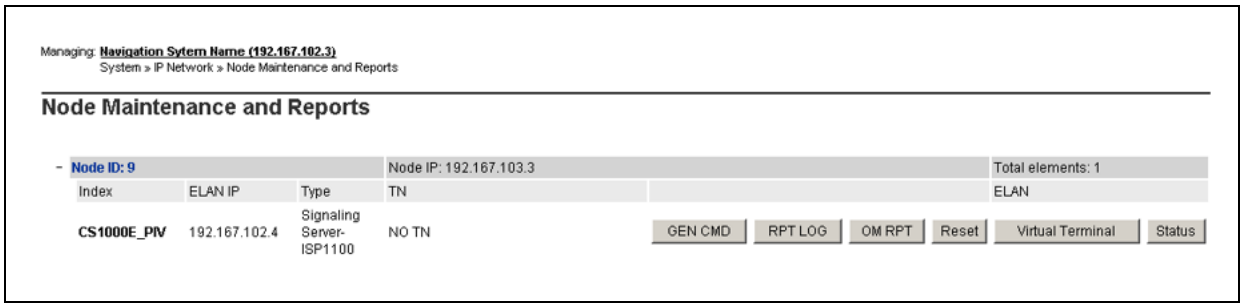
Figure 223
Node Maintenance and Reports



3 Click on the node with the Signaling Server you want to use.

The node listing expands to show the elements associated with the selected node, including the Signaling Server.

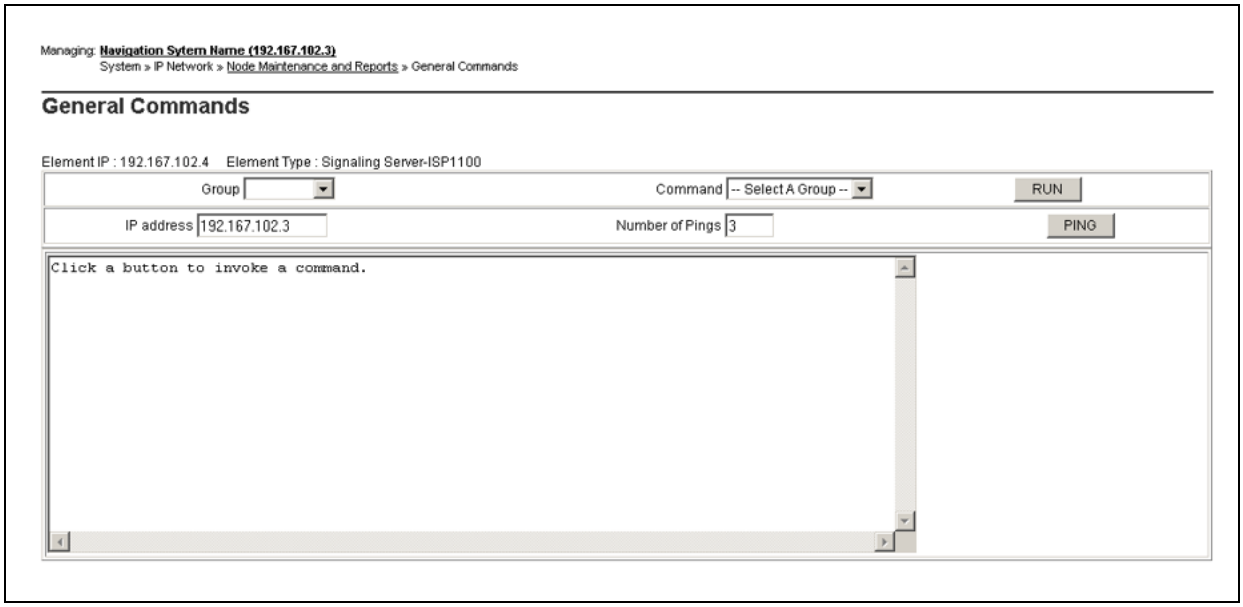
Figure 224
Expanded IP Telephony node



4 Click **GEN CMD** for the Signaling Server element.

The **General Commands** web page appears.

Figure 225
General Commands



5 To run a command:

a. Select a command group from the **Group** drop-down list.

b. Select a command from the **Command** drop-down list.

c. Click **Run**.

If the selected command has parameters, enter them in the additional text boxes that appear. Command output appears in the text area below the commands.

—End—

For more information on Element Manager, refer to "Element Manager configuration" (page 239) and *Element Manager: System Administration (NN43001-632)*.

General help commands

To display a list of command groups, type **`help`** at the prompt.

To display a list of commands in a specific group, and a brief description of each command, type help **`<command group name>`**.

Level One (OAM) CLI commands

This section lists the Level One Signaling Server CLI commands available at the OAM shell.

The prompt for each command is **`'oam>`**'.

Command groups

The following table lists the OAM CLI command groups. The commands in each group are described in the following sections.

Table 5
OAM CLI command groups

Command group	Description	Commands
DLOG	Firmware download log file commands	Table 6 "OAM DLOG commands" (page 259)
GK	Gatekeeper module commands	Table 7 "OAM GK commands" (page 260)
ISEC	Intrasystem signaling security commands.	Table 8 "OAM ISEC commands" (page 261)

Command group	Description	Commands
Network	Remote access commands	Table 9 "OAM Network commands" (page 261)
Patcher	Patching commands.	Table 10 "OAM Patcher commands" (page 262)
RID	Remote iset diagnostics commands	Table 11 "OAM RID commands" (page 262)
SSH	SSH commands.	Table 12 "OAM SSH commands" (page 263)
UFTP	UFTP IP Phone firmware download commands.	Table 13 "OAM UFTP commands" (page 264)
cds	Converged Desktop Service module commands	Table 14 "OAM cds commands" (page 264)
election	Election module commands	Table 15 "OAM election commands" (page 265)
elm	ELM module commands	Table 16 "OAM elm commands" (page 265)
emhelp	Element Manager help file related commands.	Table 17 "OAM emhelp commands" (page 265)
iset	iset module commands	Table 18 "OAM iset commands" (page 265)
mam	MAM module commands	Table 19 "OAM mam commands" (page 267)
ncs	Network Connection Service module commands	Table 20 "OAM ncs commands" (page 269)
npm	Network Protocol Module commands	Table 21 "OAM npm commands" (page 270)
nrsDB	Network Routing Service commands	Table 22 "OAM nrsDB commands" (page 271)
nrsomm	Network Routing Service operational measurement commands	Table 23 "OAM nrsomm commands" (page 272)
pbxlink	PBX link commands	Table 24 "OAM pbxlink commands" (page 272)
securityShell	Security shell commands	Table 25 "OAM securityShell commands" (page 273)
sipcti	SIP CTI module commands.	Table 26 "OAM sipcti commands" (page 273)
sipctiomm	SIP CTI OMM commands.	Table 27 "OAM sipctiomm commands" (page 274)

Command group	Description	Commands
sipnpm	SIP Network Protocol Module commands	Table 28 "OAM sipnpm commands" (page 274)
system	System administration commands	Table 29 "OAM system commands" (page 275)
tps	TPS module commands	Table 30 "OAM tps commands" (page 276)
trace	General trace tools	Table 31 "OAM trace commands" (page 278)
uipc	Universal ISDN module commands	Table 32 "OAM uipc commands" (page 279)
ums	UMS module commands	Table 33 "OAM ums commands" (page 279)
usi	RUDP timeout and retry commands	Table 34 "OAM usi commands" (page 280)
vte	Virtual Terminal Emulator commands	Table 35 "OAM vte commands" (page 280)
vtrk	Virtual Trunk module commands	Table 36 "OAM vtrk commands" (page 280)

DLOG commands: Firmware download log file

The following table lists the OAM firmware download log file commands in the DLOG command group.

Table 6
OAM DLOG commands

Command	Description	Element Manager
`activeDlogShow`	Displays the current used firmware download file. See *IP Line Fundamentals (NN43001-500)*.	N/A
`inactiveDlogShow`	Displays the inactive firmware download log file. See *IP Line Fundamentals (NN43001-500)*.	N/A
`dnldFailShow`	Displays failed results in the active firmware download log file. See *IP Line Fundamentals (NN43001-500)*.	N/A

GK commands: Gatekeeper

The following table lists the OAM Gatekeeper commands in the GK command group.

Table 7
OAM GK commands

Command	Description	Element Manager
`gkDiscoveryTrace`	Traces Gatekeeper discovery messages for a specified endpoint. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`gkRegTrace`	Traces endpoint registration messages and unregistration messages for a specified endpoint. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`gkCallTrace`	Traces endpoint call-associated messages (admission, bandwidth, disengage, and location messages). See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`gkProtocolTrace`	Traces any message for any message type. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`gkTraceOff`	Turns off the trace for the specified endpoint for all protocol types. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`gkTraceOutput`	Sets the output destination for all Gatekeeper protocol traces. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`gkTraceSettings`	Displays the trace output destination as well as the endpoint types being traced. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`gkTraceTblClear`	Clears the calling/called number table associated with the NUM trace filter(s). See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`gkTraceTblShow`	Displays the calling/called number table associated with the NUM trace filter(s). See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A

ISEC commands: Intrasystem Signaling Security

The following table lists the OAM intrasystem Signaling Security commands in the OAM ISEC command group.

Table 8
OAM ISEC commands

Command	Description	Element Manager
`isecChgPSK`	Change ISEC PSK locally.	N/A
`isecChgLevel`	Change ISEC security level locally.	N/A
`isecNewTarget`	Add a new target to the ISEC target list.	N/A
`isecOutTarget`	Delete a target from the ISEC target list.	N/A
`isecEnlTarget`	Enable the target ISEC.	N/A
`isecDisTarget`	Diable the target ISEC.	N/A
`isecprofileShow`	Show all ISEC profiles.	N/A
`isecConfirm`	Used to confirm PSK between Active Call Server and other elements.	N/A
`isecDecom`	Removes all ISEC related files, memory allocations, and tasks.	N/A
`isecIkeShowPall`	Show all protection suites (inbound and outbound IPsec Security Association pairs)	N/A
`isecIpsecShowIf`	Show all of the network interfaces on which IPsec is enabled.	N/A

Network commands: remote access

The following table lists the OAM remote access commands in the Network command group.

Table 9
OAM Network commands

Command	Description	Element Manager
`telnet [server] [-l username]`	Telnets to a server. The address can be either in IP address format or host name. Where: • server = IP • addressusername = host name	N/A

Command	Description	Element Manager
`rlogin [server] [-l username]`	Remotely logs in to a server. The address can be either an IP address or host name. Where: • server = IP • addressusername = host name	N/A
`cslogin`	Logs in to the Call Server overlays.	N/A

Patcher commands: patching

The following table lists the OAM patching commands in the OAM Patcher command group.

Table 10
OAM Patcher commands

Command	Description	Element Manager (see Note)
`mdp`	DEPLIST manipulation command	N/A

Note: The Patcher command is not available in Element Manager from the **Node Maintenance** web page. It is available from **IP Telephony > Software > Patching**

RID commands: remote iset diagnostics

The following table lists the OAM remote iset diagnostic commands in the RID command group.

Table 11
OAM RID commands

Command	Description	Element Manager
`rPing`	Pings an IP address. See *Converging the Data Network with VoIP (NN43001-260)*.	QoS
`rPingStop`	Stops pinging an IP address. See *Converging the Data Network with VoIP (NN43001-260)*.	N/A
`rTraceRoute`	Traces the route of an IP address. See *Converging the Data Network with VoIP (NN43001-260)*.	QoS

Command	Description	Element Manager
`rTraceRouteStop`	Stops tracing the route of an IP address. See *Converging the Data Network with VoIP (NN43001-260)*.	N/A
`RUDPStatShow`	Displays RUDP/UNIStim statistics for an IP Phone. See *Converging the Data Network with VoIP (NN43001-260)*.	N/A
`eStatShow`	Displays Ethernet statistics for an IP Phone. See *Converging the Data Network with VoIP (NN43001-260)*.	N/A
`isetInfoShow`	Displays DHCP configurations and iset information for an IP Phone. See *Converging the Data Network with VoIP (NN43001-260)*.	QoS

SSH commands: SSH commands

The following table lists the OAM SSH commands in the OAM SSH command group.

Table 12
OAM SSH commands

Command	Description	Element Manager
`sshKeyActivate`	Activates the SSH key.	N/A
`sshKeyClear`	Clears the SSH key.	N/A
`sshKeyGenerate`	Generates the SSH key.	N/A
`sshKeyShow`	Displays the SSH key.	N/A

UFTP commands: UFTP IP Phone firmware download

The following table lists the OAM UFTP IP Phone firmware download commands in the UFTP command group.

These OAM UFTP commands are used with a Signaling Server in maintenance mode. When the Signaling Server is in maintenance mode, the maximum number of simultaneous firmware downloads is increased,

thereby allowing the UNIStim Firmware Transfer Protocol (UFTP) server to use most of its processing resources. For more information on maintenance mode and the UFTP server, refer to *IP Line Fundamentals (NN43001-500)*.

Table 13
OAM UFTP commands

Command	Description	Element Manager
uftpShow	Displays IP Phone firmware download information. See *IP Line Fundamentals (NN43001-500)*.	N/A
uftpNodeShow	Displays IP Phone firmware download summary for the node. See *IP Line Fundamentals (NN43001-500)*.	N/A
uftpRunTimeDataReset	Resets the run time data field in the UFTP data block. See *IP Line Fundamentals (NN43001-500)*.	N/A
uftpTurboMode	Configures maintenance mode. See *IP Line Fundamentals (NN43001-500)*.	Uftp
uftpTurboModeShow	Displays current status of maintenance mode. See *IP Line Fundamentals (NN43001-500)*.	Uftp
uftpSpeedLimitShow	Display UFTP bandwidth parameters.	N/A
uftpSpeedLimitSet	Configure UFTP bandwidth parameters.	N/A
uftpTurboModeTimeoutSet	Configures the idle timeout timer for maintenance mode. See *IP Line Fundamentals (NN43001-500)*.	Uftp
uftpAutoUpgradeTimeoutSet	Configures the length of time the IP Phone waits for a user response after "Upgrade F/W?" prompt before automatically beginning the firmware upgrade. See *IP Line Fundamentals (NN43001-500)*.	Uftp

cds commands: Converged Desktop Service Module

The following table lists the OAM Converged Desktop Service (CDS) commands in the cds command group.

Table 14
OAM cds commands

Command	Description	Element Manager
cdsShow	Displays the current Converged Desktop configuration. See *CS 1000 to MCS 5100 Converged Desktop Type 2: Configuration Guide (NN43001-321)*.	N/A
cdsAgentShow	Displays the Personal Call Assistance (PCA) agents information and status. See *CS 1000 to MCS 5100 Converged Desktop Type 2: Configuration Guide (NN43001-321)*.	N/A

election commands: election module

The following table lists the OAM election module commands in the election command group.

Table 15
OAM election commands

Command	Description	Element Manager
`electShow`	Displays the card TPS state, current master, and a list of online TPS. See *IP Line Fundamentals (NN43001-500)*.	Election

elm commands: ELM module

The following table lists the OAM ELM module command in the elm command group.

Table 16
OAM elm commands

Command	Description	Element Manager
`elmShow`	Displays a list of supported languages. See *IP Line Fundamentals (NN43001-500)*.	N/A

emhelp commands: Element Manager help file related commands

The following table lists the OAM emhelp module command in the OAM emhelp command group.

Table 17
OAM emhelp commands

Command	Description	Element Manager
`unpackEmHelp`	Unpack Element manager help files	N/A

iset commands: iset module

The following table lists the OAM iset module commands in the iset command group.

Table 18
OAM iset commands

Command	Description	Element Manager
`isetShow`	Displays general information for all registered IP Phones. See *IP Line Fundamentals (NN43001-500)*.	Iset

Command	Description	Element Manager
isetFWShow	Displays the status of the firmware for IP Phones. See *IP Line Fundamentals (NN43001-500)*.	Iset
isetNATShow	Displays information about registered telephones behind a NAT router. See *IP Line Fundamentals (NN43001-500)*.	Iset
isetShowByTN	Displays general information for all registered IP Phones, sorted by TN. See *IP Line Fundamentals (NN43001-500)*.	N/A
isetShowByIP	Displays general information for all registered IP Phones, sorted by IP. See *IP Line Fundamentals (NN43001-500)*.	N/A
isetLocShow	Show location information for all connected IP Phones or a specified IP Phone.	N/A
isetLocNeedUpdateShow	Show location information for all connected IP Phones that need a location update.	N/A
isetLocNeedUpdateShow_DM	Show location information for all connected IP Phones than need a location update.	N/A
isetLocUpdate	Update location information for a specified IP Phone.	N/A
isetReset	Resets the registered IP Phone. See *IP Line Fundamentals (NN43001-500)*.	N/A
isetResetAll	Resets all registered IP Phones. See *IP Line Fundamentals (NN43001-500)*.	N/A
isetCount	Displays total number of registered IP Phones. See *IP Line Fundamentals (NN43001-500)*.	N/A
isetGet	Displays a list of IP Phones based on a specified query. See *IP Line Fundamentals (NN43001-500)*.	N/A
isetFWGet	Filters the output of the isetFWShow command by one of that command's output field names. See *IP Line Fundamentals (NN43001-500)*.	Iset
itgPLThreshold	Sets the IP Phone 2004 telephone and gateway alarm packet threshold (in units of 0.1%). See *IP Line Fundamentals (NN43001-500).*	N/A
nodePwdSet	Sets the password for the current node. See *IP Line Fundamentals (NN43001-500)*.	NodePwd
nodePwdShow	Displays the settings for the node password. See *IP Line Fundamentals (NN43001-500)*.	NodePwd
nodePwdEnable	Enables the node password setting. See *IP Line Fundamentals (NN43001-500)*.	NodePwd
nodePwdDisable	Disables the node password settings. See *IP Line Fundamentals (NN43001-500)*.	NodePwd

Command	Description	Element Manager
nodeTempPwdSet	Sets the temporary password for the current node. See *IP Line Fundamentals (NN43001-500)*.	NodePwd
nodeTempPwdClear	Clears the temporary password for the current node. See *IP Line Fundamentals (NN43001-500)*.	NodePwd
clearLockout	Clears the Branch User Config lockout. See *IP Line Fundamentals (NN43001-500)*.	N/A
dsetDelayHookswitchSet	Configure maximum time period in milliseconds that IP Phones wait for a hookswitch request.	N/A
cookieShowByTN	Print the cookie list for an IP Phone specified by TN.	N/A
cookieShowByName	Print the list of IP Phones with a particular cookie set.	N/A
cookieRegShow	Print the cookie registry.	N/A

mam commands: MAM module

The following table lists the OAM MAM module commands in the mam command group.

Table 19
OAM mam commands

Command	Description	Element Manager
firmwareVersionShow	Displays firmware version number. See *IP Line Fundamentals (NN43001-500)*.	N/A
IPInfoShow	Displays IP address information. See *IP Trunk Installation and Commissioning (NN43001-563)* and *IP Line Fundamentals (NN43001-500)*.	Mam
itgCardShow	Displays Voice Gateway Media Card information. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	Mam
itgMemShow	Displays memory usage. See *IP Line Fundamentals (NN43001-500)*.	N/A
resetOM	Resets the operational measurement file timer. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	N/A
bootPFileGet	Sends an updated bootptab file from the MAT to the ITG. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	N/A

Command	Description	Element Manager
bootPFilePut	Sends the bootptab file to the specified host. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	N/A
configFileGet	Sends an undated config.ini file from the MAT to the ITG. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	N/A
omFilePut	Sends the current OM file to the specified host. See *IP Line Fundamentals (NN43001-500)*.	N/A
currOMFilePut	Sends the current OM file to the specified host. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	N/A
prevOMFilePut	Sends the previous OM file to the specified host. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	N/A
hostFileGet	Transfers any file from the MAT to the ITG. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	N/A
hostFilePut	Transfers any file from the ITG to the specified host. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	N/A
swDownload	Loads new version of software from the FTP host to the ITG card. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	N/A
itgAlarmTest	Generates **ITGxxxx** test alarms. See *IP Line Fundamentals (NN43001-500)*.	N/A
itgPLThreshold	Sets the IP Phone 2004 telephone and gateway alarm packet threshold (in units of 0.1%). See *IP Line Fundamentals (NN43001-500)*.	N/A
disiAll	Gracefully disables the LTPS and voice gateway. See *IP Line Fundamentals (NN43001-500)*.	N/A
enaAll	Enables the LTPS and voice gateway. See *IP Line Fundamentals (NN43001-500)*.	N/A

Command	Description	Element Manager
`disServices`	Gracefully switches the registered resources to the other services. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	Mam
`forcedisServices`	Forces the server to switch the registered resources to the other services in the same node. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	Mam
`enlServices`	Enables all services to accept registration of resources. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	Mam
`servicesStatusShow`	Displays the status of services. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	Mam
`soCmdStatusShow`	Displays the status of Service Switch-Over commands.	N/A
`soHelpMenu`	Displays all the commands that can be used for Services Switch-Over. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`lossPlanPrt`	Displays the offsets and current values for the handset, headset, and handsfree RLR and SLR. See *IP Line Fundamentals (NN43001-500)*.	N/A

ncs commands: Network Connection Service module

The following table lists the OAM Network Connection Service (NCS) module commands in the ncs command group.

Table 20
OAM ncs commands

Command	Description	Element Manager
`tpsARTrace`	Enables tracing for the Network Connection Server (NCS). See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	N/A
`tpsARTraceOff`	Disables tracing for the Network Connection Server (NCS). See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	N/A

Command	Description	Element Manager
tpsARTraceAllOff	Turns off the trace for all tpsAR trace identifiers. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
tpsAROutput	Modifies the destination for the traced output of the NCS. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	N/A
tpsARTraceSettings	Displays the trace settings and items being traced for the NCS trace. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	N/A
tpsARTraceHelp	Displays help on the tpsARTrace commands. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A

npm commands: Network Protocol Module

The following table lists the OAM Network Protocol Module (NPM) commands in the npm command group.

Table 21
OAM npm commands

Command	Description	Element Manager
H323GwRegTrace	Turns on or off the traces for H.323 Registration at the gateway. See *IP Peer Networking Installation and Commissioning (NN43001-313)*	N/A
H323CallTrace	Traces H.323 incoming and outgoing call setup messages for selected channels. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
H323TraceShow	Displays input and output display settings for **H323CallTrace** and **H323Output** commands. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
H323Output	Directs H323Trace output to TTY or syslog file. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
H323GwShow	Displays information about the H.323 Network Protocol Module. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A

nrsDB commands: Network Routing Service

The following table lists the OAM Network Routing Service (NRS) commands in the nrsDB command group.

Table 22
OAM nrsDB commands

Command	Description	Element Manager
nrsGWEndpointShow	Lists all the endpoints in the database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
nrsUserEPShow	Lists all the NRS users with corresponding IP addresses. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
nrsCollaboratingServerShow	Lists all the Collaborating Servers in the database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
nrsL0DomainShow	Lists all the Level 0 domains in the database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
nrsL1DomainShow	Lists all the Level 1 domains in the database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
nrsRoutingEntryShow	Lists all the Routing Entries in the database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
nrsServiceDomainShow	Lists all the Service Domains in the database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
nrsCollaboratingServerQuery	Queries one Collaborating Server from the database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
nrsGWEndpointQuery	Queries one Endpoint from the database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
nrsUserEPQuery	Queries an NRS endpoint with IP and protocol information. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
nrsL0DomainQuery	Queries one L 0 Domain from the database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
nrsL1DomainQuery	Queries one L 1 Domain from the database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A

Command	Description	Element Manager
`nrsServiceDomainQuery`	Queries one Service Domain from the database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`nrsDefaultRouteQuery`	Displays all the default routes which belong to an endpoint in the database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`nrsDBShow`	DIsplays the state of the Primary and Alternate NRS database, and the local NRS database. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`nrsDBSyncForce`	Force synchronization of the active NRS database with the Alternate or Failsafe NRS database.	N/A

nrsomm commands: NRS operational measurements

The following table lists the OAM NRS operational measurements commands in the nrsomm command group.

Table 23
OAM nrsomm commands

Command	Description	Element Manager
`NrsOmmShow`	Displays the SIP and H.323 NRS statistics for the current hour. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`NrsOmmAvShow`	Displays the SIP and H.323 NRS total and average statistics for the last seven days. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`nrsDBStateShow`	Show the internal state of the NRS database.	N/A

pbxlink commands: PBX link

The following table lists the OAM PBX link commands in the pbxlink command group.

Table 24
OAM pbxlink commands

Command	Description	Element Manager
`pbxLinkShow`	Displays PBX link status. See *IP Line Fundamentals (NN43001-500)*.	pbxLink

securityShell commands: Security shell

The following table lists the OAM Security shell commands in the securityShell command group.

Table 25
OAM securityShell commands

Command	Description	Element Manager
`disInsecureShells`	Disables all insecure shells in the system, including TELNET and RLOGIN sessions. See *Security Management (NN43001-604)*.	See Note.
`enlInsecureShells`	Enables all insecure shells in the system, including TELNET and RLOGIN sessions. See *Security Management (NN43001-604)*.	See Note.
`statInsecureShells`	Displays whether insecure shell access is enabled or disabled. See *Security Management (NN43001-604)*.	See Note.
`disSecureShells`	Disables all secure shells in the system, including SSH, SFTP, and SCP sessions.	N/A
`enlSecureShells`	Enables all secure shells, including SSH, SFTP, and SCP sessions.	N/A
`statSecureShells`	Shows whether secure shell access is enabled or disabled.	N/A

Note: These commands are not accessible from Element Manager as described in "Element Manager" (page 255). They are available in Element Manager at **Security > Login Options > Shell Login**. Refer to *Security Management (NN43001-604)* for more information.

sipcti commands: SIP CTI module commands

The following table lists the OAM sipcti commands in the OAM sipcti command group.

Table 26
OAM sipcti commands

Command	Description	Element Manager
`SIPCTISessionShow`	Shows the total number of TR87 SIP sessions.	N/A
`SIPCTIClientShow`	Shows information about all the associated soft clients.	N/A
`SIPCTIShow`	Shows SIP CTI application status and configuration.	N/A
`SIPCTIStop`	Deacquire one or all AST DN(s) and remove associated SIP CTI sessions.	N/A

Command	Description	Element Manager
SIPCTITraceLevel	Sets the MessageTrace Level output to TR87 body only or Detailed format.	N/A
SIPCTITraceShow	Prints SIPCTI trace settings.	N/A
SIPCTIOutput	Redirect the SIP CTI trace to a specific output destination.	N/A
SIPCTITrace	Trace incoming and outgoing TR87 SIP messages.	N/A
SIPCTILdapForceUpdate	Update LDAP cache from LDAP server.	N/A
SIPCTILdapSetPageSize	Set LDAP page size for LDAP caching.	N/A

sipctiomm commands: SIP CTI OMM commands

The following table lists the OAM sipctiomm commands in the OAM sipctiomm command group.

Table 27
OAM sipctiomm commands

Command	Description	Element Manager
SipCtiOmmShow	Show the current hour count statistics for SIP CTI.	N/A

sipnpm commands: SIP Network Protocol Module

The following table lists the OAM SIP Network Protocol Module commands in the sipnpm command group.

Table 28
OAM sipnpm commands

Command	Description	Element Manager
SIPGwShow	Displays SIP Virtual Trunk settings. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	Sip
SIPCallTrace	Traces messages sent through SIP channels. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
SIPTraceShow	Displays the SIP trace settings and all active traces for the SIP call trace tool. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A

Command	Description	Element Manager
SIPOutput	Specifies where the output for the trace tool is to be directed. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
SIPTraceLevel	Sets the SIPCallTrace output to Summary or Detailed format. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
SIPGwRegTrace	Turns on or off the traces for SIP Registration at the signaling gateway. See *IP Peer Networking Installation and Commissioning (NN43001-313)*	N/A

system commands: system administration commands

The following table lists the OAM system administration commands in the system command group.

Table 29
OAM system commands

Command	Description	Element Manager
routeShow	Displays host and network routing tables. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	System
routeAdd	Adds a route to the routing tables. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	N/A
routeDelete	Deletes a route from the routing tables. See *IP Trunk Installation and Commissioning (NN43001-563)*.	N/A
ping	Tests that a remote site is reachable. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	N/A
who	Displays all active User IDs and ports.	N/A
arpShow	Displays entries in the system ARP table.	N/A
arpFlush	Flushes all the entries in the system ARP table.	N/A
diskSizeShow	Displays the total physical size of the hard disk.	N/A
memSizeShow	Displays the total physical size of the memory.	N/A
swVersionShow	Displays software version. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	N/A
date	Displays the system date and time, and prompts to configure new system date and time.	N/A

Command	Description	Element Manager
`uptime`	Displays the amount of time lapsed since the last system reboot.	N/A
`stty [speed]`	Sets console speed. Available speeds are 9600, 19200, 38400, and 115200.	N/A
`consoleShow`	Displays console speed.	N/A
`ppp [-l localAdd -r remoteAdd -o optionsFile -f]`	Initiates a PPP connection with options. Where: • localAdd is the local IP address. Default is 137.135.x.1. • remoteAdd is the remote IP address. Default is 137.135.x.2. • optionsFile is the full path to the options file. • -f signifies no hardware flow control signals during PPP connection.	N/A
`sysResShow`	Displays the current usage of File Descriptors (FD) on the system.	N/A
`cppmLoopChange`	Changes the IPMG loop number location (Nortel CP PM Signaling Server only).	N/A
`cppmShelfChange`	Changes the IPMG shelf number location (Nortel CP PM Signaling Server only).	N/A
`cppmLocationShow`	Displays the loop and shelf location (Nortel CP PM Signaling Server only).	N/A

tps commands: TPS module

The following table lists the OAM TPS module commands in the tps command group.

Table 30
OAM tps commands

Command	Description	Element Manager
`disiTPS`	Disables TPS service when idle. See *IP Line Fundamentals (NN43001-500)*.	N/A

Command	Description	Element Manager
enaTPS	Enables TPS service. See *IP Line Fundamentals (NN43001-500)*.	N/A
tpsShow	Displays TPS information.	N/A
disTPS	Causes the Line TPS to gracefully switch the registered telephones to the other cards located in the same node. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	Tps
forcedisTPS	Forces all registered Line TPS to unregister from the local server. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	Tps
enlTPS	Causes Line TPS application to be enabled and to accept IP Telephone registrations. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	Tps
loadBalance	Causes Line TPS application to attempt to balance the registration load of sets between this card and the rest of the node components. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	Tps
UKLossPlanSet	Sets IP Phone's loss plan to UK-specific values. See *IP Line Fundamentals (NN43001-500)*.	N/A
lossPlanSet	Adjusts the levels of a given transducer by the entered RLR and SLR offsets. See *IP Line Fundamentals (NN43001-500)*.	N/A
UKLossPlanClr	Sets IP Phone's loss plan to default values. See *IP Line Fundamentals (NN43001-500)*.	N/A
lossPlanClr	Sets IP Phone's loss plan to default values. See *IP Line Fundamentals (NN43001-500)*.	N/A
echoServerShow	Displays information about the Echo Servers used by this system. See *IP Line Fundamentals (NN43001-500)*.	Tps

trace commands: General trace tools

The following table lists the OAM General trace tools in the trace command group.

Table 31
OAM trace commands

Command	Description	Element Manager
traceAllOff	Disables the trace facilities from writing to the TTY, SYSLOG, and specified files. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	N/A
traceAllOn	Enables the trace facilities to resume writing to the TTY, SYSLOG, and/or specified files. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	N/A
tracePrintOff	Disables the trace facilities from writing to the TTY. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	N/A
tracePrintOn	Enables the trace facilities to resume writing to the TTY. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	N/A
traceFileOff	Disables the trace facilities from writing to the SYSLOG and specified files. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	N/A
traceFileOn	Enables the trace facilities to resume writing to the SYSLOG and/or specified files. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	N/A
traceShow	Displays the names of active traces in the system. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Line Fundamentals (NN43001-500)*.	N/A

uipc commands: Universal ISDN Protocol module

The following table lists the OAM Universal ISDN Protocol module commands in the uipc command group.

Table 32
OAM uipc commands

Command	Description	Element Manager
DCHmenu	Displays a menu of DCH diagnostic tools. See *IP Peer Networking Installation and Commissioning (NN43001-313)* or *IP Trunk Installation and Commissioning (NN43001-563)*.	N/A

ums commands: UMS module

The following table lists the OAM UMS module commands in the ums command group.

Table 33
OAM ums commands

Command	Description	Element Manager
firmwareFileGet	Initiates a firmware download from a specified FTP server. See *IP Line Fundamentals (NN43001-500)*.	N/A
firmwareFileGetI2004	Initiates a firmware download for an IP Phone 2004 from a specified FTP server. Replaced by **firmwareFileGet**. See *IP Line Fundamentals (NN43001-500)*.	N/A
firmwareFileGetI2002	Initiates a firmware download for an IP Phone 2002 from a specified FTP server. Replaced by **firmwareFileGet**. See *IP Line Fundamentals (NN43001-500)*.	N/A
umsPolicyShow	Displays the current upgrade policy. See *IP Line Fundamentals (NN43001-500)*.	Ums
umsUpgradeAll	Upgrades all registered sets according to policy and firmware file. See *IP Line Fundamentals (NN43001-500)*.	N/A
umsUpgradeTimerShow	Displays the upgrade schedule. See *IP Line Fundamentals (NN43001-500)*.	N/A
umsUpgradeTimerCancel	Cancels the scheduled upgrade. See *IP Line Fundamentals (NN43001-500)*.	N/A

usi commands: RUDP timeout and retry commands

The following table lists the OAM RUDP timeout and retry commands in the usi command group.

Table 34
OAM usi commands

Command	Description	Element Manager
`usiSetPhoneRudpRetries`	Sets the RUDP Max Retries count for IP Phones. See *IP Line Fundamentals (NN43001-500)*.	N/A
`usiGetPhoneRudpRetries`	Displays the RUDP Max Retries count for IP Phones. See *IP Line Fundamentals (NN43001-500)*.	N/A
`usiSetPhoneRudpTimeout`	Sets the RUDP Timeout value (in ms) for IP Phones. See *IP Line Fundamentals (NN43001-500)*.	N/A
`usiGetPhoneRudpTimeout`	Displays the RUDP Timeout value (in ms) for IP Phones. See *IP Line Fundamentals (NN43001-500)*.	N/A

vte commands: Virtual Terminal Emulator

The following table lists the OAM Virtual Terminal Emulator commands in the vte command group.

Table 35
OAM vte commands

Command	Description	Element Manager
`unpackVTHelp`	Unpacks Virtual Terminal Emulator help files. See "Unpack Help files for Virtual Terminal Emulator" (page 146).	N/A

vtrk commands: Virtual Trunk module

The following table lists the OAM Virtual Trunk module commands in the vtrk command group.

Table 36
OAM vtrk commands

Command	Description	Element Manager
`vtrkShow`	Displays information about the Virtual Trunk channels. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	Vtrk

Command	Description	Element Manager
disVTRK	Gracefully switches the registered Virtual Trunks to another Signaling Server in the same node. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	Vtrk
forcedisVTRK	Forces all registered Virtual Trunks to unregister from the local server. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	Vtrk
enlVTRK	Enables the Virtual Trunk application to accept Virtual Trunk registrations. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	Vtrk
vtrkNetMonShow	Print out the current list of monitored IP addresses and their status. See *IP Peer Networking Installation and Commissioning (NN43001-313)*	N/A

Level Two (PDT) CLI commands

All Level One Signaling Server CLI commands are also available at the PDT shell. This section lists additional CLI commands and command groups that are available at the PDT Shell. These additional CLI commands are Level Two Signaling Server CLI commands, or expert-level commands. The prompt for each command is **pdt>**.

To access the PDT shell from the OAM Shell, hold down CTRL and type PDT at the **oam>** prompt. The PDT shell can only be accessed if your password is configured for PDT access.

Command groups

Table 37 "PDT CLI command groups" (page 281) lists the CLI command groups that contain Level Two CLI Commands. Command groups available only in PDT are shown in *italics*. The PDT commands in each group are described in the following sections.

Table 37
PDT CLI command groups

Command group	Description	PDT Commands
Accounts	Standalone NRS commands	Table 38 "PDT Accounts commands" (page 282)
disk	File system maintenance and diagnostics.	Table 39 "PDT disk commands" (page 283)

Command group	Description	PDT Commands
rdtools	rd tools commands	Table 40 "PDT rdtools commands" (page 283)
nrsDB	Network Routing Service commands	Table 41 "PDT nrsDB commands" (page 284)
sipnpm	SIP Network Control Module commands	Table 42 "PDT sipnpm commands" (page 285)
system	System administration commands	Table 43 "PDT system commands" (page 286)
ums	UMS module commands.	Table 44 "PDT ums commands" (page 289)

Accounts commands: user account administration commands

The following table lists the commands for an NRS running on a Standalone Signaling Server in the PDT Accounts command group.

Table 38
PDT Accounts commands

Command	Description	Element Manager
`adminUserPasswordChange`	Changes administrator-level user password for an NRS running on a Standalone Signaling Server. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`adminUserCreate`	Creates an administrator-level user of an NRS running on a Standalone Signaling Server. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`adminUserDelete`	Deletes an administrator-level user of an NRS running on a Standalone Signaling Server. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
`adminAccountShow`	Displays User ID and access privileges for all users of an NRS running on a Standalone Signaling Server. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A

disk commands: file system maintenance and diagnostics

The following table lists the PDT file system maintenance and diagnostic command in the disk command group.

Table 39
PDT disk commands

Command	Description	Element Manager
`fsck [m] [devname]`	Checks the integrity of the file system on the specified device. Errors are repaired unless the mount flag is specified. Where: • m is the mount flag. • devname is the device to check.	N/A

rdtools commands: rd tools

The following table lists the PDT rd tools commands in the rdtools command group.

Table 40
PDT rdtools commands

Command	Description	Element Manager
`rdopen [filename]`	Opens a report log file. Where [filename] is the name of the report file to be opened.	N/A
`rdgo [N]`	Goes to a specific record. Where [N] is the absolute record number.	N/A
`rd [S] [R]`	Displays a specified number of records starting at a specified point. Where: • [S] is the number of steps to traverse to the starting point. • [R] is the number of records to display. Both [S] and [R] can be negative.	N/A

Command	Description	Element Manager
`rds [S] [R]`	Displays a specified number of records, with a symbolic dump, starting at a specified point. Where: • [S] is the number of steps to traverse to the starting point. • [R] is the number of records to display. Both [S] and [R] can be negative.	N/A
`rdshow`	Displays general information about the current log file and the current rd settings.	N/A
`rdall`	Displays all records.	N/A
`rdtail [N]`	Displays the specified number of newest records. Where [N] is the number of records to display.	N/A
`rdhead [N]`	Displays the specified number of oldest records. Where [N] is the number of records to display.	N/A
`rdnext`	Opens the next log file.	N/A
`rdprev`	Opens the previous log file.	N/A
`rdsconvert [filename]`	Converts a log file to text. Where [filename] is the name of the log file to be converted.	N/A

nrsDB commands: Network Routing Service

The following table lists the PDT Network Routing Service (NRS) commands in the nrsDB command group. These commands are in addition to the OAM commands listed in Table 22 "OAM nrsDB commands" (page 271).

Table 41
PDT nrsDB commands

Command	Description	Element Manager
`nrsDBStateShow`	Show the internal state of the NRS database.	N/A

Note: The database cutover, revert, commit, and rollback commands are not available in Element Manager as described in "Element Manager" (page 255). The same functionality is available in NRS Manager at **Tools > Database Actions**. See *Network Routing Service Installation and Commissioning NN43001-564)* for details.

sipnpm commands: SIP Network Protocol Module

The following table lists the PDT SIP Network Protocol Module commands in the sipnpm command group. These commands are in addition to the OAM commands listed in Table 28 "OAM sipnpm commands" (page 274).

Table 42
PDT sipnpm commands

Command	Description	Element Manager
SIPTLSConfigShow	Show the TLS parameter details.	N/A
SIPTLSSessionShow	Show the TLS session details.	N/A
SIPMessageTrace	Set filters to turn the message trace ON or OFF.	N/A
sip2IsdnSet	Changes the SIP status code to the ISDN cause code mapping. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
sip2IsdnReset	Resets a single SIP status code to the default ISDN cause code mapping. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
sip2IsdnResetAll	Resets all SIP status codes to the default ISDN cause code mappings. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
sip2IsdnShow	Shows one specific SIP status code to ISDN cause code mapping. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
sip2IsdnShowAll	Shows all mappings from SIP status code to ISDN cause code. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
isdn2SipSet	Changes the ISDN cause code to the SIP status code mapping. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
isdn2SipReset	Resets a single ISDN cause code to the default SIP status code mapping. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
isdn2SipResetAll	Resets all the ISDN cause codes to the default SIP status code mappings. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A

Command	Description	Element Manager
isdn2SipShow	Shows one specific ISDN cause code to SIP status code mapping. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A
isdn2SipShowAll	Shows all mappings from ISDN cause codes to SIP status codes. See *IP Peer Networking Installation and Commissioning (NN43001-313)*.	N/A

system commands: System administration

The following table lists the PDT system administration commands in the system command group. These commands are in addition to the OAM commands listed in Table 29 "OAM system commands" (page 275).

Table 43
PDT system commands

Command	Description	Element Manager
lkup	Look up a symbol.	N/A
devs	Displays list of the devices.	N/A
echo	Echoes the input.	N/A
hosts	Displays list of hosts.	N/A
memShow	Displays memory usage.	N/A
ti [name | taskID]	Displays task information for task specified by name or task ID. Where: • name is the task name. • taskID is the task ID.	N/A
i	Displays task information. See *IP Line Fundamentals (NN43001-500)*.	System
version	Displays vxWorks™ version, date of build, and other information.	N/A
x [name]	Executes a function. Where name is the name of the function.	N/A

Command	Description	Element Manager
ifShow	Displays the attached network interfaces. See *IP Trunk Installation and Commissioning (NN43001-563)* or *IP Line Fundamentals (NN43001-500)*.	System
reboot [-1]	Warm restarts the system. If -1 specified, cold restarts the system.	N/A
ls [path]	Displays the contents of a directory. Where path is the path name of the directory. If path is not specified, the contents of the current directory are specified.	N/A
ll [path]	Displays a long list of the contents of a directory. Where path is the path name of the directory. If path is not specified, the contents of the current directory are specified.	N/A
cd [path]	Changes the default directory. Where path is the path and name of the new directory. The path of the new directory can be specified as a relative path.	N/A
pwd	Displays the current default directory.	N/A
copy [input output]	Copies from one file to another file until an end-of-file (CTRL+d) is reached. Where: • input is the name of the file to be copied from. If NULL, stdin is used. • output is the name of the new or destination file to be copied to. If NULL, stdout is used.	N/A

Command	Description	Element Manager
rename [file1 file2]	Renames one file or moves one file to another. Where: • file1 is the file to be renamed or moved. • file2 is the new or destination filename.	N/A
remove [file]	Removes a file. Where file is the name of the file to be removed.	N/A
moduleShow	Displays the list of all loaded modules.	N/A
inetstatShow	Displays all the active connections for the IP sockets.	N/A
tcpstatShow	Displays statistics for the TCP protocol.	N/A
udpstatShow	Displays statistics for the UDP protocol.	N/A
syslogShow	Displays the log level for all tasks.	N/A
syslogLevelSet [tid | name level] Sets the log level for a task, given by task ID or task name. Where: • tid is the task ID. • name is the task name. • level is the log level in the range 0-7.		N/A
hwdShow	Displays the status of the system hardware watchdog timer.	N/A
uudecode	Decode data that were encoded with **uuencode**	N/A
arpPrivLogDisable	Disable the Arp Warning messages report (when ELAN and TLAN are not isolated).	N/A
arpPrivLogEnable	Enable the Arp Warning messages report.	N/A

ums commands : UMS module

The following table lists the UMS module commands in the ums command group that are available only at the PDT access level. These commands are in addition to the OAM access level ums commands listed in Table 33 "OAM ums commands" (page 279)

Table 44
PDT ums commands

Command	Description	Element Manager
`umsSetPolicy`	Assigns the policy for the particular firmware. See *IP Line Fundamentals (NN43001-500)*.	N/A
`umsSetPolicyUpgradeType`	Set upgrade type for policy.	N/A
`umsSetPolicyRetries`	Sets the number of retries for the policy. See *IP Line Fundamentals (NN43001-500)*.	N/A
`umsSetPolicyProtocol`	Sets the protocol for the policy. See *IP Line Fundamentals (NN43001-500)*.	N/A
`umsCreatePolicy`	Creates a firmware policy. See *IP Line Fundamentals (NN43001-500)*.	N/A
`umsDeletePolicy`	Deletes a firmware policy. See *IP Line Fundamentals (NN43001-500)*.	N/A

Signaling Server Maintenance

Contents

This chapter contains information on the following topics:

Introduction

This section describes various topics related to the operational maintenance of a Signaling Server. These topics include:

- connect and configure a maintenance terminal
- logging on to the Signaling Server from the maintenance terminal
- setting the Signaling Server port speed
- replacing a defective Signaling Server
- using the Tools menu of the Signaling Server Software Installation Tool

Configure a maintenance terminal

This section contains detailed instructions for configuring the following types of maintenance terminals:

- HP700/32

- VT420
- VT220

A maintenance terminal is required for the installation, configuration and maintenance of a Signaling Server. To connect a maintenance terminal to your Signaling Server, refer to the appropriate section of "Hardware connection" (page 77).

After the maintenance terminal is connected to the Signaling Server, it must be properly configured.

ATTENTION

To avoid data loss, do not configure a maintenance terminal during data transmission.

Use the following procedure to configure a maintenance terminal.

Procedure 50

Configuring a maintenance terminal

Step	Action
1	Turn on the power for the maintenance terminal.
2	Enter setup mode by pressing the **SETUP** key on the top row of the special function keys. A maintenance terminal setup parameters screen appears that contains the existing setup values. The terminal setup parameters screen is specific to the type of maintenance terminal you are using.
3	Change maintenance terminal setup parameters as necessary. Refer to "Maintenance terminal setup parameters" (page 292) for the setup parameters and instructions.
4	To save changes, return to the **General setup** screen, move the cursor to the **Saved** field, and press **Enter**.

—End—

Maintenance terminal setup parameters

This section contains all of the setup parameters necessary to configure each of the supported types of maintenance terminals supported on a Signaling Server.

- HP700/32: see Figure 226 "HP700/32 setup values" (page 294)

- VT420: see Figure 227 "VT420 setup values" (page 295)
- VT220: see Figure 228 "VT220 setup values" (page 296)

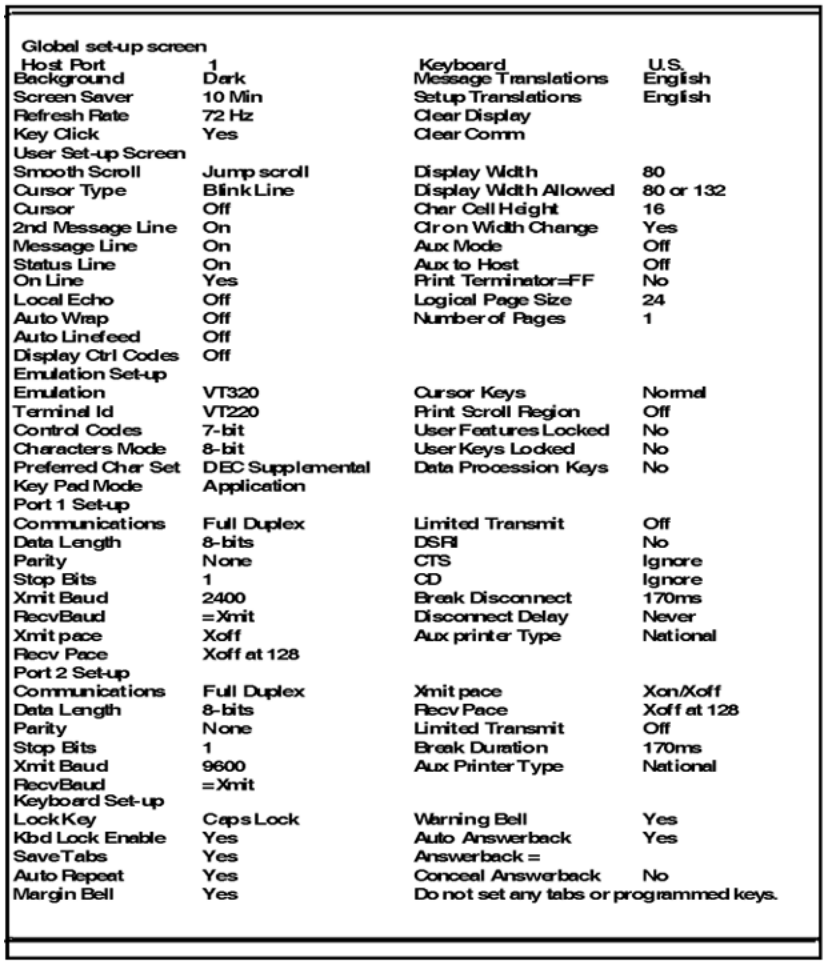
Use the keys in the following table to view and change setup values.

Table 45
SDI key function

Key	Function
Arrow	Move from field to field
Enter	Scroll through possible values or invoke an action (action depends on type of field)
Next Screen	Move to the next setup screen
Prev Screen	Move to the previous setup screen

The following table identifies all set-up values for an HP700/32 maintenance terminal.

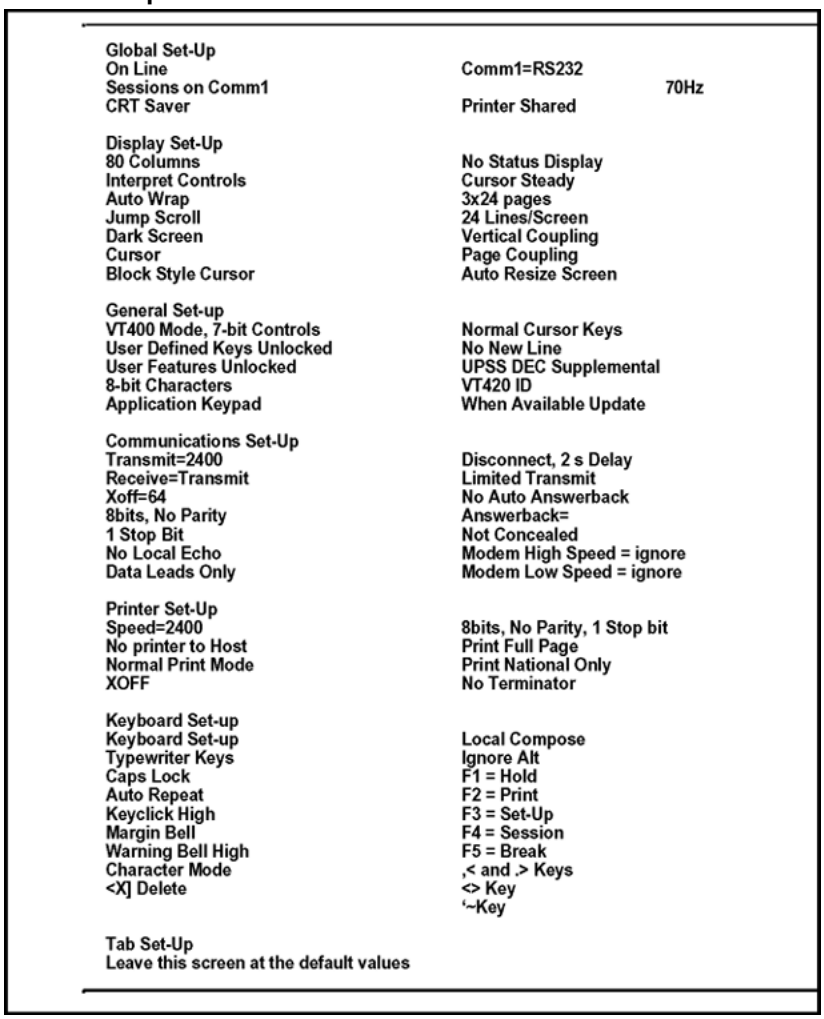
Figure 226
HP700/32 setup values



Global set-up screen			
Host Port	1	Keyboard	U.S.
Background	Dark	Message Translations	English
Screen Saver	10 Min	Setup Translations	English
Refresh Rate	72 Hz	Clear Display	
Key Click	Yes	Clear Comm	
User Set-up Screen			
Smooth Scroll	Jump scroll	Display Width	80
Cursor Type	Blink Line	Display Width Allowed	80 or 132
Cursor	Off	Char Cell Height	16
2nd Message Line	On	Ctr on Width Change	Yes
Message Line	On	Aux Mode	Off
Status Line	On	Aux to Host	Off
On Line	Yes	Print Terminator=FF	No
Local Echo	Off	Logical Page Size	24
Auto Wrap	Off	Number of Pages	1
Auto Linefeed	Off		
Display Ctrl Codes	Off		
Emulation Set-up			
Emulation	VT320	Cursor Keys	Normal
Terminal Id	VT220	Print Scroll Region	Off
Control Codes	7-bit	User Features Locked	No
Characters Mode	8-bit	User Keys Locked	No
Preferred Char Set	DEC Supplemental	Data Procession Keys	No
Key Pad Mode	Application		
Port 1 Set-up			
Communications	Full Duplex	Limited Transmit	Off
Data Length	8-bits	DSRI	No
Parity	None	CTS	Ignore
Stop Bits	1	CD	Ignore
Xmit Baud	2400	Break Disconnect	170ms
RecvBaud	=Xmit	Disconnect Delay	Never
Xmit pace	Xoff	Aux printer Type	National
Recv Pace	Xoff at 128		
Port 2 Set-up			
Communications	Full Duplex	Xmit pace	Xon/Xoff
Data Length	8-bits	Recv Pace	Xoff at 128
Parity	None	Limited Transmit	Off
Stop Bits	1	Break Duration	170ms
Xmit Baud	9600	Aux Printer Type	National
RecvBaud	=Xmit		
Keyboard Set-up			
Lock Key	Caps Lock	Warning Bell	Yes
Kbd Lock Enable	Yes	Auto Answerback	Yes
Save Tabs	Yes	Answerback =	
Auto Repeat	Yes	Conceal Answerback	No
Margin Bell	Yes	Do not set any tabs or programmed keys.	

The following table identifies all set-up values for a VT420 maintenance terminal.

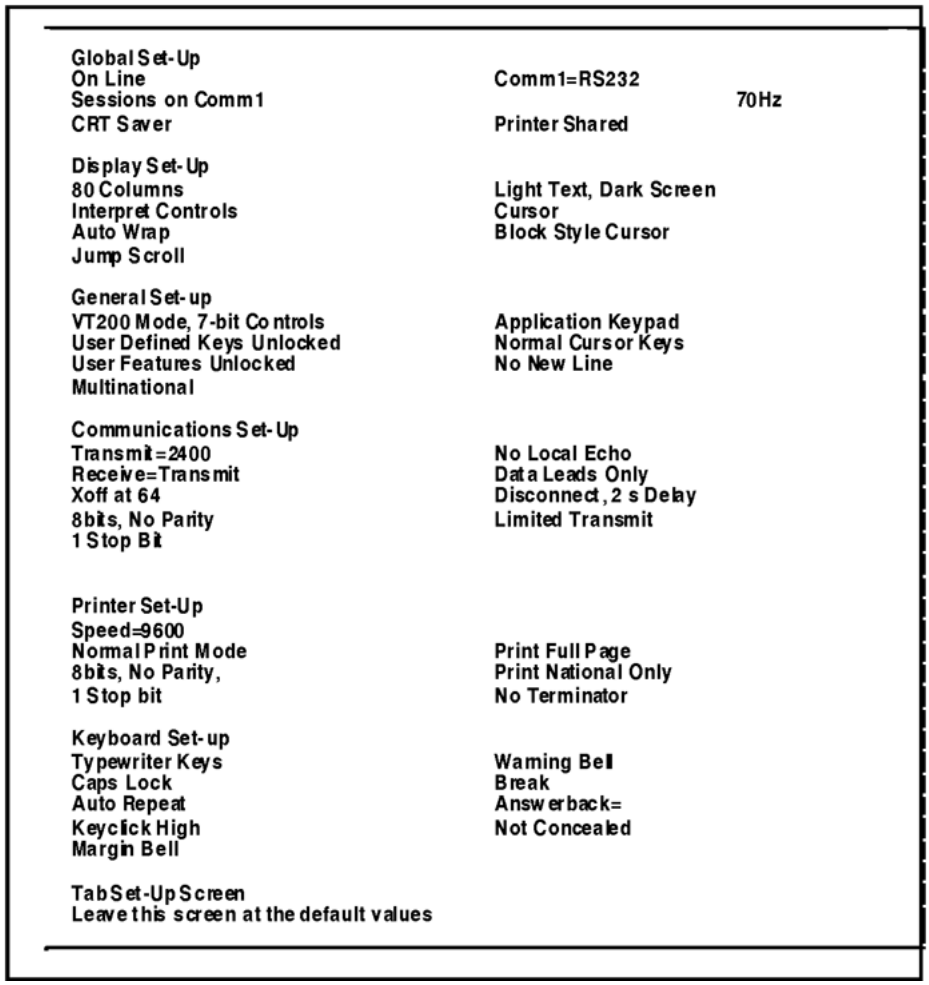
Figure 227
VT420 setup values



Global Set-Up	
On Line	Comm1=RS232
Sessions on Comm1	70Hz
CRT Saver	Printer Shared
Display Set-Up	
80 Columns	No Status Display
Interpret Controls	Cursor Steady
Auto Wrap	3x24 pages
Jump Scroll	24 Lines/Screen
Dark Screen	Vertical Coupling
Cursor	Page Coupling
Block Style Cursor	Auto Resize Screen
General Set-up	
VT400 Mode, 7-bit Controls	Normal Cursor Keys
User Defined Keys Unlocked	No New Line
User Features Unlocked	UPSS DEC Supplemental
8-bit Characters	VT420 ID
Application Keypad	When Available Update
Communications Set-Up	
Transmit=2400	Disconnect, 2 s Delay
Receive=Transmit	Limited Transmit
Xoff=64	No Auto Answerback
8bits, No Parity	Answerback=
1 Stop Bit	Not Concealed
No Local Echo	Modem High Speed = ignore
Data Leads Only	Modem Low Speed = ignore
Printer Set-Up	
Speed=2400	8bits, No Parity, 1 Stop bit
No printer to Host	Print Full Page
Normal Print Mode	Print National Only
XOFF	No Terminator
Keyboard Set-up	
Keyboard Set-up	Local Compose
Typewriter Keys	Ignore Alt
Caps Lock	F1 = Hold
Auto Repeat	F2 = Print
Keyclick High	F3 = Set-Up
Margin Bell	F4 = Session
Warning Bell High	F5 = Break
Character Mode	,< and .> Keys
<X] Delete	<> Key
	'~Key
Tab Set-Up	
Leave this screen at the default values	

The following table identifies all set-up values for a VT220 maintenance terminal.

Figure 228
VT220 setup values



Log on to the Signaling Server

To access the Signaling Server from a maintenance terminal, you must log on to the VxWorks™ shell using Procedure 22 "Logging on to the Signaling Server" (page 147). From this shell, you can change the Signaling Server port speed (see Procedure 54 "Changing the Signaling Server port speed" (page 303)) and run the commands described in "Command Line Interface (CLI) commands" (page 253).

Signaling Server Tools Menu

The Signaling Server Tools Menu is accessed through the Signaling Server Software Installation Tool Main Menu. All models of Signaling Server available in CS 1000 Release 5.0 share a common set of tools.

Use the following procedure to access the Signaling Server Tools Menu.

Procedure 51
Accessing the Signaling Server Tools Menu

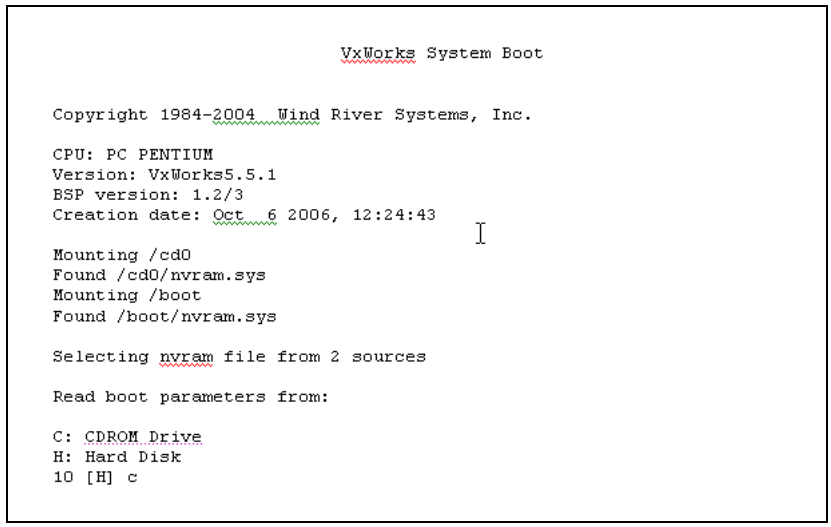
Step	Action

1 Trigger the Signaling Server Software Installation Tool.

For Nortel CP PM Signaling Servers:

- If you don't have a Signaling Server Software CF Card
  - — press the **RST** button on the faceplate of the Signaling Server to trigger a cold boot. The VxWorks™ boot banner screen appears.

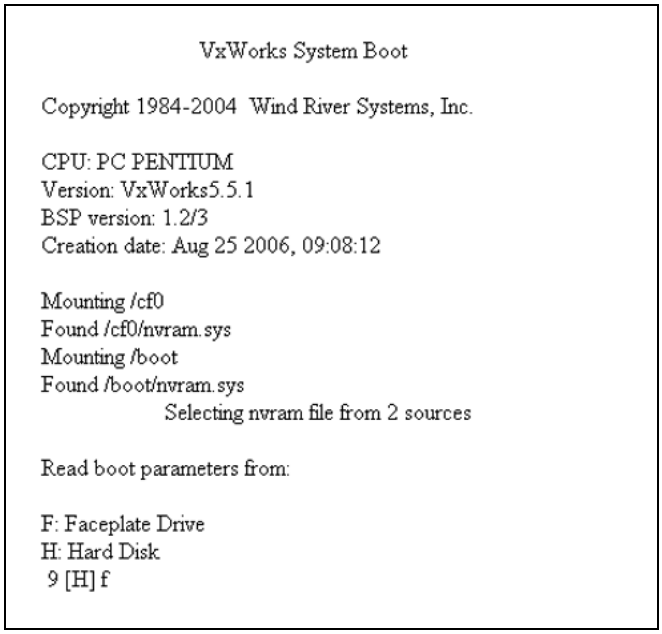
    Figure 229
    VxWorks system boot banner

  - — enter **Ctrl+B** at the countdown prompt to stop the boot sequence
  - — enter **c** to change the boot parameters
  - — press **<CR>** until you reach the "flags" parameter
  - — update the contents of the "flags" parameter with the value **0x40000**
  - — press **<CR>** until the VxWorks™ system boot banner screen re-appears.
  - — enter **@** to continue the boot sequence

- If you do have a Signaling Server Software CF card:
  - — insert the Signaling Server Software CF Card into the faceplate CFdrive

— press the **RST** button on the faceplate of the Signaling Server to trigger a cold boot of the Signaling Server. The VxWorks™ system boot banner screen appears.

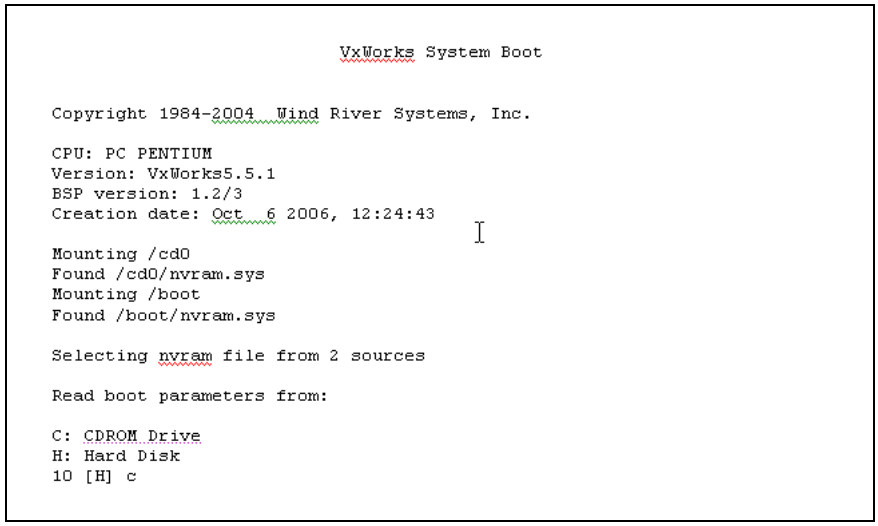


— enter **f** at the countdown prompt to trigger the Signaling Server to boot from the faceplate CF drive.

For IBM X306m, HP DL320-G4 and Nortel ISP1100 Signaling Servers:

- Insert the Signaling Server Software CD into the CD drive of the Signaling Server.
- Press the **RST** button on the front of the Signaling Server to trigger a cold boot. The VxWorks™ system boot banner screen appears.

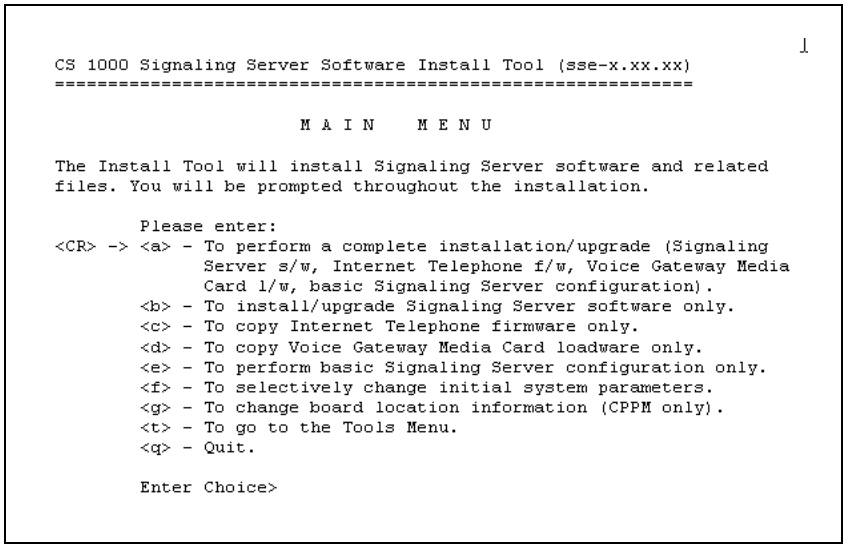
Figure 230
VxWorks system boot banner



- Enter **c** at the countdown prompt to trigger the Signaling Server to boot from the CD drive.

The Installation Tool Main Menu appears.

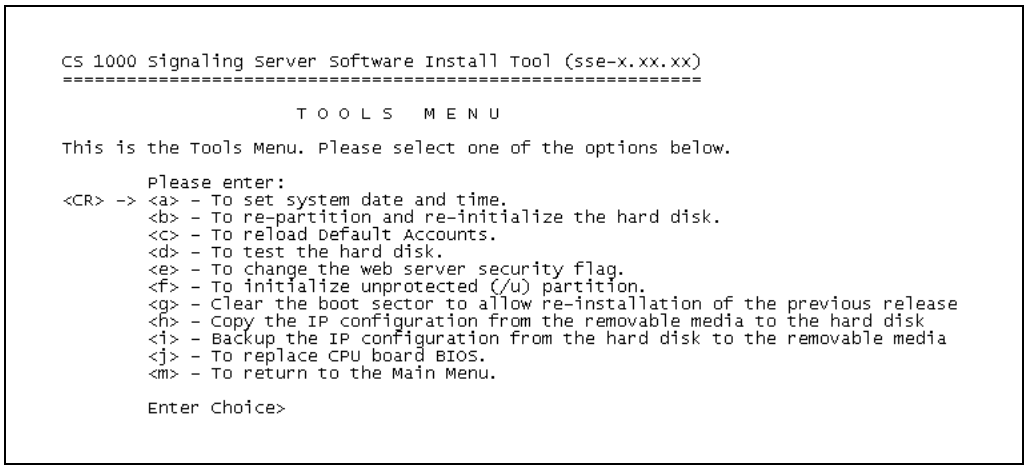
Figure 231
Installation Tool Main Menu



2 Enter **t** to access the Tools Menu.

The Tools Menu appears.

Figure 232
Tools Menu



—End—

The Tools Menu provides the following tools:

- **a** — configure the date and time
- **b** — re-partition and re-initialize the hard disk

WARNING
IMPORTANT!
This option results in the loss of all Signaling Server software installed on the hard drive and a reboot of the Signaling Server.

WARNING
IMPORTANT!
Do not choose this option for a Nortel CP PM Signaling Server. The Nortel CP PM Signaling Server is delivered with CS 1000 Release 5.0 software pre-loaded onto the hard drive. It has no CD-ROM drive and thus, no way to reinstall CS 1000 Release 5.0 software.

For Nortel ISP1100, IBM X306m or HP DL320-G4 Signaling Servers, leave the Signaling Server Software CD in the CD-ROM drive so that the Signaling Server Software Installation Tool is triggered during reboot and the Signaling Server software can be re-installed (see Procedure 19 "Installing Signaling Server software " (page 113)).

- **c** — reset the Administrator logon and password.

- **d** — test the hard disk on the Signaling Server.
  - This test can take a considerable amount of time depending on the size of the hard disk. Expect approximately 30 minutes per 10 GB of size.
- **e** — change the web server security flag (see "Restricting web access to the ELAN subnet" (page 246)).
- **f** — initialize the unprotected partition (/u).
- **g** — clear the boot sector before reinstalling the previous software release (see "Re-install the previous software release" (page 197))
- **h** — copy the IP configuration from the removable media device to the hard drive (see "Restoring the IP configuration" (page 302))
- **i** — back up the IP configuration from the hard drive to the removable media device (see "Backing up the IP configuration" (page 301))
- **j** — change the CPU board BIOS
  - this option is only applicable to Nortel CP PM Signaling Servers
  - option will be blocked from use from all other Signaling Server platforms
- **m** — return to the Signaling Server Installation Tool Main Menu.

Backing up and restoring the IP configuration

This section contains information and procedures for backing up and restoring the IP configuration data of a Signaling Server. The IP configuration data is backed up to, and restored from, a removable media device (RMD). The Nortel ISP1100 Signaling Server uses a 3.5-inch floppy disk. The Nortel CP PM Signaling Server uses a Compact Flash (CF) card. The IBM X306m and HP DL320-G4 Signaling Servers use USB memory sticks.

When you migrate from one Signaling Server (source) to another Signaling Server (target), backing up your IP configuration data from the source Signaling Server before you start, saves you the time and effort of having to manually re-enter them during the migration.

Backing up the IP configuration

Use the following procedure to back up IP configuration from your Signaling Server to the removable media device (RMD).

Procedure 52
Backing up the IP configuration

Step	Action
1	Access the Tools Menu of the Signaling Server Software Installation Tool (see Procedure 51 "Accessing the Signaling Server Tools Menu" (page 297)
2	Enter **i** on the Tools Menu to back up the IP configuration from the hard disk to the RMD. The Back up IP configuration screen appears.

Figure 233
Back up IP configuration

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

Please insert the diskette in the removable drive
to copy back the IP configuration to disk

        Please enter:
<CR> -> <a> - Diskette is now in the removable drive.
               Continue.
        <q> - Quit.

        Enter Choice>
```

3	Insert the appropriate RMD in the appropriate drive, and press **<CR>** or enter **a** to trigger the backup. • for Nortel ISP1100 Signaling Servers, insert a 3.5-inch floppy disk in the floppy drive • for Nortel CP PM Signaling Servers, insert a CF card in the faceplate CF drive • for IBM X306m and HP DL320-G4 Signaling Servers, insert a USB memory stick in a USB drive After the backup is complete, the following system message appears. `Done copying IP configuration to removable media device`

—End—

Restoring the IP configuration

Use the following procedure to restore IP configuration from the Removable Media Device (RMD) to the Signaling Server.

Procedure 53
Restoring the IP configuration

Step	Action
1	Access the Tools Menu of the Signaling Server Software Installation Tool (see Procedure 51 "Accessing the Signaling Server Tools Menu" (page 297)
2	Enter **h** to restore the IP configuration from the RMD to the hard disk. The Restore IP configuration screen appears.

Figure 234
Restore IP configration

```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
============================================================

Please insert the diskette in the removable drive
to copy back the IP configuration to disk

        Please enter:
<CR> -> <a> - Diskette is now in the removable drive.
              Continue.
        <q> - Quit.

        Enter Choice>
```

3	Insert the appropriate RMD into the appropriate drive, and press **<CR>** or enter **a** to trigger the restore. After the restore is complete, the following system message appears. `Done copying IP configuration to disk`

—End—

Set the Signaling Server port speed

Administrators can change the port speed of the Signaling Server for a maintenance terminal connection.

Procedure 54
Changing the Signaling Server port speed

Step	Action
1	Log on to the Signaling Server. See Procedure 22 "Logging on to the Signaling Server" (page 147).
2	Enter **stty 9600** to change the port speed to 9600 baud.

Note: Acceptable values for the maintenance port speed are 9600, 19200, 38400 and 115200.

3 Change the port speed on the terminal, terminal emulator, or PC (can require a terminal emulator reset).

4 Press **<CR>** several times until the command line prompt is visible at the new speed.

5 Enter the **exit** command to log off of the CLI.

—End—

Replace a defective Signaling Server

Replacing a defective CS 1000 Release 5.0 Signaling Server requires that you perform a migration of the Signaling Server from one hardware platform to another. See "Signaling Server migration" (page 215) for appropriate instructions.

Upgrade the RAM on a Nortel ISP1100 Signaling Server

Contents

This section contains information on the following topics:

Introduction

To run CS 1000 Release 5.0 software, a Nortel ISP1100 Signaling Server (NTDU27AA) must be equipped with 1 GB of memory. To enable customers to reconfigure their existing Nortel ISP1100 Signaling Servers for operation in a CS 1000 Release 5.0 environment, a RAM Upgrade Kit (NTDU80CA) is available. A Nortel NTDU80CA Ram Upgrade Kit consists of 2 x 256 Mb DIMM (RAM memory) boards.

The Nortel ISP1100 Signaling Server accomodates up to four DIMM boards. In earlier releases of the CS 1000 system software (Succession 2.0, Succession 3.0), only 256 Mb of RAM was required to support your Signaling Server. This requirement was satisfied with two 128 Mb DIMM boards. In later releases of the CS 1000 system software (CS 1000 Rel. 4.0, CS 1000 Rel. 4.5), a minimum of 512 Mb of RAM was required to

support your Signaling Server. This requirement was satisfied with four 128 Mb DIMM boards, or two 256 Mb DIMM boards. If your CS 1000 Rel. 4.0 or CS 1000 Rel. 4.5 Signaling Server had to support more than 382 virtual trunks, support more than 10,000 IP Phones, or host an IP Phones Application Server (IP Phone Directory services), then 1 Gb of RAM was required to support the associated operational requirement. This requirement was satisfied with four 256 Mb DIMM boards (two Nortel NTDU80CA RAM Upgrade kits.

If your Nortel ISP1100 Signaling Server is currently running Succession 2.0 or Succession 3.0 software (256 Mb of RAM configured), you must remove the two 128 Mb DIMM boards, and replace them with four 256 DIMM boards (two Nortel NTDU80CA RAM Upgrade kits) to configure 1 Gb of RAM.

If your Nortel ISP1100 Signaling Server is currently running CS 1000 Rel. 4.0 or CS 1000 Rel. 4.5, your Signaling Server could have 512 Mb of RAM configured using four 128 Mb DIMM boards, or two 256 Mb DIMM boards. If your Signaling Server has 512 Mb of RAM configured using four 128 Mb DIMM boards, you must remove and replace them with four 256 Mb DIMM boards (two NTDU80CA RAM Upgrade kits) to configure 1 Gb of RAM. If your Signaling Server has 512 Mb of RAM configured using two 256 Mb DIMM boards, you only need to add two more 256 Mb DIMM boards (one Nortel NTDU80CA RAM Upgrade kit) to configure 1 Gb of RAM. If you already have 1 Gb of RAM configured on your Nortel ISP1100 Signaling Server for operational reasons (see above), you do not need to upgrade your RAM.

Depending on your existing RAM configuration, you need either none, one or two Nortel NTDU80CA RAM Upgrade Kits to upgrade your legacy Nortel ISP1100 Signaling Server to 1 Gb of RAM.

This section explains how to upgrade the RAM on a Nortel ISP1100 Signaling Server using the Nortel NTDU80CA RAM Upgrade Kit.

> ***Note:*** If you are in possession of a PCI Riser Board kit (NTDU27AE), you should install it while you have the cover of the Nortel ISP1100 Signaling Server removed, during the RAM upgrade. For instructions, see "Install a PCI Riser board on a Nortel ISP1100 Signaling Server" (page 315).

Preparation

Read the following warnings carefully before beginning the RAM upgrade process.

DANGER

SYSTEM POWER ON/OFF: The Power button on the front panel of the Nortel ISP1100 Signaling Server DOES NOT remove AC power to the Nortel ISP1100 Signaling Server system. Some circuitry in the Nortel ISP1100 Signaling Server can continue to operate even through the front panel Power button is off. Always disconnect the power cord from the AC power source or wall outlet before performing any of the procedures in this section. Failure to do so can result in personal injury or equipment damage.

DANGER

HAZARDOUS CONDITIONS, POWER SUPPLY: Hazardous voltage, current, and energy levels are present inside the power supply. There are no-user-serviceable parts inside the power supply; servicing must be done by technically qualified personnel.

DANGER

HAZARDOUS CONDITIONS, DEVICES, AND CABLES: Hazardous electrical conditions can be present on power, telephone, and communication cables. Press the Power button to turn off the Signaling Server, and disconnect the power cord from the AC power source, telecommunications systems, networks, and modems attached to the Signaling Server before removing the cover. Failure to do so can result in personal injury or equipment damage.

CAUTION

ELECTROSTATIC DISCHARGE (ESD) AND ESD PROTECTION: Because the Nortel ISP1100 Signaling Server can be extremely sensitive to ESD, perform the procedures in this section only at an ESD workstation. If an ESD station is not available, you can reduce the risk of ESD damage by:

- Wearing the antistatic wrist strap provided and attach it to a metal part of the Nortel ISP1100 Signaling Server.
- Touch the metal on the Nortel ISP1100 Signaling Server before touching the other components.
- Keep part of your body in contact with the metal Nortel ISP1100 Signaling Server to dissipate the static charge while handling the components.
- Avoid moving around unnecessarily.
- Hold the Nortel ISP1100 Signaling Server components (especially boards) only by the edges.
- Place the Nortel ISP1100 Signaling Server components on a grounded, static-free surface. Use a conductive foam pad if available, but NOT the component wrapper.
- Do not slide the components over any surface.

CAUTION

Service interruption

COOLING AND AIRFLOW: For proper cooling and airflow, always install the Nortel ISP1100 Signaling Server access cover before turning on the system. Operating the system without the cover in place can cause overheating and damage to system parts.

Perform the RAM upgrade

Use the following procedure to upgrade the RAM on a Nortel ISP1100 Signaling Server.

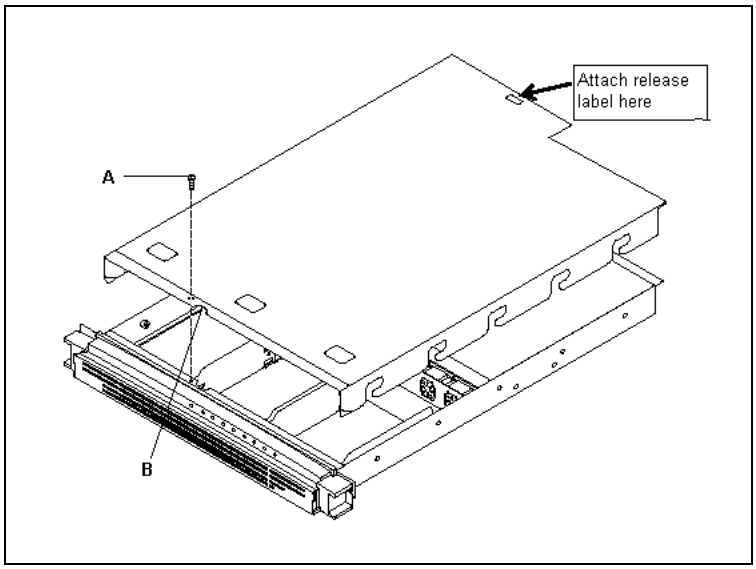
Note: These instructions are intended for qualified technical personnel with experience installing and configuring servers.

Procedure 55

Upgrading the RAM of a Nortel ISP1100 server

Step	Action
1	Remove the cover from the Nortel ISP1100 Signaling Server.

Figure 235
Removing/replacing the cover



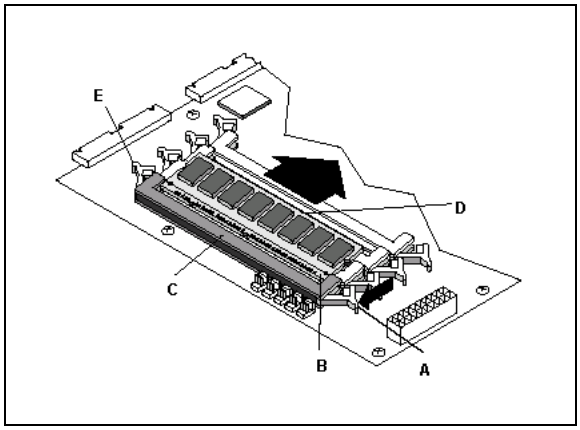
a. Use a Phillips screwdriver to remove the screw (A) from the front edge of the cover.

b. Grasp the back edge of the cover. Simultaneously, pull from the back edge and push near the front edge until the cover slides out from under the edge of the Nortel ISP1100 Signaling Server front panel.

c. Grasp the notch (B) in the front center of the cover and lift up to remove the cover.

2 Remove the existing 128 Mb DIMM boards (if necessary).

Figure 236
Remove a DIMM board



a. Grasp the ejector lever (A) on one end of the DIMM board and push down on the lever until the edge of the board connector (B) just lifts out of the socket (C).

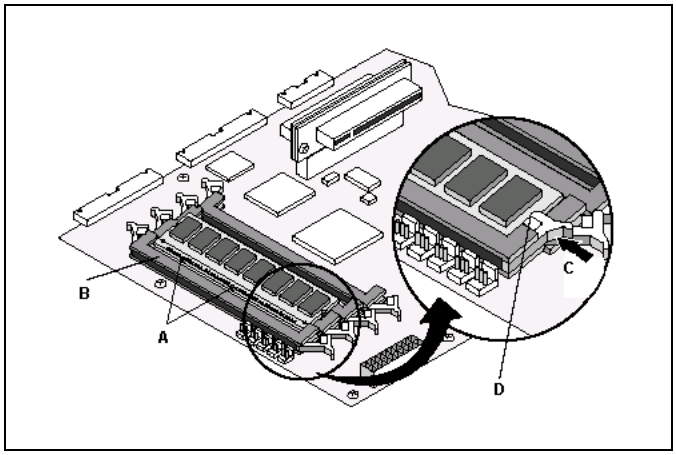
CAUTION
Hold the tips of your fingers lightly on the back edge (D) of the DIMM board to prevent the board from suddenly ejecting from the socket (C). The DIMM board or other components on the Nortel ISP1100 Signaling Server board can be damaged if the DIMM board is allowed to suddenly eject from the socket.

b. Grasp the ejector lever (E) on the other end of the DIMM board and carefully push down on the lever until the DIMM board is loose from the socket.

3 Install the new 256 Mb DIMM boards (two or four, as required).

Note: Use only DIMM boards contained in the NTDU80CA Nortel ISP1100 Signaling Server RAM Upgrade Kit. Nortel does not recommend the use of other memory modules.

Figure 237
Install a DIMM board



a. Align the key slots (A) in the edge of the DIMM board with the corresponding slots in the mating board socket (B).

The connectors are keyed to mate in one direction only.

CAUTION
Use extreme care when installing a DIMM board. Applying too much pressure or mis-aligning the board in the socket can damage the sockets or DIMM board edge connectors. DIMM board edge connectors are keyed and can be inserted only one way.

To reduce the risk of damaging a connector, install the DIMM boards starting with the back socket on the Nortel ISP1100 Signaling Server board and move toward the front of the board.

b. Firmly press the DIMM board straight down and all the way into the Signaling Server board socket.

c. Ensure the DIMM board is locked in by pressing the levers (C) on each end of the Signaling Server board socket into the mating notches (D) on each edge of the DIMM board.

4 Replace the cover on the Nortel ISP1100 Signaling Server. Refer to Figure 235 "Removing/replacing the cover" (page 308).

a. Position the cover on the Nortel ISP1100 Signaling Server with the notched edge (B) facing the front and the slotted sides of the cover *inside* the frame.

b. Grasp the back edge of the cover. Simultaneously, push from the back and top until the cover slides all the way under the edge of the Nortel ISP1100 Signaling Server front panel.

c. Use a Phillips screwdriver and the screw (A) removed in step 1 to securely attach the cover to the Nortel ISP1100 Signaling Server.

d. Attach the memory label (reading "1 GB" or "1024 MB") to the back edge of the cover.

—End—

Verify the RAM upgrade

Use the following procedure to ensure that the RAM upgrade was successful.

Procedure 56
Verifying the RAM upgrade on a Nortel ISP1100 server

Step	Action

When upgrading to 1 GByte, the system responses indicate "1 GB" instead of "512 MB".

1. Connect a standard serial interface (straight-through) cable to the maintenance terminal and to the serial port on the back (not the front) of the Nortel ISP1100 Signaling Server.

2. Using a terminal software program, such as Microsoft Windows HyperTerminal, configure the terminal type of the maintenance terminal serial port to "auto detect" terminal type.

3. Connect the power cable to the Nortel ISP1100 Signaling Server.

4. Press the power switch, the left-most button on the front of the Nortel ISP1100 Signaling Server.

   The following system messages appear on the maintenance terminal screen:

```
AMIBIOS (C)2001 American Megatrends Inc.
  Copyright 1996-2001 Intel Corporation
TR440BXA.86B.0042.P15.0107200951
Intel(R) Pentium(R)III processor, 700MHz
1 GB OK
Hit <F2> if you want to run SETUP
```

5. <Optional> To do a more detailed RAM test:

   a. Press the **F2** button.

   b. Navigate to the "Boot" menu.

   c. Disable the Quickstart option.

   d. Exit, saving the changes.

   Do not change any other settings. The Nortel ISP1100 Signaling Server reboots and performs a more detailed RAM test at boot time.

   If "1 GB OK" appears on the screen, the RAM upgrade was successful. If not, the RAM upgrade failed.

6. Power off the Nortel ISP1100 Signaling Server by depressing the Power button for seven seconds.

7. Disconnect the power cable.

—End—

Install the hard drive on a Nortel CP PM Signaling Server

This section describes the procedure for installing a hard drive on both models of the Nortel CP PM Signaling Server (NTDW61BAE5 and NTDW66AAE5). A Nortel CP PM Signaling Server Hard Drive kit (NTDW6102E5) ships with the servers, and if required, can also be ordered from Nortel.

The hard drive kit contains a hard drive with a jumper, 4 screws, and installation instructions (document N0120776). You need only a small Phillips screw driver to install the hard drive.

ATTENTION

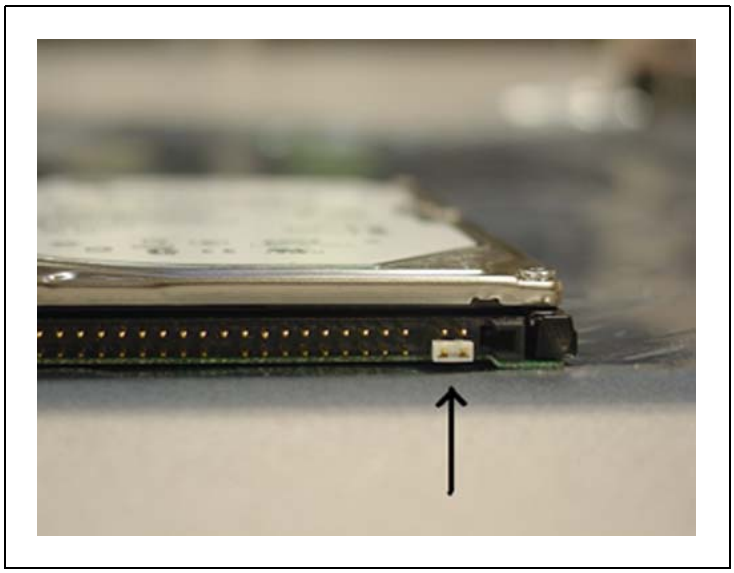
IMPORTANT!
Observe proper ESD precautions while handling the hard drive and Nortel CP PM server.

Use the following procedure to replace the hard drive on a Nortel CP PM server.

Procedure 57
Replacing the hard drive on a Nortel CP PM Signaling Server

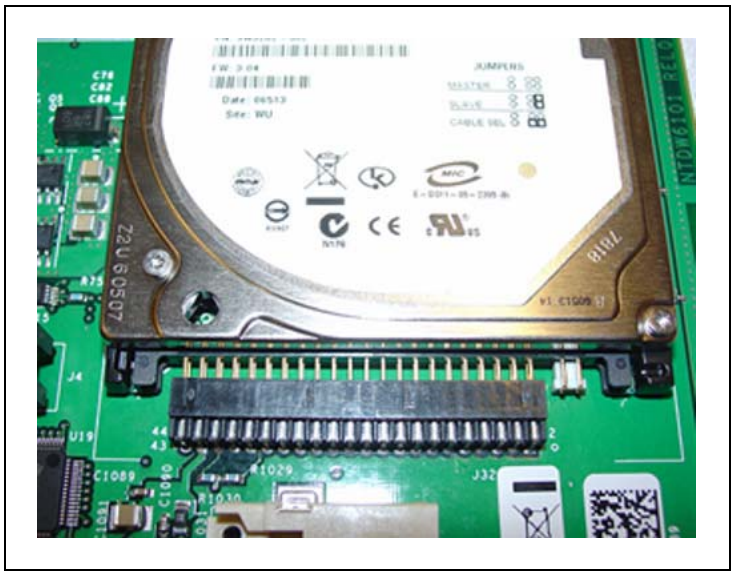
Step	Action
1	Ensure jumper is located in the cable select (CS) position according to the labeling on the hard drive.

Figure 238
CP PM hard drive jumper



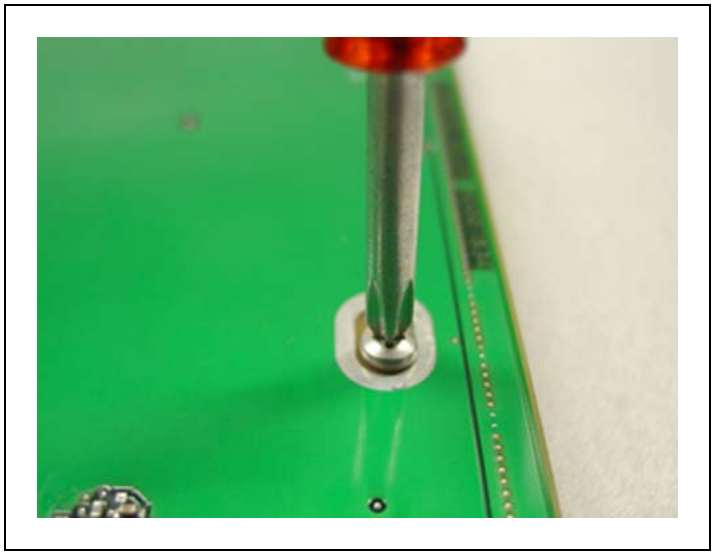
Step	Action
2	Place hard drive on printed circuit board and slide to mate with connector J32.

Figure 239
CP PM hard drive and connector J32



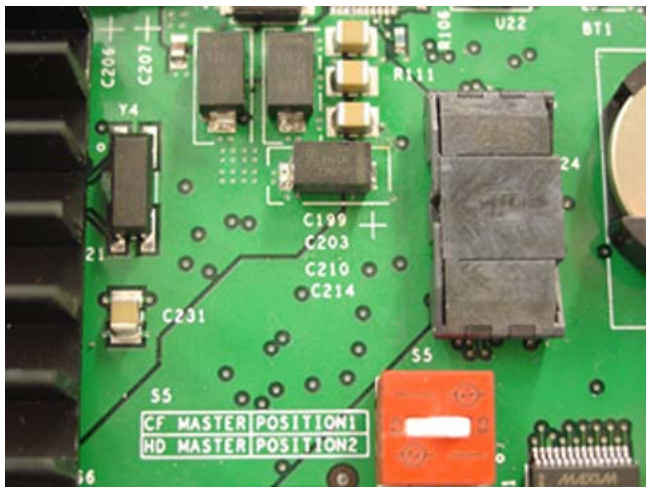
3 Secure hard drive from the bottom side with the included screws.

Figure 240
Securing CP PM hard drive to circuit board



4 Place Dip Switch S5 in position 2 to select HD Master option.

Figure 241
CP PM Signaling Server FMD dip switch



ATTENTION

IMPORTANT!

A Nortel CP PM circuit card has an on-board switch (S5) for designating the internal hard drive (HD) or internal Compact Flash (CF) drive as the Fixed Media Device (FMD) for the Signaling Server. You must configure the on-board FMD switch (S5) to position 2 to designate the HD as the FMD for the Signaling Server.

5 Remove on-board compact flash retainer clip if populated.

Figure 242
CP PM Signaling Server internal CF card retainer clip

—End—

New Nortel CP PM Signaling Servers ship with CS 1000 Release 5.0 software and system components preloaded on the hard drive. When you install a new hard drive on a Nortel CP PM Signaling Server, you need to install CS 1000 Release 5.0 software and system components on the new hard drive. To accomplish this task, you need to obtain the software and system components from the Nortel software download web site, load them onto a Compact Flash (CF) card, and install them on the new hard drive.

For instructions to obtain CS 1000 Release 5.0 software and components and load them onto a CF card, see "Obtain a CP PM Signaling Server software compact flash card" (page 102).

Install a PCI Riser board on a Nortel ISP1100 Signaling Server

This section explains how to install a PCI Riser Board on the server board of a Nortel ISP1100 server using the PCI Riser Board Upgrade Kit (NTDU27AE).

Earlier versions of the Nortel ISP1100 Signaling Server (NTDU27AA - Release 1 to 5) have a remote chance of not recovering during boot-up when the server is manually reset or powered up after a loss of power. See Nortel technical bulletin #2005006501, Version 3 for more details and information. To avoid this situation, you must install a PCI Riser Board Upgrade Kit (NTDU27AE). The PCI Riser Upgrade Kit consists of a PCI Riser board that must be installed on the server board.

Note: These instructions are intended for qualified technical personnel with experience installing and configuring servers.

Preparation

Read the following warnings carefully before beginning thePCI Riser Board installation process.

DANGER

SYSTEM POWER ON/OFF: The Power button on the front panel of the Nortel ISP1100 Signaling Server DOES NOT remove AC power to the Nortel ISP1100 Signaling Server system. Some circuitry in the Nortel ISP1100 Signaling Server can continue to operate even through the front panel Power button is off. Always disconnect the power cord from the AC power source or wall outlet before performing any of the procedures in this section. Failure to do so can result in personal injury or equipment damage.

DANGER

HAZARDOUS CONDITIONS, POWER SUPPLY: Hazardous voltage, current, and energy levels are present inside the power supply. There are no-user-serviceable parts inside the power supply; servicing must be done by technically qualified personnel.

DANGER

HAZARDOUS CONDITIONS, DEVICES, AND CABLES: Hazardous electrical conditions can be present on power, telephone, and communication cables. Press the Power button to turn off the Signaling Server, and disconnect the power cord from the AC power source, telecommunications systems, networks, and modems attached to the Signaling Server before removing the cover. Failure to do so can result in personal injury or equipment damage.

CAUTION

ELECTROSTATIC DISCHARGE (ESD) AND ESD PROTECTION: Because the Nortel ISP1100 Signaling Server can be extremely sensitive to ESD, perform the procedures in this section only at an ESD workstation. If an ESD station is not available, you can reduce the risk of ESD damage by:

- Wearing the antistatic wrist strap provided and attach it to a metal part of the Nortel ISP1100 Signaling Server.
- Touch the metal on the Nortel ISP1100 Signaling Server before touching the other components.
- Keep part of your body in contact with the metal Nortel ISP1100 Signaling Server to dissipate the static charge while handling the components.
- Avoid moving around unnecessarily.
- Hold the Nortel ISP1100 Signaling Server components (especially boards) only by the edges.
- Place the Nortel ISP1100 Signaling Server components on a grounded, static-free surface. Use a conductive foam pad if available, but NOT the component wrapper.
- Do not slide the components over any surface.

CAUTION
Service interruption
COOLING AND AIRFLOW: For proper cooling and airflow, always install the Nortel ISP1100 Signaling Server access cover before turning on the system. Operating the system without the cover in place can cause overheating and damage to system parts.

Install the PCI Riser Board

Use the following procedure to install a PCI Riser Board on a Nortel ISP1100 Signaling Server.

Procedure 58
Installing the PCI Riser board on a Nortel ISP1100 Signaling Server

Step	Action

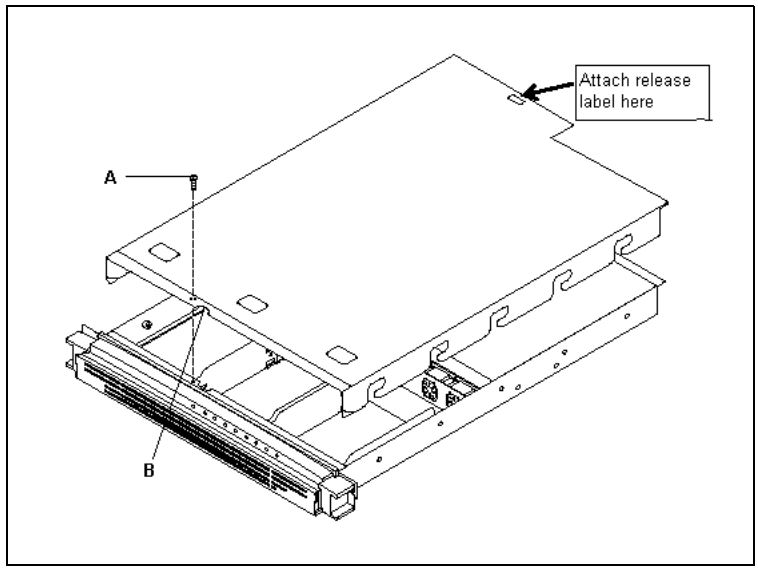
1 Remove the cover from the Nortel ISP1100 Signaling Server. Refer to Figure 243 "Removing/replacing the cover" (page 317).

a. Use a Phillips screwdriver to remove the screw (A) from the front edge of the cover.

b. Grasp the back edge of the cover. Simultaneously, pull from the back edge and push near the front edge until the cover slides out from under the edge of the Nortel ISP1100 Signaling Server front panel.

c. Grasp the notch (B) in the front center of the cover and lift up to remove the cover.

Figure 243
Removing/replacing the cover



2 Install the PCI Riser board.

CAUTION

Make sure that the PCI Riser board you install is provided in the NTDU27EA Signaling Server PCI Riser Upgrade kit.

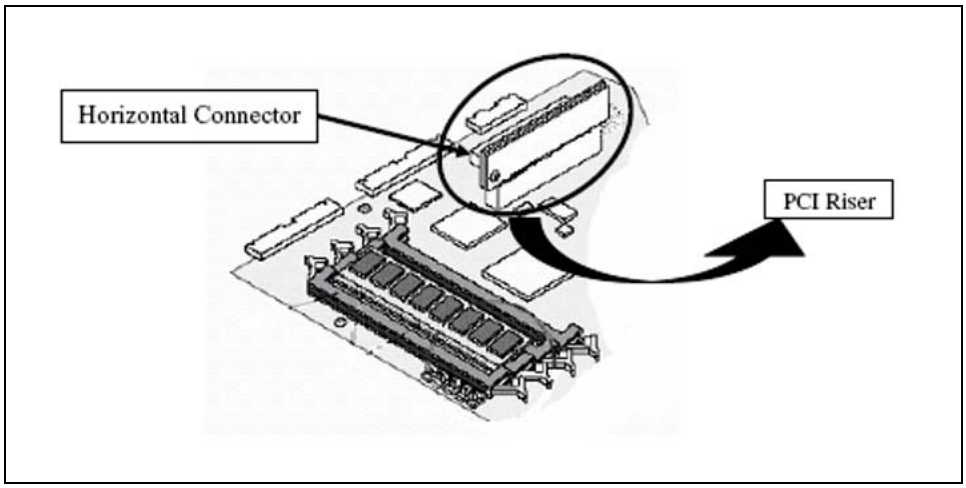
Use extreme care when installing a Riser board. Applying too much pressure or misaligning the board in the socket can damage the sockets or Riser board edge connectors. The Riser board edge connector is keyed and can be inserted only one way.

a. Orient the Riser board noting the position of the horizontal PCI connector relative to the mother board (see Figure 244 "Install a PCI Riser board" (page 318).

Note: The PCI Riser connectors are keyed to mate in only one direction.

b. Firmly press the PCI Riser board straight down and all the way into the server board socket.

Figure 244
Install a PCI Riser board



3 Replace the cover on the Nortel ISP1100 Signaling Server. Refer to Figure 243 "Removing/replacing the cover" (page 317).

a. Position the cover on the Nortel ISP1100 Signaling Server with the notched edge (B) facing the front and the slotted sides of the cover *inside* the frame.

b. Grasp the back edge of the cover. Simultaneously, push from the back and top until the cover slides all the way under the edge of the Nortel ISP1100 Signaling Server front panel.

c. Use a Phillips screwdriver and the screw (A) removed in step 1 to securely attach the cover to the Nortel ISP1100 Signaling Server.

d. Attach the memory label (reading "Release 6") to the back edge of the cover.

—End—

List of terms

ELAN sub-net

Embedded Local Area Network (ELAN) sub-net. This isolated sub-net connects the Signaling Server to other system components for system communication purposes.

H.323

A standard approved by the International Telecommunication Union (ITU) that defines how audiovisual conferencing data is transmitted across networks. In theory, H.323 enables users to participate in the same conference even though they are using different video-conferencing applications. Although most video-conferencing vendors have announced that their products conform to H.323, it is too early to say whether such adherence actually results in inter-operability.

IP

Abbreviation of **Internet Protocol**, pronounced as two separate letters. IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP by itself is something like the postal system. It enables you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

SIP

Short for Session Initiation Protocol. SIP is a protocol standard used for establishing, modifying, and terminating conference and telephony sessions in IP networks. A session can be a simple two-way telephone call or it can be a collaborative multi-media conference session. SIP initiates real-time, multimedia sessions that can integrate voice, data, and video. The protocol's text-based architecture speeds access to new services with greater flexibility and more scalability.

TLAN subnet

Telephony Local Area Network subnet. This subnet is separated from the rest of the network and connects the Voice Gateway Media Cards, the Signaling Server, and the IP Phones for telephony communication purposes.

TPS

IP Phone Terminal Proxy Server. This server controls the connection of IP Phones. It resides on the Signaling Server with an emergency backup on the Voice Gateway Media Card.

Index

Nortel Communication Server 1000

Signaling Server Installation and Commissioning

Publication: NN43001-312
Document status: Standard
Document version: 01.02
Document date: 30 May 2007

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

Sourced in Canada