**Nortel Communication Server 1000**

Nortel Communication Server 1000 Release 4.5

# Signaling Server

## Installation and Configuration

Document Number: 553-3001-212
Document Release: Standard 10.00
Date: March 2007

Produced in Canada

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

# Revision history

**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 and configuration” 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 and reconfiguration” 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

**July 2006**

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

CR Q01382679:

- addition of missing system display messages and procedure steps in the “Upgrading Signaling Server software” procedure found in the “Software upgrade and reconfiguration” 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 for CR Q01273279, correcting the default login credentials for the Signaling Server on page 93.

**January 2006**

Standard 4.00. This document is upissued for CR Q01190789, with information on backing up the Gatekeeper database and storing it locally during a software upgrade.

**August 2005**

Standard 3.00. This document is upissued to support Communication Server 1000 Release 4.5.

**September 2004**

Standard 2.00. This document is upissued 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, which resulted 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

# List of procedures

# About this document

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

## Subject

This document describes the Signaling Server and provides the information necessary to install and configure it in a Communication Server 1000 system.

### Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 4.5 software. For more 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 systems:

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)

- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)

*Note:* When upgrading software, memory upgrades may be required on the Signaling Server, the Call Server, or both.

# Intended audience

This document is intended for individuals responsible for installing, configuring, and maintaining the Signaling Server.

Only qualified personnel should install Signaling Servers. To use this document, you should have a basic knowledge of CS 1000S, 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.

# Conventions

## Terminology

In this document, the following systems are referred to generically as "system":

- Communication Server 1000S (CS 1000S)
- Communication Server 1000M (CS 1000M)
- Communication Server 1000E (CS 1000E)
- Meridian 1

The following systems are referred to generically as "Small System":

- Communication Server 1000M Chassis (CS 1000M Chassis)
- Communication Server 1000M Cabinet (CS 1000M Cabinet)
- Meridian 1 PBX 11C Chassis
- Meridian 1 PBX 11C Cabinet

The following systems are referred to generically as “Large System”:

- Communication Server 1000M Half Group (CS 1000M HG)
- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Meridian 1 PBX 51C
- Meridian 1 PBX 61C
- Meridian 1 PBX 81
- Meridian 1 PBX 81C

# Related information

This section lists information sources that relate to this document.

### NTPs

The following NTPs are referenced in this document:

- *IP Peer Networking: Installation and Configuration* (553-3001-213)
- *Branch Office: Installation and Configuration* (553-3001-214)
- *Element Manager: System Administration* (553-3001-332)
- *IP Line: Description, Installation, and Operation* (553-3001-365)
- *Software Input/Output: Maintenance* (553-3001-511)
- *CS 1000 to MCS 5100 Converged Desktop Type 2: Configuration Guide* (553-3001-521)
- *Communication Server 1000M and Meridian 1: Small System Planning and Engineering* (553-3011-120)
- *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210)
- *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures* (553-3011-258)
- *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120)

- *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210)
- *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures* (553-3021-258)
- *Communication Server 1000S: Planning and Engineering* (553-3031-120)
- *Communication Server 1000S: Installation and Configuration* (553-3031-210)
- *Communication Server 1000S: Upgrade Procedures* (553-3031-258)
- *Communication Server 1000E: Planning and Engineering* (553-3041-120)
- *Communication Server 1000E: Installation and Configuration* (553-3041-210)
- *Communication Server 1000E: Upgrade Procedures* (553-3041-258)

### Online

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

www.nortel.com

### CD-ROM

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, shown in Figure 1 on page 20, is an industry-standard PC-based server that provides a central processor to drive Session Initiation Protocol (SIP) and H.323 signaling, IP Phone signaling, and IP Peer Networking. It is required in all CS 1000S, CS 1000M, and CS 1000E systems.

**Figure 1**
**Signaling Server**

The Signaling Server provides signaling interfaces to the IP network using software components that run on the VxWorks$^{TM}$ real-time operating system.

The Signaling Server performs the following functions:

- acts as a SIP Redirect Server and an H.323 Gatekeeper
- runs the SIP and H.323 signaling gateways (for Virtual Trunks)
- acts as a Terminal Proxy Server (TPS)
- acts as a web server for CS 1000 Element Manager
- runs the Application Server for the Personal Directory, Callers List, and Redial List feature

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

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

# Software applications

The Signaling Server provides signaling interfaces to the IP network using software components that run on the VxWorks$^{TM}$ real-time operating system. The software components are:

- IP Phone TPS
- 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 feature

## 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
- Nortel IP Phone Key Expansion Module (KEM)
- IP Phone 2007
- IP Audio Conference Phone 2033
- Nortel IP Softphone 2050

Each IP Phone can be configured 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 the IP Phones that are registered to it. Accordingly, the TPS also manages the updating of the firmware for those IP Phones. For more information on upgrading the firmware, refer to *IP Line: Description, Installation, and Operation* (553-3001-365) and *Branch Office: Installation and Configuration* (553-3001-214)

## SIP and H.323 signaling gateway (Virtual Trunk)

### Session Initiation Protocol (SIP) trunking

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 1000S/Meridian 1 domain and users in the SIP domain.

The SIP trunking software is responsible for functioning as:

- SIP User Agent
- signaling gateway for all IP Phones

For more information about SIP trunking, refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

### H.323 trunking

H.323 is a protocol 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 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
- interoperability

For more information about H.323 signaling, refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

## Network Routing Service

The IP Peer Networking feature provides a Network Routing Service (NRS) where all systems in the network are registered. The NRS has three components:

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

Only one NRS is required in a network. NRS redundancy is supported and is highly recommended. See "Redundancy" on page 25.

### SIP Redirect Server

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

The SIP Redirect Server software provides telephone number-to-IP address resolution. It 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 Configuration* (553-3001-213).

### H.323 Gatekeeper

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

The H.323 Gatekeeper software provides telephone number-to-IP address resolution. Since 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, it also eliminates the duplication of numbering plan information among sites. However, static registration and manual configuration are still supported for backward compatibility.

For more information about the H.323 Gatekeeper, refer to *IP Peer Networking: Installation and Configuration* (553-3001-213).

### Network Connection Service

The Network Connection Service (NCS) provides an interface to the TPS, enabling 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 can be accessed directly through a web browser or Optivity Telephony Manager (OTM). 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 greater efficiency.

For more information on Element Manager, refer to “Element Manager configuration” on page 165 and *Element Manager: System Administration* (553-3001-332).

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

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

For more information on Personal Directory, Callers List, and Redial List, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

## Redundancy

To provide redundancy in the event the Signaling Server fails, install an additional Signaling Server. A redundant Signaling Server also provides load sharing for the TPS and an alternate route for the SIP and H.323 Gateway software.

In a redundant configuration, one of the Signaling Servers is designated the Leader Signaling Server. The other Signaling Server(s) are designated the Follower(s). In the event of Leader Signaling Server failure, a Follower Signaling Server assumes the role of the Leader Signaling Server. The NRS must reside on the Leader Signaling Server.

In a redundant configuration, the NRS is configured as Primary, Alternate, or Failsafe (if required). Although a network requires only one (Primary) NRS, Nortel recommends that an Alternate NRS, and in some cases at least one Failsafe NRS, be configured in the network.

**IMPORTANT!**

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

See “Redundancy” on page 36 for more details.

## Hardware description

This section describes the physical components of the Signaling Server.

> ***Note:*** With the exception of installing memory upgrades, there are no user-serviceable components in the Signaling Server. Any defective Signaling Servers should be returned to the supplier.

## Product code

The product code for the Signaling Server is NTDU27.

## Power

The power cord connector is located on the left-hand corner on the rear of the Signaling 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 not customer replaceable.

## Cooling

The Signaling Server has forced air cooling. The fan runs whenever the unit is on. The air flow is front-to-back.

## Card slots

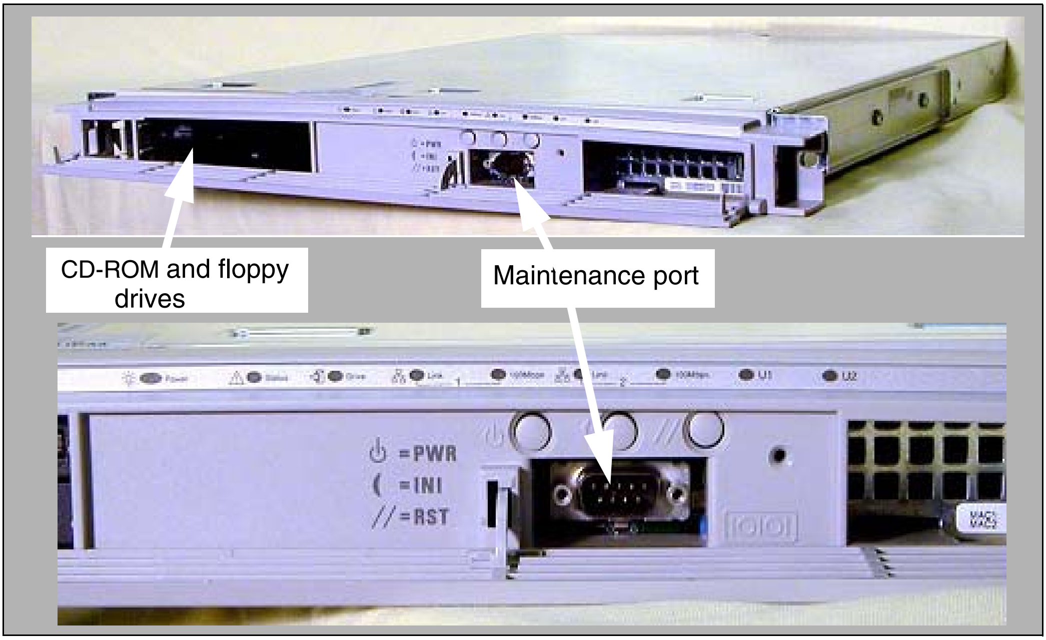
The Signaling Server has no available card slots.

## Connectors

### Front connectors and media drives

Figure 2 on page 27 shows the connectors and drives on the front of the Signaling Server.

**Figure 2**
**Connectors on the front of the Signaling Server**



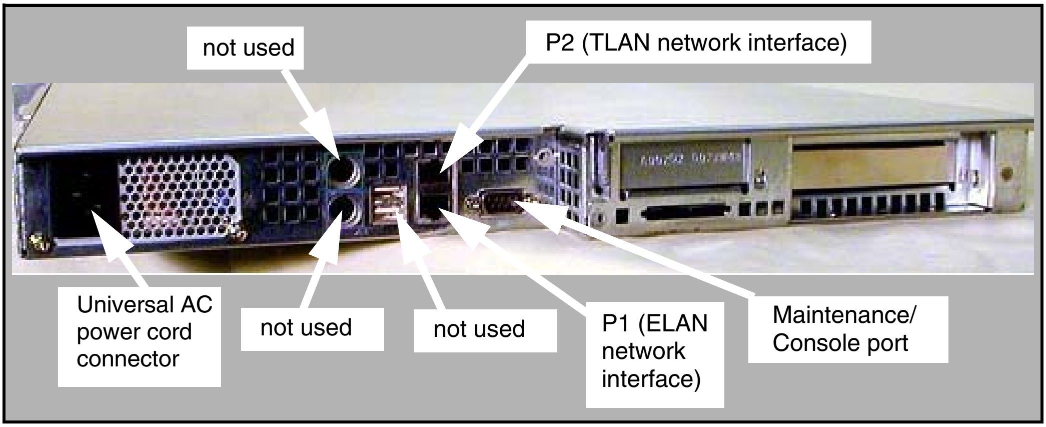
Refer to Figure 2.

- The front DB-9 serial port can support a login session for Command Line Interface (CLI) management.
- 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, and 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.

## Rear connectors and ports

Figure 3 shows the cable connectors on the back of the Signaling Server.

**Figure 3**
**Connectors on the back of the Signaling Server**


not used
P2 (TLAN network interface)
Universal AC power cord connector
not used
not used
P1 (ELAN network interface)
Maintenance/ Console port

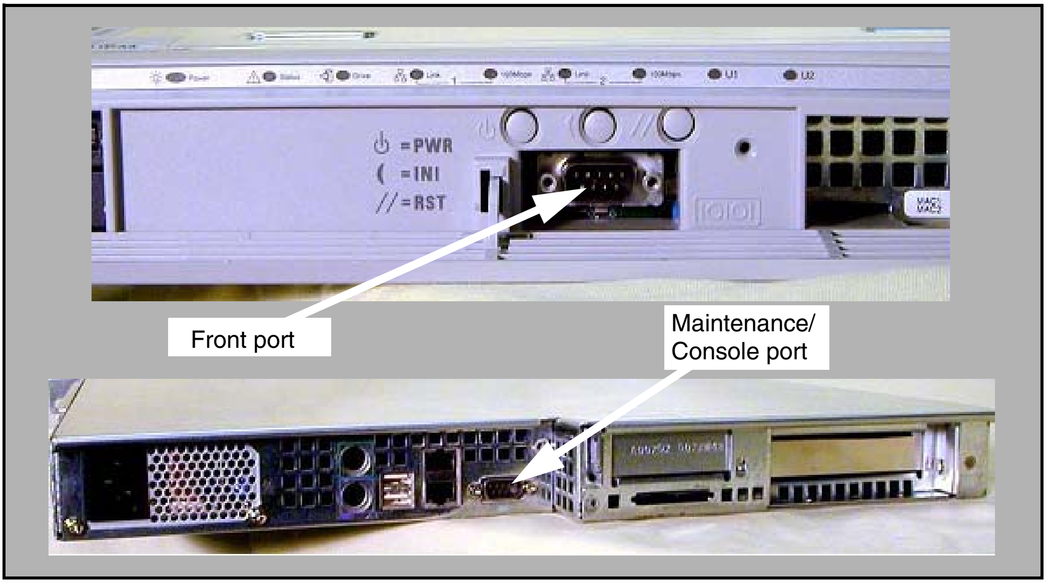
Refer to Figure 3.

- The AC power cord connector is at the back of the Signaling Server on the left side.
- The TLAN network interface (P2) connects the Signaling Server to a TLAN Layer 2 switch port.
- The ELAN network interface (P1) connects the Signaling Server to an ELAN Layer 2 switch port.
- The maintenance port connects the Signaling Server to a maintenance and administration terminal.
- The remaining ports are not used for any function. Do not plug any device into these ports.

## Maintenance ports

The Signaling Server has two maintenance ports, as shown in Figure 4 on page 29. Both ports can be used for maintenance. The console port is used during Signaling Server software installation and basic configuration.

**Figure 4**
**Maintenance port location on the front and back of the Signaling Server**



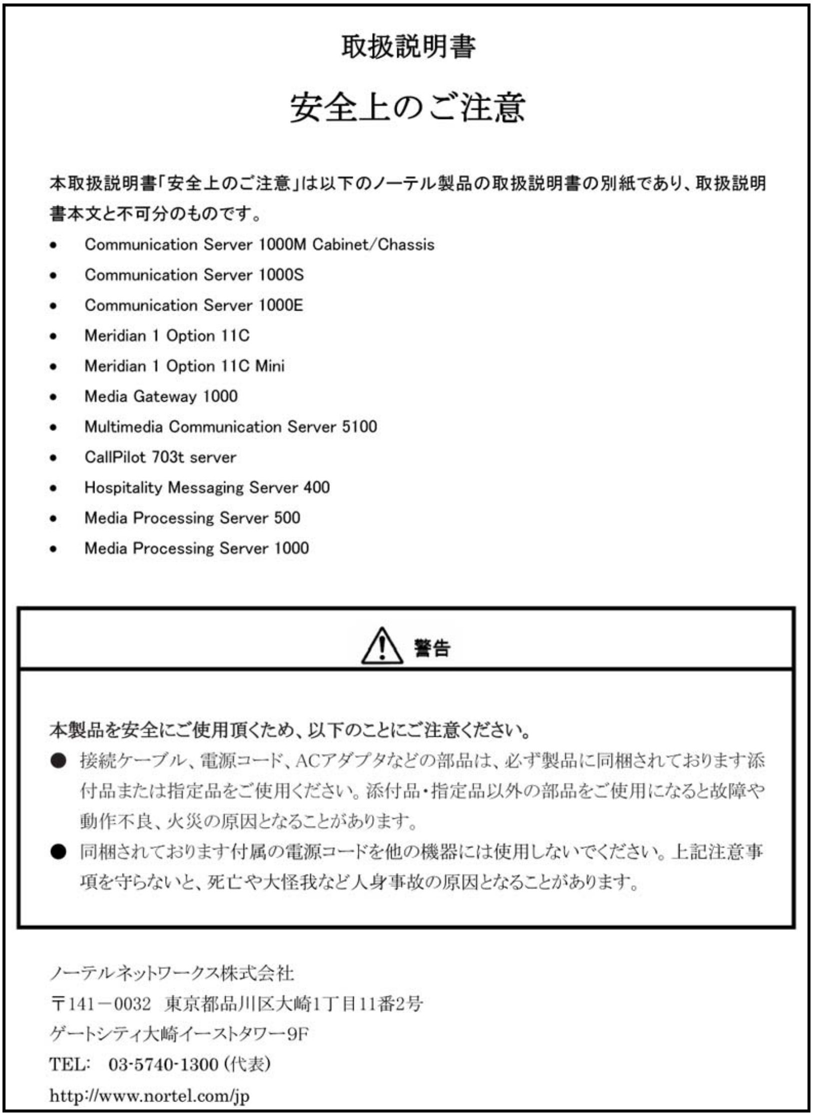
# Planning and engineering

## Contents

This section contains information on the following topics:

# Regulatory information

## DenAn regulatory notice for Japan



取扱説明書

安全上のご注意

本取扱説明書「安全上のご注意」は以下のノーテル製品の取扱説明書の別紙であり、取扱説明書本文と不可分のものです。

- Communication Server 1000M Cabinet/Chassis
- Communication Server 1000S
- Communication Server 1000E
- Meridian 1 Option 11C
- Meridian 1 Option 11C Mini
- Media Gateway 1000
- Multimedia Communication Server 5100
- CallPilot 703t server
- Hospitality Messaging Server 400
- Media Processing Server 500
- Media Processing Server 1000

⚠ 警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

● 接続ケーブル、電源コード、ACアダプタなどの部品は、必ず製品に同梱されております添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因となることがあります。

● 同梱されております付属の電源コードを他の機器には使用しないでください。上記注意事項を守らないと、死亡や大怪我など人身事故の原因となることがあります。

ノーテルネットワークス株式会社
〒141－0032　東京都品川区大崎1丁目11番2号
ゲートシティ大崎イーストタワー9F
TEL:　03-5740-1300 (代表)
http://www.nortel.com/jp

## Environmental conditions

The environment in which the Signaling Server operates must meet the following general conditions:

- Ventilating openings on the Signaling Server must be free of obstructions.
- Temperature must be maintained between 0° and 35° C (32° and 98° F).
- Humidity must be between 5% and 95% at 30° C non-condensing.
- The Signaling Server must not be subject to constant vibration.
- The Signaling Server and other system equipment must be located at least 12 ft. (3.66 m) away 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

Each Signaling Server can dissipate up to 125 Watts of power.

## Grounding

Like all system equipment, the Signaling Server must be thoroughly grounded. Refer to *Communication Server 1000S: Planning and Engineering* (553-3031-120), *Communication Server 1000E: Planning and Engineering* (553-3041-120), *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120), or *Communication Server 1000M and Meridian 1: Small System Planning and Engineering* (553-3011-120) as appropriate for the particular system.

The Signaling Server is not connected to a grounding block. It is properly grounded when:

- 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. This is the 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 only proper grounding of the Signaling Server itself. It 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.

# Power

Tables 1, 2, and 3 on page 35, list the AC power input requirements for the Signaling Server in North America, the United Kingdom, and Europe. Table 4 on page 36 summarizes these input requirements to determine the power consumption of the Signaling Server.

**Table 1**
**AC input requirements for a Signaling Server (North America)**

| | |
|---|---|
| **Voltage** | Recommended: 100-120 Volts<br>Maximum limits: 90 and 132 Volts<br>Single phase |
| **Frequency** | 50-60 Hz |
| **Power (I/P max)** | 200 VA maximum |
| **Outlet Type** | 120 Volts, 15 Amp supply |

**Table 2**
**AC input requirements for a Signaling Server (UK and Europe, except Germany)**

| | |
|---|---|
| **Voltage** | Recommended: 208/220 Volts<br>Maximum limits: 180 and 250 Volts<br>Single phase |
| **Frequency** | 50-60 Hz |
| **Power (I/P max)** | 200 VA maximum |
| **Outlet Type** | 208/240 Volts, 15 Amp supply |
| ***Note 1:*** Because local power specifications vary, consult a qualified local electrician when planning your power requirements.<br>***Note 2:*** The supplied power must be single-phase 240 or three-phase 208 Y, and must have a system ground conductor. | |

**Table 3**
**AC input requirements for a Signaling Server (Germany)**

| | |
|---|---|
| **Voltage** | Recommended: 230 Volts<br>Maximum limits: 180 and 250 Volts<br>Single phase |
| **Frequency** | 50 Hz |
| **Power (I/P max)** | 200 VA maximum |
| **Fuse** | 16 A |
| **Outlet Type** | Receptacles by DIN regulation |

**Table 4**
**Power consumption for a Signaling Server**

| Slot | Circuit card | Type | Power consumption from Table 1, Table 2, and Table 3 |
|---|---|---|---|
| 1 | N/A | N/A | 200W |
| | | Total Power In | 200W |

# 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 alternate route for the SIP and H.323 Gateway software.

When planning survivability strategies for the Signaling Server, a second Signaling Server should be included 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 acts as the primary, or master, TPS. The other Signaling Server is a Follower Signaling Server that acts as a secondary redundant TPS. The NRS must reside on the Leader Signaling Server.

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 Leader Signaling Server’s IP address if necessary.

**4** The Time-to-Live (TTL) of IP Phones registered with the failed Signaling Server expires. This 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.

*Note:* The same functionality is available without a redundant Signaling Server. Voice Gateway Media Cards can assume a TPS role and become a source for IP Phone registration.

# Scalability

Table 5 on page 38 summarizes the limits for each Signaling Server. The values in the table are to be used as a quick overview, for planning purposes. For detailed calculations, refer to *Communication Server 1000S: Planning and Engineering* (553-3031-120), *Communication Server 1000E: Planning and Engineering* (553-3041-120), *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120), or *Communication Server 1000M and Meridian 1: Small System Planning and Engineering* (553-3011-120) as appropriate to the particular system.

*Note:* Real-time capacity must also be considered for the specific application, and can also constrain any applications in reaching resource limits.

**Table 5**
**Signaling Server limits**

| Signaling Server component | Limit |
|---|---|
| NRS | • 5000 total endpoints (up to 5000 SIP endpoints and up to 2000 H.323 endpoints<br>• 20 000 numbering plan entries (total number of endpoints and routing entries)<br>• 100 000 calls per hour |
| Terminal Proxy Server (TPS) | • 5000 IP Phones |
| Virtual Trunks | • Up to 1800 trunks.<br>***Note:*** Depends on the split between SIP and incoming and outgoing H.323 calls. Refer to *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120) for details. |

# Branch offices

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

**IMPORTANT!**

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

There are 30 default Virtual Trunks at a branch office. 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 1000S: Planning and Engineering* (553-3031-120), *Communication Server 1000E: Planning and Engineering* (553-3041-120), *Communication Server 1000M and Meridian 1: Large System Planning and Engineering* (553-3021-120), or *Communication Server 1000M and Meridian 1: Small System Planning and Engineering* (553-3011-120), as appropriate.

For more information on the Branch Office feature, refer to *Branch Office: Installation and Configuration* (553-3001-214).

# Hardware installation

## Contents

This section contains information on the following topics:

## Introduction

This chapter describes how to install the Signaling Server in a 19-inch rack and connect it to the ELAN and TLAN subnets. This chapter also contains instructions on upgrading the memory in the Signaling Server.

## Hardware installation

This section describes how to install the Signaling Server hardware in a 19-inch rack.

## Readiness checklist

Before starting the installation, complete the checklist in Table 6.

**Table 6**
**Readiness checklist**

| **Have you:** | ✓ |
|---|---|
| Read all safety instructions in *Communication Server 1000S: Installation and Configuration* (553-3031-210)? | |
| Received all equipment? | |
| Made sure the area meets all environmental requirements? | |
| Checked for all power requirements? | |
| Checked for correct grounding facilities? | |
| Obtained the following:<br>• screwdrivers<br>• an ECOS 1023 POW-R-MATE or similar type of multimeter<br>• appropriate cable terminating tools<br>• a computer to be connected directly to the Signaling Server by a DTE—DTE null modem cable, with:<br>— teletype terminal (ANSI-W emulation, serial port, 19 200 bps) for the Signaling Server<br>— a web browser for Element Manager (configure cache settings to check for new web pages every time and to empty the cache when the browser is closed) | |
| Prepared the network data as suggested in *Converging the Data Network with VoIP* (553-3001-160) and *Communication Server 1000S: Planning and Engineering* (553-3031-120)? | |

## Materials required

To install the Signaling Server, obtain the following items:

**1** The Signaling Server.

*Note:* Save the packaging container and packing materials in case you must reship the product.

**2** The power cable for the Signaling Server. Check that the power cord is the exact type required in the host region. Do not modify or use the supplied AC power cord if it is not the correct type.

**3** The serial cable for the Signaling Server.

**4** The CAT5 cables for networking.

**5** The contents of the accessories pouch to install the Signaling Server. The accessories pouch should contain the following items:

**a** Two support brackets (A)

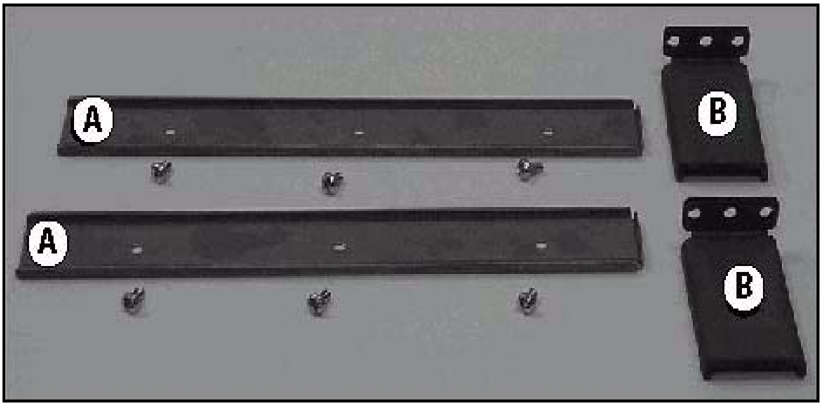
**b** Two rack-mounting brackets (B)

**c** Six rack-mount bracket screws (10-25 x 1/4” panhead Phillips)

**d** Two bezel door long rack-mount screws

Refer to Figure 5 on page 44. If any parts are missing, contact your supplier immediately.

**Figure 5**
**Signaling 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

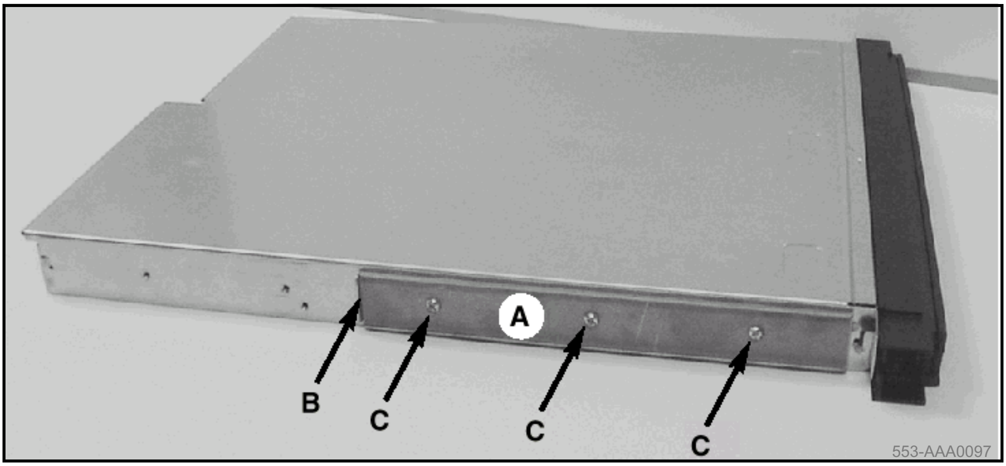
**Procedure 1**
**Preparing the Signaling Server for rack-mounting**

***Note:*** The Front Mount Bracket assembly is not intended for use as a slide rail system. The Signaling Server must be firmly attached to the rack.

**1** Make sure the Signaling Server is not plugged-in to an electrical outlet.

**2** Align the end of the rail (A in Figure 5) on the side of the Signaling Server with the flange (B in Figure 6 on page 45) toward the back of the Signaling Server. See Figure 6 on page 45.

**Figure 6**
**Support bracket**



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

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

4 Attach the bezel door to the faceplate of the Signaling Server, as shown in Figures 7 and 8 on page 46.

**Figure 7**
**Left hinge mount**

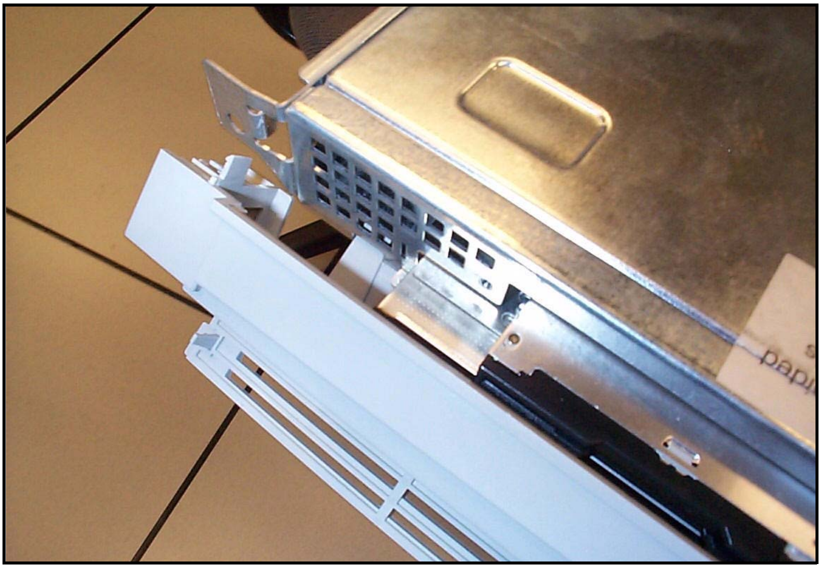
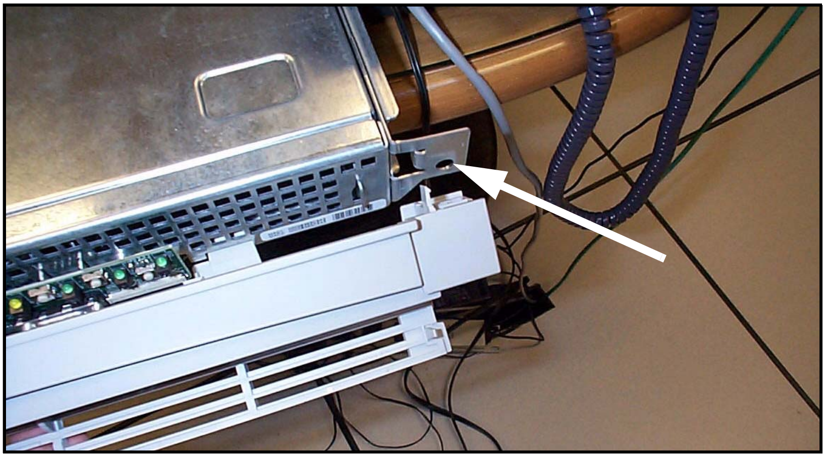
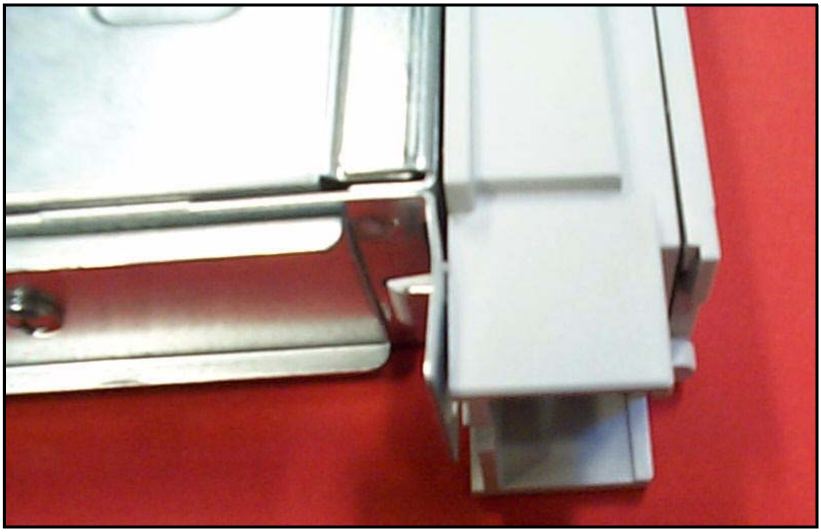


**Figure 8**
**Right hinge mount**



When the door is attached to the Signaling Server and rack-mount apparatus, it should appear as shown in Figure 9.

**Figure 9**
**Snapped-in bezel door**



**End of Procedure**

## Rack-mounting

Read the following warnings carefully before installing the Signaling Server in the rack.

**DANGER OF ELECTRIC SHOCK**
DISCONNECT AC POWER

Make sure the Signaling Server is completely disconnected from any AC power source before performing this procedure. Pressing the Power button DOES NOT turn off power to the Signaling Server. Some circuitry in the Signaling Server can continue to operate even though the front panel Power button is off. Failure to disconnect the Signaling 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 just to the Signaling Server(s).

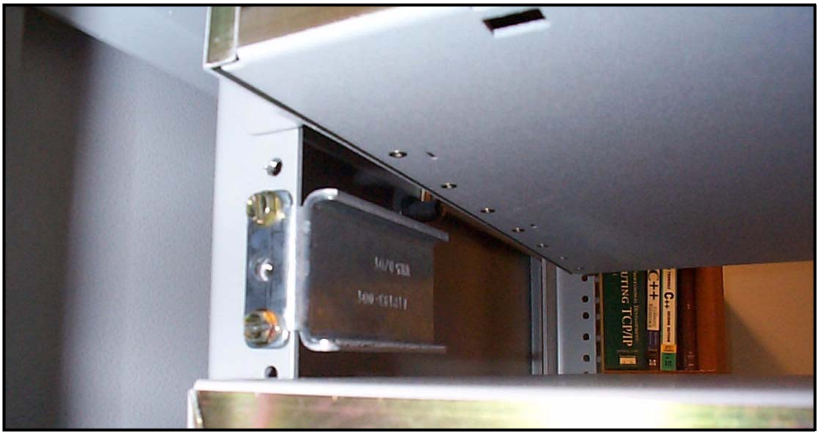
**Damage to Equipment**
OVERCURRENT PROTECTION

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

**Procedure 2**
**Rack-mounting the Signaling Server**

**1** Attach the rack-mount brackets (B in Figure 5 on page 44) to the front of the equipment rack. Install the left and right side at an equal height. Use standard length screws from the accessories pouch, and screw them into the top and bottom drill holes of the bracket. See Figure 10 on page 49.

**Figure 10**
**Installed rack-mount bracket**



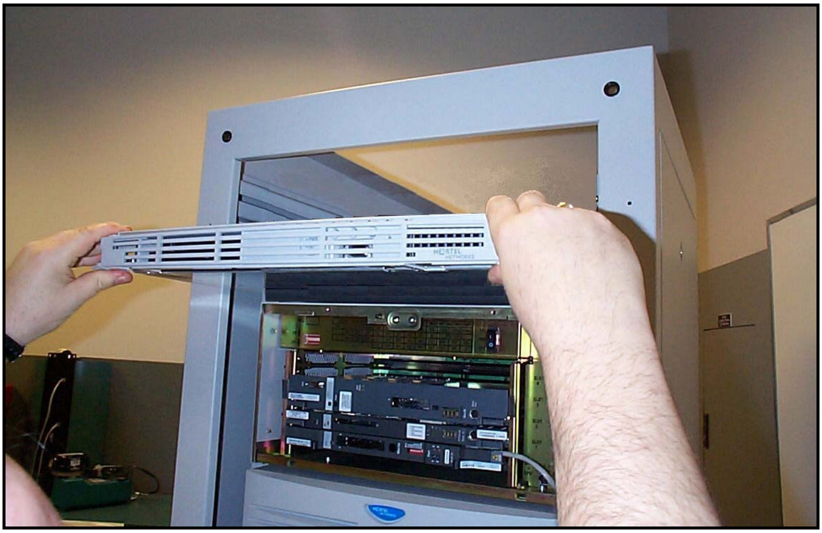
**2** When both brackets are fixed in place, do the following:

**a.** Align the rack-mount brackets on the Signaling Server with the slide rail system on the rack posts.

**b.** Slide the Signaling Server in place.

Refer to Figure 11 on page 50.

**Figure 11**
**Rack-mounting the Signaling Server**



3 Tighten the screws through the faceplate of the Signaling Server to the rack-mount bracket.

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

**End of Procedure**

## Connecting and powering up the Signaling Server

**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.

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

**Procedure 3**
**Connecting and powering up the Signaling Server**

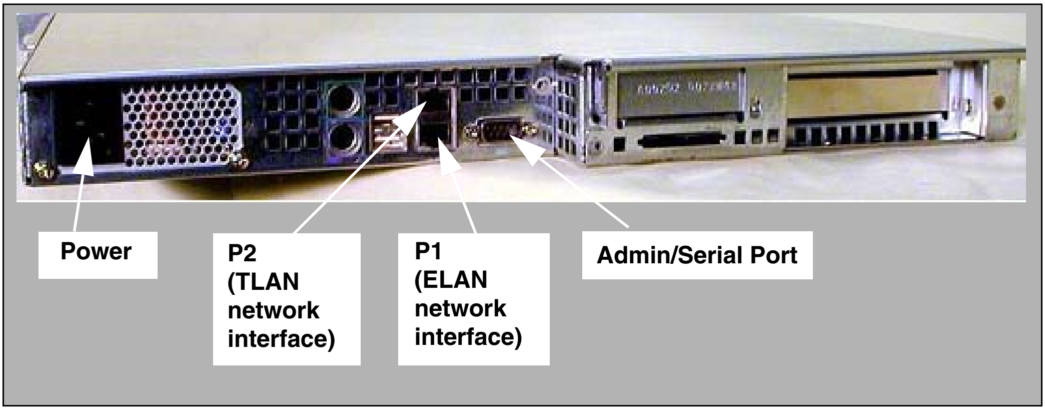
**1** Connect the Signaling Server to the TLAN subnet.

Insert the RJ-45 CAT5 (or better) cable into the P2 port (TLAN network interface) on the back of the Signaling Server. The P2 port (TLAN network interface) is the top one of the two network interfaces shown in Figure 12.

**2** Connect the Signaling 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 one of the two network interfaces shown in Figure 12.

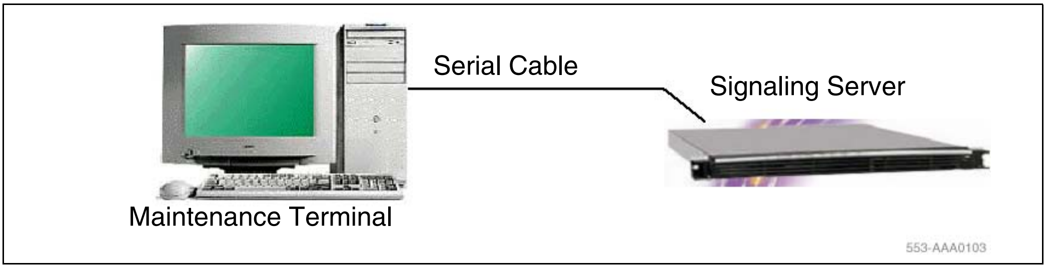
**Figure 12**
**Back of Signaling Server**



**3** Connect a maintenance terminal to the Signaling Server.

**a.** Connect a DTE–DTE null modem serial cable (supplied with the Signaling Server) from the Serial Port on the back of the Signaling Server to a maintenance terminal. The connection looks like that shown in Figure 13 on page 52.

**Figure 13**
**Maintenance to Signaling Server connection**



**b.** Set the COM port on the maintenance terminal as follows:

- Terminal type: VT100
- Speed: 19 200
- Data bits: 8
- Parity: none
- Stop bits: 1
- Flow control: none

***Note:*** The Signaling Server is shipped with the Admin/Serial port set to 19 200 Bit/s. Other available speeds are 38 400 and 115 200 Bit/s. Once the Signaling Server software has been installed, you can change the port speed using the Tools Menu on the Signaling Server Install Tool. See Procedure 39 on page 239.

**4** Configure the maintenance terminal.

The maintenance terminal can be configured any time, except during data transmission. Do not configure the terminal during data transmission to avoid data loss.

**a.** Turn on the power for the maintenance terminal.

**b.** Enter setup mode by pressing the **`SETUP`** key located on the top row of the special function keys. The terminal screen displays the current setup values.

c. Change the value in each field on each setup screen as necessary. Use the keys listed in Table 7 to view and change setup values.

**Table 7**
**SDI key function**

| **Key** | **Function** |
|---|---|
| Arrow | Move from field to field |
| Enter | Scroll through possible values or cause requested action to occur (depends on type of field) |
| Next Screen | Move to next setup screen |
| Prev Screen | Move back to last screen |

d. Save changes by returning to the **General setup** screen, moving the cursor to the **Saved** field, and pressing **Enter**.

To configure the maintenance terminal, refer to “Maintenance terminal configuration parameters” on page 56.

5 Connect the Signaling Server power cord.

a. Check that the power cord is the type required in the region where the Signaling Server is used.

Do not modify or use the supplied AC power cord if it is not the correct type. Refer to *Communication Server 1000S: Installation and Configuration* (553-3031-210) for a detailed power cord description.

b. Attach the female end of the power cord to the mating AC power receptacle on the left side of the Signaling Server’s back panel. See Figure 12 on page 51. Plug the male end of the AC power cord into the AC power source (wall outlet).

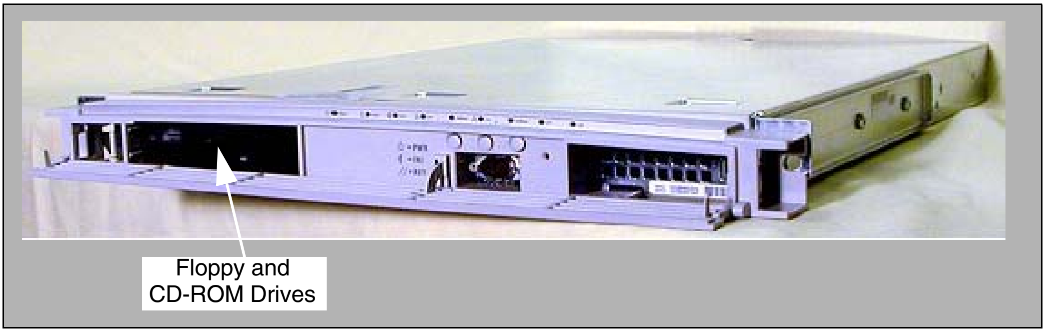
6 Power up the Signaling Server.

a. Open the bezel door (Figure 14 on page 54) to access the Power switch:

i. Grasp the tab at each end of the hinged bezel door.

ii. Gently pull the tabs out and down to open the hinged bezel door.

Figure 14
Signaling Server with open bezel door



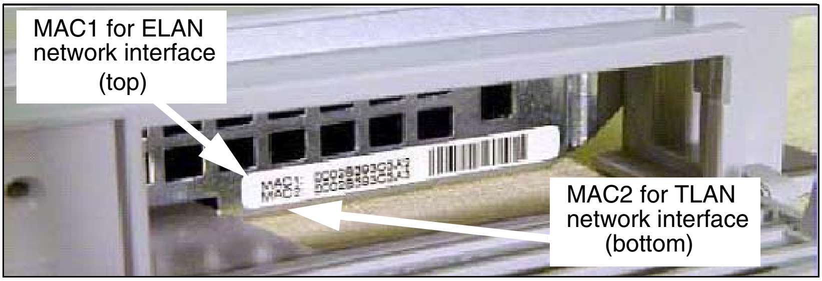
***Note 1:*** The MAC addresses are visible on the lower right-hand side when the bezel door is open. See Figure 15 on page 54.

***Note 2:*** MAC1 is Port 1 (ELAN network interface), and MAC2 is Port 2 (TLAN network interface).

***Note 3:*** Though the MAC1 address is the top address, Port 1 is the bottom network interface on the back of the Signaling Server.

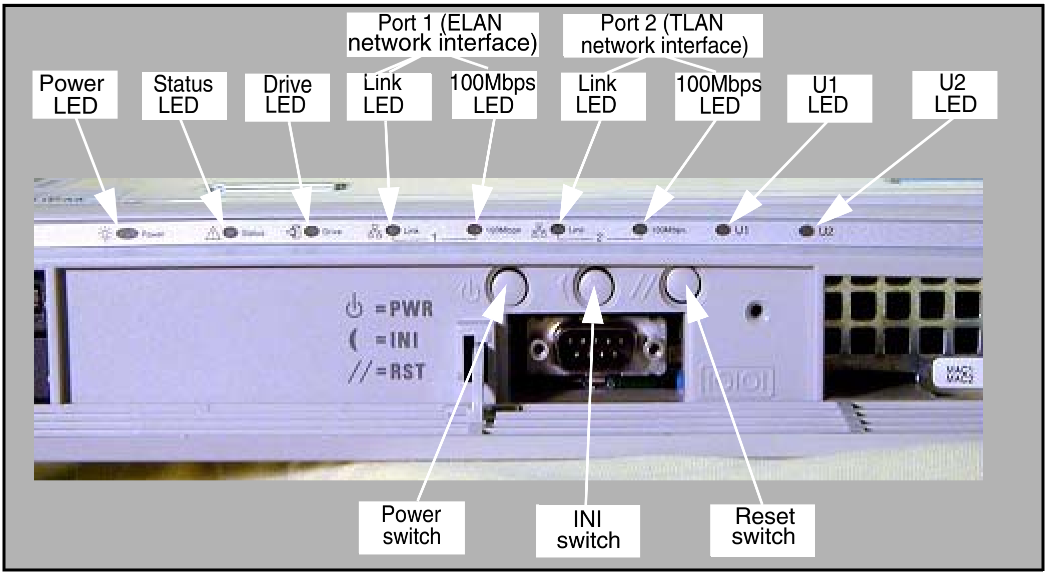
***Note 4:*** Figure 16 on page 55 shows the LEDs that correspond to the ELAN and TLAN network interfaces.

Figure 15
MAC address



**b.** Press the Power switch (Figure 16). Notice that the green LED power indicator is lit.

**Figure 16**
**Signaling Server indicators and power switch**



The Signaling 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 Mbps - Green LED on, Ethernet port running at 100 Mbps; LED off, Ethernet port running at 10 Mbps.

***Note:*** When the power is turned off on a Signaling Server, the two Link LEDs for Port 0 and Port 1 continue to flash. Depress the Power button for approximately seven seconds to completely turn the power off.

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

**End of Procedure**

## Maintenance terminal configuration parameters

This section contains the parameters for configuring one of the following maintenance terminals for use with the Signaling Server:

- HP700/32 — see Table 8 on page 57
- VT420 — Table 9 on page 58
- VT220 — Table 10 on page 59

Use these parameters in conjunction with Table 7 on page 53.

**Table 8**
**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 | Clr 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. | |

**Table 9**
**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 | |

**Table 10**
**VT220 setup values**

```
Global Set-Up
On Line                             Comm1=RS232
Sessions on Comm1                                         70Hz
CRT Saver                           Printer Shared

Display Set-Up
80 Columns                          Light Text, Dark Screen
Interpret Controls                  Cursor
Auto Wrap                           Block Style Cursor
Jump Scroll

General Set-up
VT200 Mode, 7-bit Controls          Application Keypad
User Defined Keys Unlocked          Normal Cursor Keys
User Features Unlocked              No New Line
Multinational

Communications Set-Up
Transmit=2400                       No Local Echo
Receive=Transmit                    Data Leads Only
Xoff at 64                          Disconnect, 2 s Delay
8bits, No Parity                    Limited Transmit
1 Stop Bit


Printer Set-Up
Speed=9600
Normal Print Mode                   Print Full Page
8bits, No Parity,                   Print National Only
1 Stop bit                          No Terminator

Keyboard Set-up
Typewriter Keys                     Warning Bell
Caps Lock                           Break
Auto Repeat                         Answerback=
Keyclick High                       Not Concealed
Margin Bell

Tab Set-Up Screen
Leave this screen at the default values
```

# Upgrading the Signaling Server memory

For capacity reasons, the memory on the Signaling Server has been increased from 256 Mbytes to 512 Mbytes. 256 Mbytes is more than sufficient for Succession 1000 Release 1.0 and 2.0 systems in smaller environments (less than 1000 IP Phones). This change applies to all Signaling Servers shipped with Succession 3.0 Software or later.

For CS 1000 Release 4.0 or higher, all Signaling Servers must be equipped with at least 512 MBytes of memory. In addition, any Signaling Server running the Personal Directory, Callers List, and Redial List features and serving over 10 000 IP Phone users must be equipped with 1 GByte of memory.

To enable customers to redeploy their current NTDU27AA 01, 02, or 03 Signaling Servers into a CS 1000 Release 4.0 or higher environment, a Signaling Server Memory Upgrade Kit (NTDU80) is available. Two NTDU80 Upgrade Kits can be used to provision 1 GByte of memory on any 256-MByte or 512-MByte Signaling Server.

Appendix A on page 243 provides installation instructions for upgrading the memory using this kit.

# Signaling Server Software Install Tool

## Contents

This section contains information on the following topics:

## Introduction

The Signaling Server Software Install Tool runs from the Signaling Server Software CD-ROM. Use this tool to:

- install Signaling Server software (see “Software installation and configuration” on page 65)
- upgrade Signaling Server software (see “Software upgrade and reconfiguration” on page 95)
- reconfigure the Signaling Server (see “Software upgrade and reconfiguration” on page 95)
- run Signaling Server utilities, such as backing up and restoring an IP Telephony configuration (see “Maintenance” on page 233)

***Note:*** The Signaling Server is out-of-service during software installation or upgrade.

To perform a software installation or upgrade, reboot the Signaling Server with the Software CD-ROM in its drive. No floppy disk is required, since the Software CD-ROM is bootable.

The Install Tool installs all Signaling Server software, including the operating system, applications, and web files. The Install Tool also copies software files for the Voice Gateway Media Cards and IP Phones, which are used to upgrade these components. For a new installation, the Install Tool prompts for IP Telephony parameters to perform basic system configuration.

After installing the Signaling Server software and configuring basic information about the Signaling Server, the Signaling Server components can be configured using the web-based Element Manager interface. Refer to *Element Manager: System Administration* (553-3001-332).

## Signaling Server Software CD-ROM

If you do not have the latest version of the CD-ROM:

- Order or download the CD-ROM image from the Nortel Electronic Software Download site. See Procedure 4 on page 62 for instructions on downloading the image.
- Create the Install Tool CD-ROM from the image. See Procedure 5 on page 63.

A single ".iso" file is provided to create the Software CD-ROM. 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. As the CD image is preconfigured, your software automatically creates a bootable CS 1000 Release 4.5 CD-ROM. See your software's help pages to create a CD from an ISO file. Also review the associated README file that is associated with the Nortel Signaling Server Software download.

**Procedure 4**
**Downloading the Signaling Server CD image**

1 Connect to the Nortel website at http://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 displays.

c. Click **Communication Servers**. The **By Product Family** page opens.

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

**3** Download the Signaling Server CD image.

a. Click on the link for the appropriate **Signaling Server CD image**.

The CD-ROM image includes the Signaling Server software as well as IP Phone firmware and Voice Gateway Media Card loadware.

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

***Note:*** If you are not registered to access this web site, refer to the CS 1000 product bulletin for directions on how to register.

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 of Procedure**

**Procedure 5**
**Creating a Signaling Server Software CD-ROM**

**1** Use the software option to “burn” or “create” a CD from the CD image. Do not drag-and-drop, as this can result in a file copy and a CD-ROM that does not work. Do not write the ISO file to the CD-ROM.

***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.

**End of Procedure**

The Software CD-ROM must be readable in a standard CD-ROM 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's software documentation.

Once the CD is created, you can use it to install new software or upgrade software on an existing Signaling Server.

# Software installation and configuration

## Contents

This section contains information on the following topics:

## Introduction

This chapter explains how to install Signaling Server software on a new Signaling Server and perform basic configuration. If you are upgrading the software, see “Software upgrade and reconfiguration” on page 95.

## Before you begin

Before installing the software, you must do the following:

- Connect and power up the Signaling Server—use Procedure 3 on page 51.
- Obtain the Signaling Server Software Install CD-ROM—see “Signaling Server Software CD-ROM” on page 62.

# Installing the software

The Signaling Server requires a minimum of 512 MB of RAM to run CS 1000 Release 4.5 software. If the Signaling Server must support more than 382 H.323 virtual trunks, a minimum of 768 MB of RAM is required. If necessary, use Procedure 41 on page 246 to upgrade the RAM before beginning this procedure.

Use Procedure 6 to install the software on a new Signaling Server.

**Procedure 6**
**Installing the Signaling Server software**

After you complete step 1 below, this procedure takes approximately 20 minutes.

**1** From your Planning and Engineering group, obtain the following network and IP Telephony data for this Signaling Server:

- node ID for the IP Telephony node
- node IP address for the IP Telephony node
- hostname 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 Configuration* (553-3001-213))
- NRS role, if applicable (refer to *IP Peer Networking: Installation and Configuration* (553-3001-213))

**2** Insert the Software CD-ROM into the Signaling Server CD drive, and press the **RST** button on the front panel to cold-reboot the Signaling Server.

***Note:*** The Software CD-ROM should be bootable. If not, create a boot floppy using the files in the `/mkboot` directory on the Signaling Server Software CD-ROM.

**3** If this is a re-installation on an existing system, observe the boot sequence. Enter **c** at the boot menu shown in Figure 17 on page 67.

***Note 1:*** Entering **c** in the “ISP1100 System Boot” banner screen speeds up this process, as the keyboard input is buffered.

***Note 2:*** If you do not select **c** within the ten-second time-out, the Signaling Server boots to the existing software on the hard disk.

**Figure 17**
**Upgrade boot sequence**

```
       ISP1100 System Boot
Copyright 2002-2005 Nortel Networks, Inc.

CPU: PC PENTIUM
Version: x
BSP version: 1.2/0
Creation date: Apr 4 2005, 15:44:38
ataDrv 1.0: ATAPI Drive Found
Controller 1 drive 0
Controller 1 drive 1
ATAPI Controller 1 #drives found = 1
Read boot parameters from:
[C]DROM
[H]ard Disk
5 [H]
```

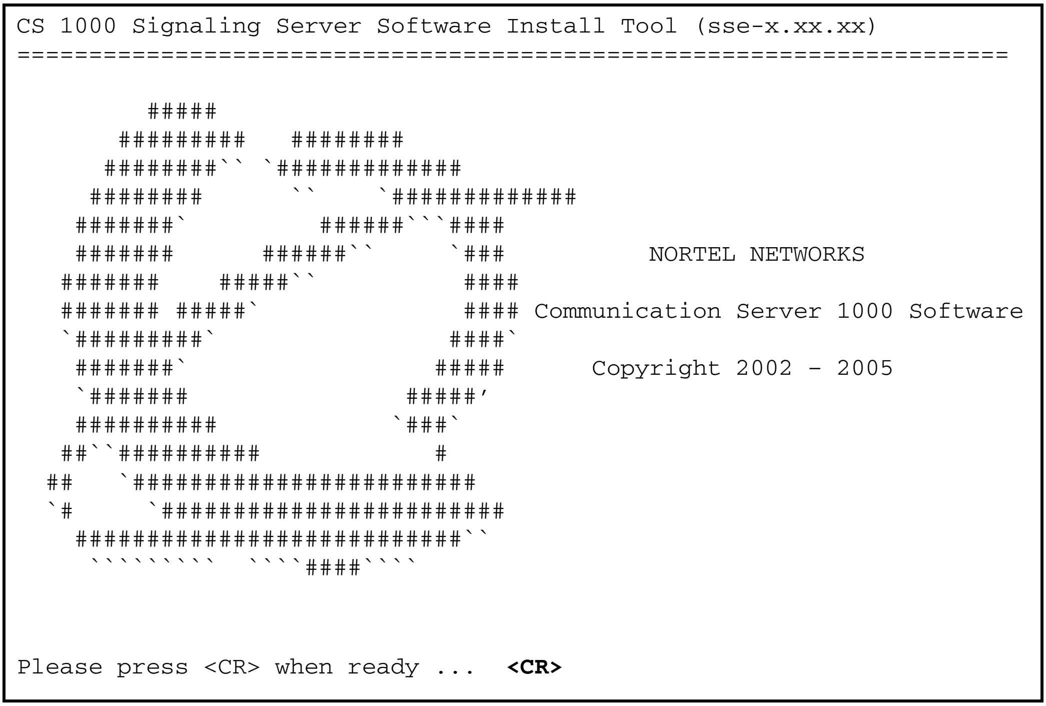
**4** Enter **b** at the menu shown in Figure 18.

**Figure 18**
**Copy IP configuration**

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

Please insert an empty diskette in the floppy drive
to backup the IP configuration.

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

        Enter Choice>
```

5 When the Install Tool banner appears (Figure 19 on page 68), press <CR> to perform system checks and begin software installation.

**Figure 19**
**Install Tool banner screen**



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

         #####
       #########  ########
      ########`` `#############
     ########      ``     `#############
    #######`         ######```####
    #######      ######``     `###          NORTEL NETWORKS
   #######    #####``         ####
   ####### #####`             #### Communication Server 1000 Software
   `#########`               ####`
    #######`                #####      Copyright 2002 - 2005
    `#######              #####'
    ##########           `###`
   ##``##########           #
  ##   `########################
  `#      `########################
    ###########################``
     `````````  ````####````


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

***Note:*** If the system has less than 512 MBytes of RAM, the following error message appears:

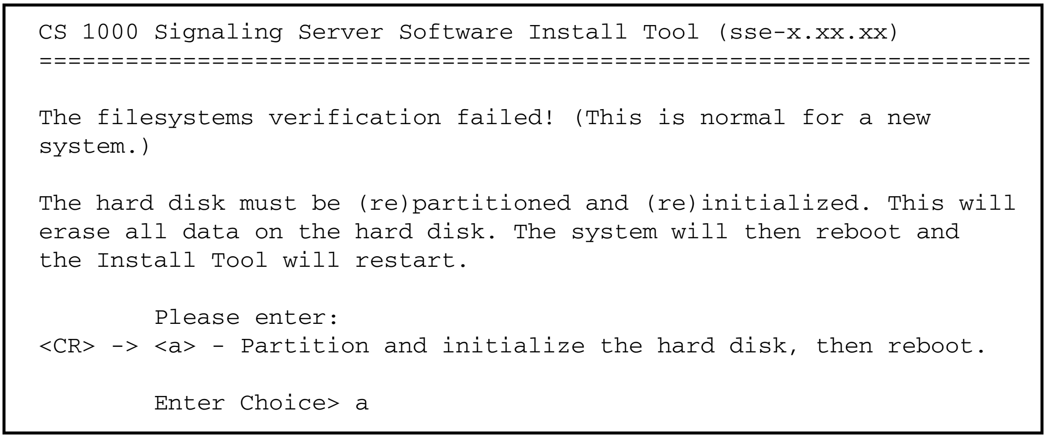
```
WARNING: Your system has less than 512 MB RAM.
In order to run Rls 4.5 software you must
upgrade RAM to 512 MB and repeat install.
Otherwise serious service problems are likely

   Please enter:
<CR> -> <q> - Quit.
        <a> - Accept the possible risks and
continue install.
```

Press <CR> to quit. Use Procedure 41 on page 246 to upgrade to 512 MBytes of RAM and restart the Signaling Server Install Tool again.

The system verifies the file systems.

- When the software runs for the first time on a new system, the hard disk will not be partitioned, so the test normally fails. Upon failure, the menu in Figure 20 appears.

**Figure 20**
**First boot of a new system**



```
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
```

**a.** Enter **a** to start the new installation.

The system displays the messages:

```
Partitioning hard disk ...
Hard disk partitioning succeeded.
```

```
Creating filesystems ...
Filesystems creation succeeded.
```

```
Rebooting system ...
```

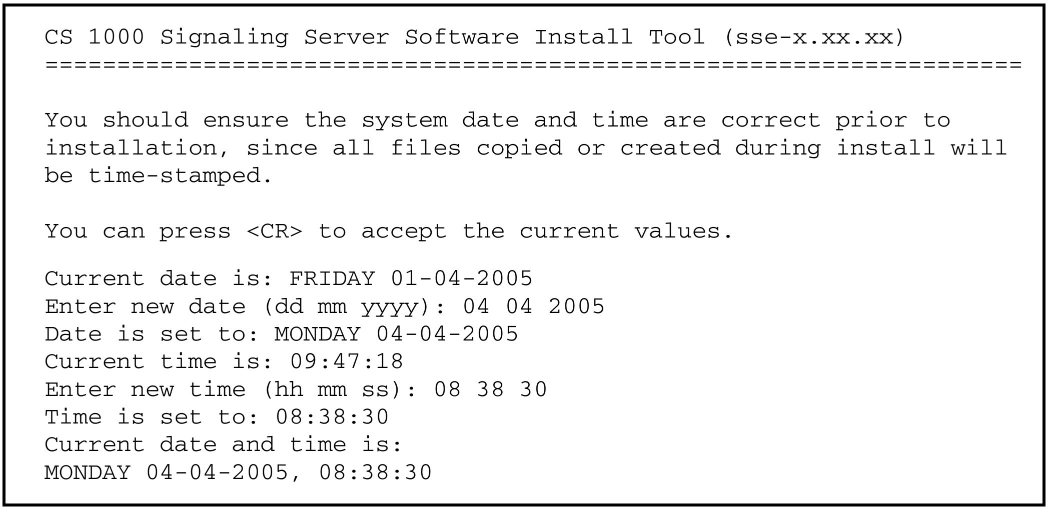
b. The Install Tool banner screen (Figure 19 on page 68) reappears. Press <CR> to verify the filesystems.

The disk check reports:

```
Filesystems verification succeeded.
```

c. Confirm or enter the date and time (Figure 21 on page 70).

**Figure 21**
**Date and time**



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

You should ensure 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 01-04-2005
Enter new date (dd mm yyyy): 04 04 2005
Date is set to: MONDAY 04-04-2005
Current time is: 09:47:18
Enter new time (hh mm ss): 08 38 30
Time is set to: 08:38:30
Current date and time is:
MONDAY 04-04-2005, 08:38:30
```

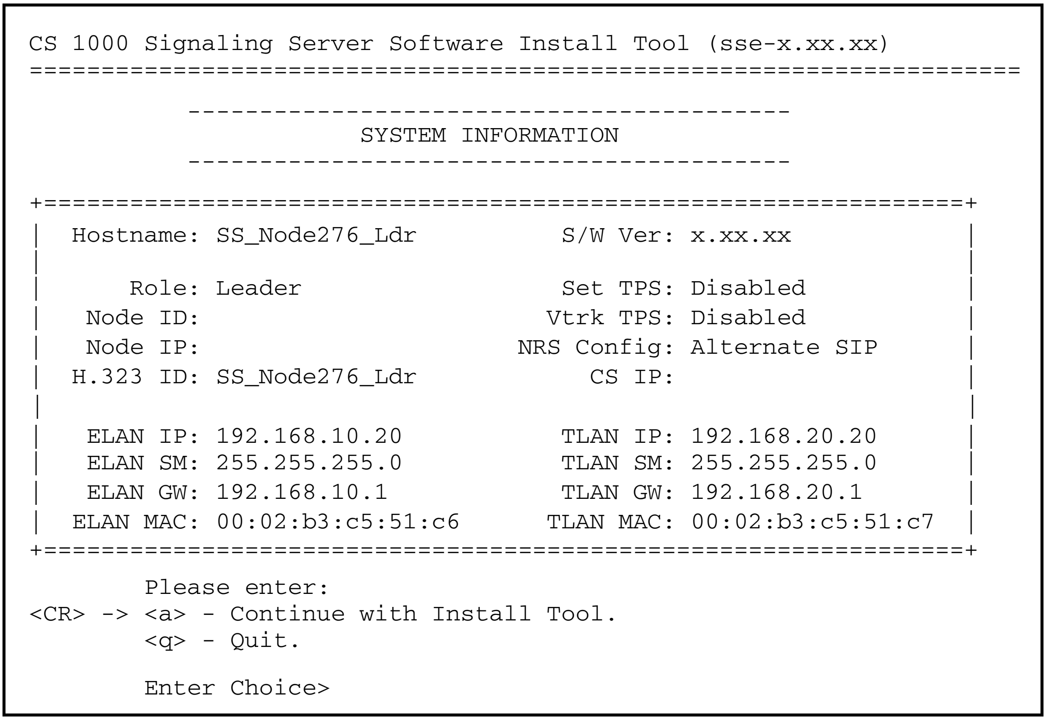
- When reinstalling the software on an existing system, the system verifies the file systems. The disk check reports:

  ```
  Filesystems verification succeeded.
  ```

  The system summary appears (Figure 22 on page 71). Enter **a** to continue the installation.

  ***Note:*** For a new installation, the data fields in the system summary are blank.

**Figure 22**
**System Summary**

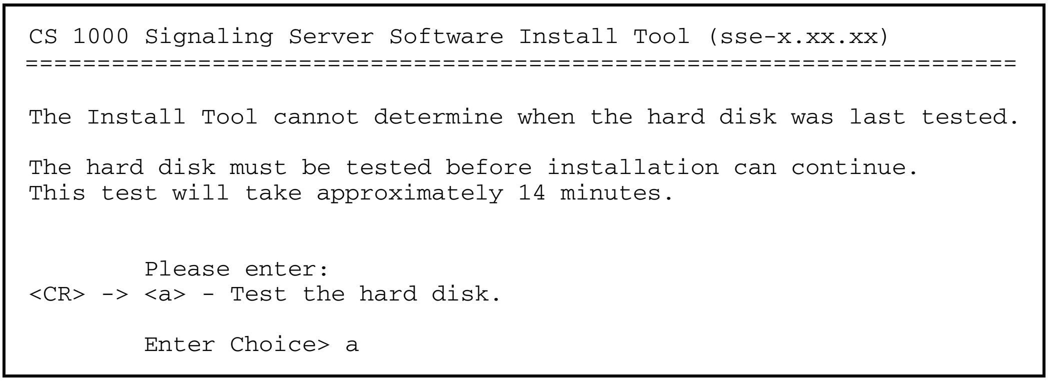


```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

           ------------------------------------------
                       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>
```

6 Test the disk.

- If the hard drive has never been tested or is corrupt, enter **a** at the menu shown in Figure 23 on page 72.

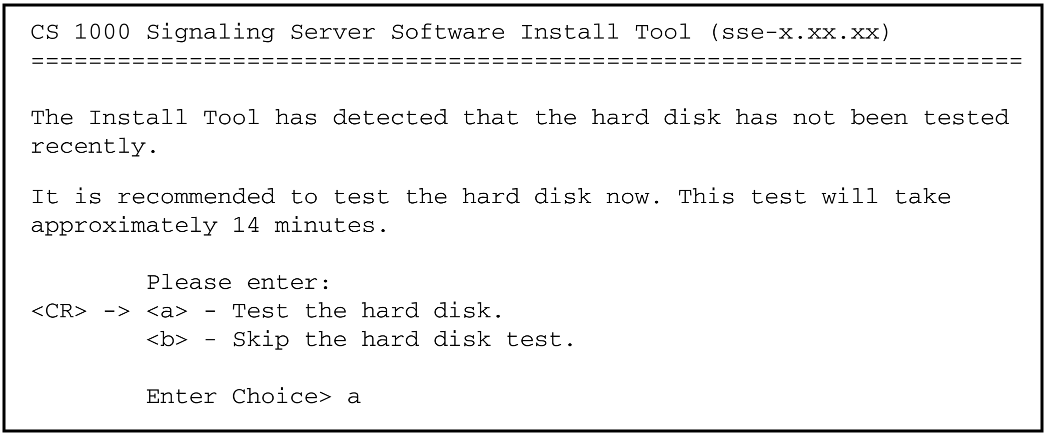
**Figure 23**
**Hard disk test**



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

The Install Tool cannot determine when the hard disk was last tested.

The hard disk must be tested before installation can continue.
This test will take approximately 14 minutes.


        Please enter:
<CR> -> <a> - Test the hard disk.

        Enter Choice> a
```

- If the hard disk has not recently been tested, enter **a** at the menu shown in Figure 24.

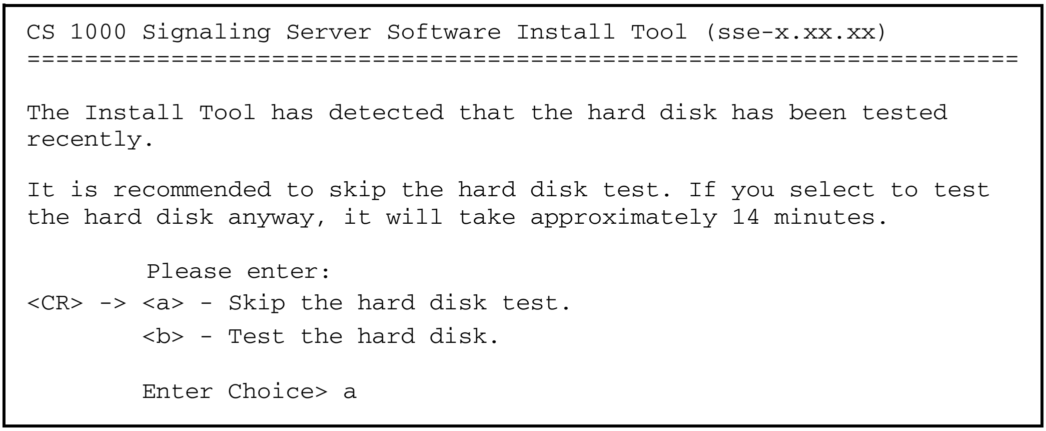
**Figure 24**
**Not recently tested**



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

The Install Tool has detected that the hard disk has not been tested
recently.

It is recommended to test the hard disk now. This test will take
approximately 14 minutes.

        Please enter:
<CR> -> <a> - Test the hard disk.
        <b> - Skip the hard disk test.

        Enter Choice> a
```

- If the hard disk has been checked in the last 24 hours, enter **a** at the menu shown in Figure 25 on page 73.

**Figure 25**
**Tested within 24 hours**



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

The Install Tool has detected that the hard disk has been tested
recently.

It is recommended to skip the hard disk test. If you select to test
the hard disk anyway, it will take approximately 14 minutes.

        Please enter:
<CR> -> <a> - Skip the hard disk test.
        <b> - Test the hard disk.

        Enter Choice> a
```

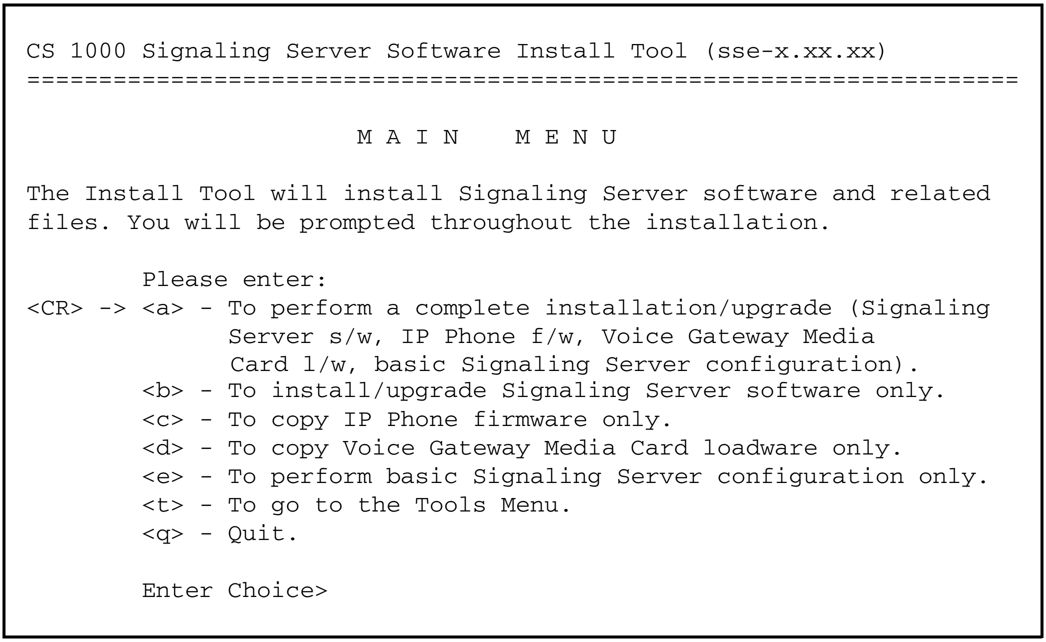
The following messages display on the screen:

```
Testing hard disk ...
Testing partition /u (4194241 blocks) ...
xxx% complete

Testing partition /p (4194241 blocks) ...
xxx% complete

Hard disk testing succeeded.
```

Where xxx = 0 to 100.

***Note:*** If the physical check did not pass, contact your technical support group.

**Figure 26**
**Install 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, IP Phone f/w, Voice Gateway Media
              Card l/w, basic Signaling Server configuration).
        <b> - To install/upgrade Signaling Server software only.
        <c> - To copy IP Phone firmware only.
        <d> - To copy Voice Gateway Media Card loadware only.
        <e> - To perform basic Signaling Server configuration only.
        <t> - To go to the Tools Menu.
        <q> - Quit.

        Enter Choice>
```

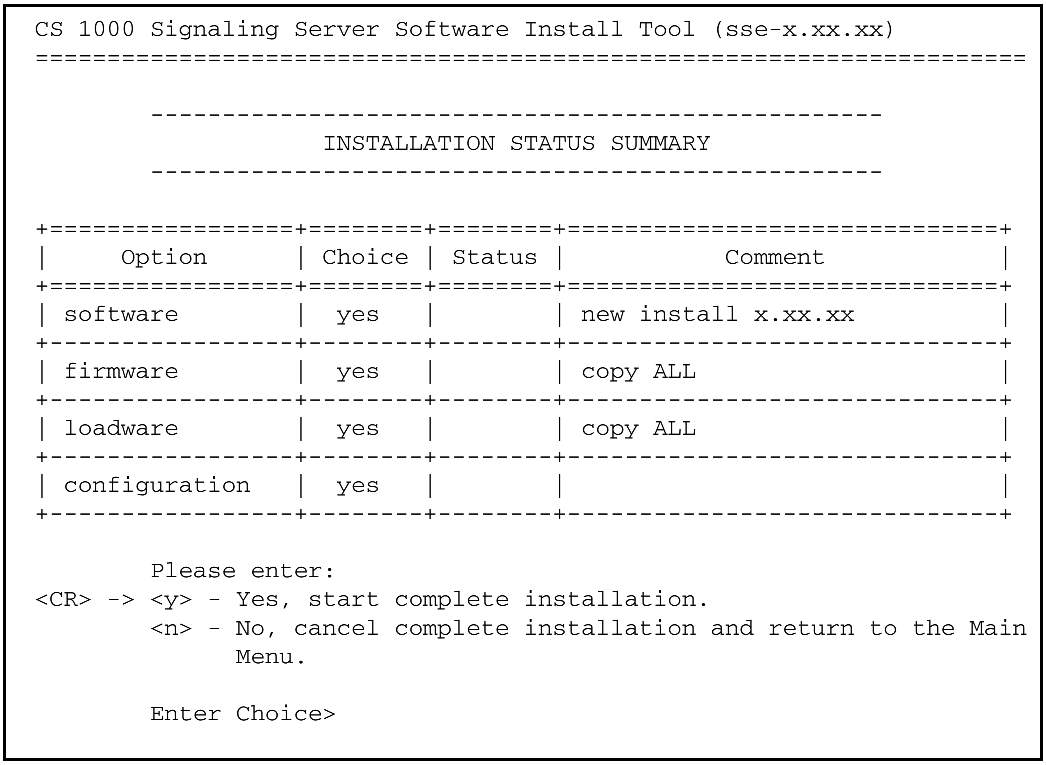
7 At the Main Menu (Figure 26), enter **a** to install Signaling Server software. Option **a** performs options **b**, **c**, **d**, and **e**.

The following sample lines display on the screen:

```
Copying "/cd0/sse37012.p3/disk.sys" to "/u/disk.sys".
Processing the install control file ...
"/cd0/sse37012.p3/install.dat" parsed.
```

The screen shown in Figure 27 on page 75 shows actions that can be performed.

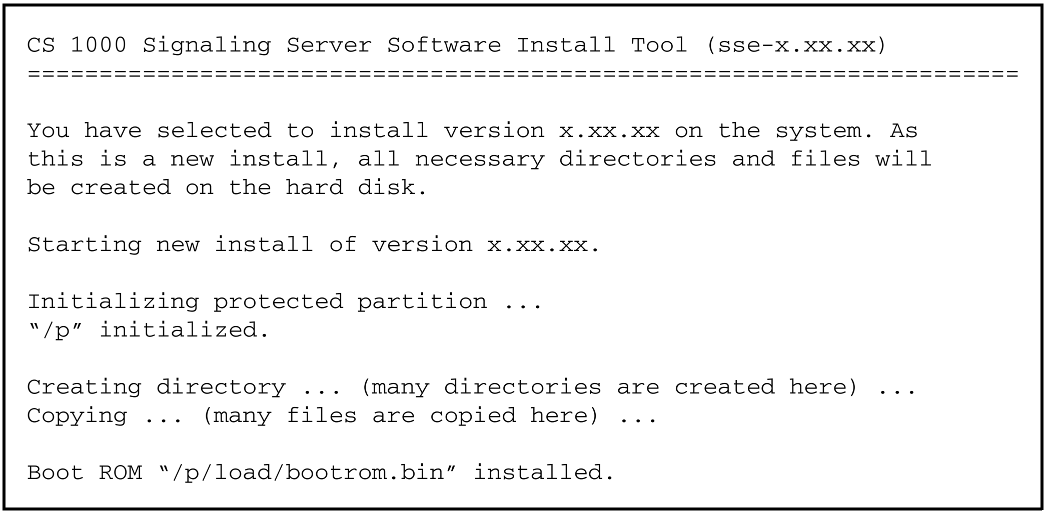
**Figure 27**
**Installation Status**



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


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


+==================+========+========+===============================+
|      Option      | Choice | Status |            Comment            |
+==================+========+========+===============================+
| software         |  yes   |        | new install x.xx.xx           |
+------------------+--------+--------+-------------------------------+
| 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>
```

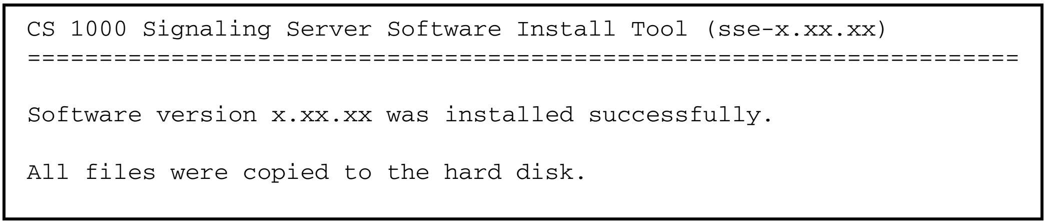
8 Enter **y** to start the installation. The screens shown in Figures 28 to 32, which start on page 78, appear.

**Figure 28**
**Installation output**



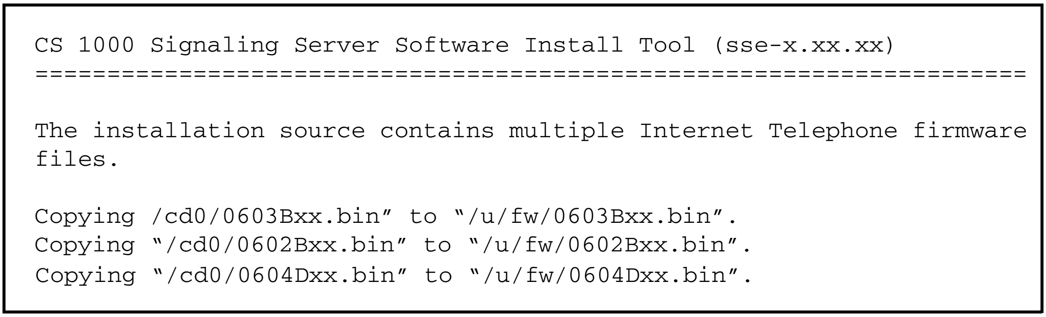
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

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 ...
“/p” initialized.

Creating directory ... (many directories are created here) ...
Copying ... (many files are copied here) ...

Boot ROM “/p/load/bootrom.bin” installed.
```

**Figure 29**
**Success**



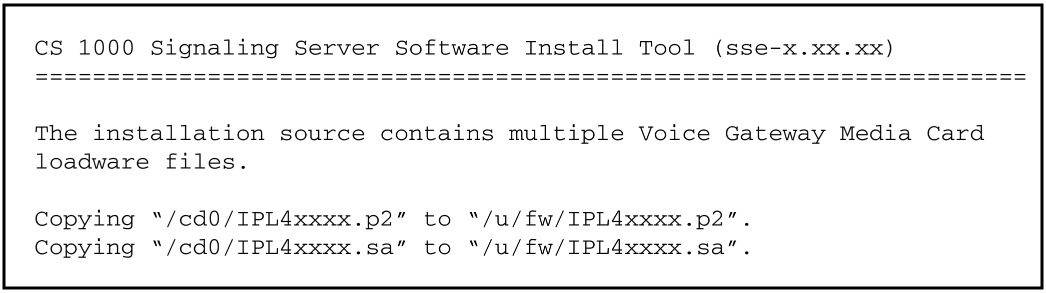
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

Software version x.xx.xx was installed successfully.

All files were copied to the hard disk.
```

**Figure 30**
**IP Phone firmware**



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

The installation source contains multiple Internet Telephone firmware
files.

Copying /cd0/0603Bxx.bin” to “/u/fw/0603Bxx.bin”.
Copying “/cd0/0602Bxx.bin” to “/u/fw/0602Bxx.bin”.
Copying “/cd0/0604Dxx.bin” to “/u/fw/0604Dxx.bin”.
```

**Figure 31**
**Voice Gateway Media Card loadware**



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

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

Copying “/cd0/IPL4xxxx.p2” to “/u/fw/IPL4xxxx.p2”.
Copying “/cd0/IPL4xxxx.sa” to “/u/fw/IPL4xxxx.sa”.
```

The system echoes the ELAN network interface MAC address.

```
For future reference, the ELAN MAC address is:
“00:02:b3:c5:51:c6”.
```

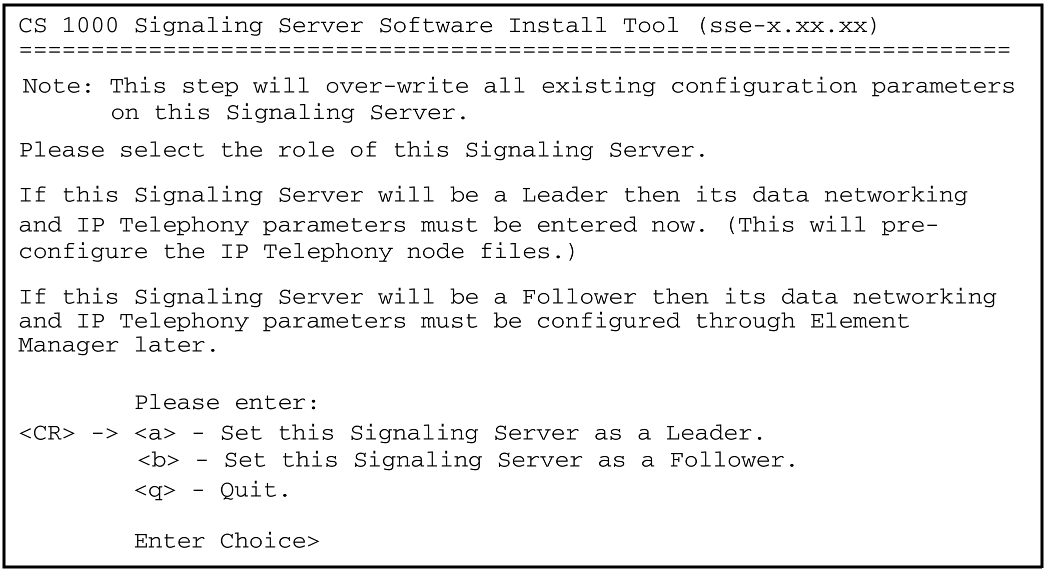
This address is found on the face of the Signaling Server, on the right-hand side when the bezel door is open. See Figure 15 on page 54.

***Note:*** The ELAN network interface MAC address must be configured in the Element Manager node configuration web page.

**9** Configure the Signaling Server as Leader or Follower. See Figure 32.

- If there is not already a Leader Signaling Server in the IP Telephony node, or if the Signaling Server is to be a stand-alone Signaling Server, enter **a** at the prompt to configure this Signaling Server as Leader.
- If there is already a Leader Signaling Server in the IP Telephony node, enter **b** at the prompt to set this Signaling Server as Follower. Then go to step 13 on page 82.

**Figure 32**
**Leader/Follower Signaling Server configuration**

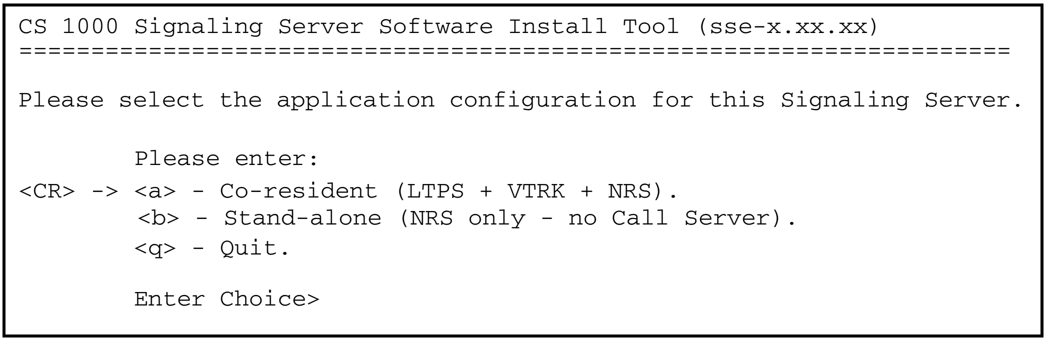


```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================
 Note: This step will over-write all existing configuration parameters
       on this Signaling Server.
Please select the role of this Signaling Server.

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>
```

**10** Configure the application configuration for this Signaling Server. See Figure 33.

- If the Set TPS, Virtual Trunk TPS, and optional Network Routing Service (NRS) applications are to be enabled on this Signaling Server, enter **a** at the prompt to configure this Signaling Server as a co-resident 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 co-resident Signaling Server. After you finished installing the Signaling Server software, you can disable the Set TPS and Virtual Trunk TPS in Element Manager (refer to *Element Manager: System Administration* (553-3001-332)).
  - — If this Signaling Server is not to be associated with a Call Server, enter **b** at the prompt to set this Signaling Server as a stand-alone Signaling Server.

**Figure 33**
**Application configuration**



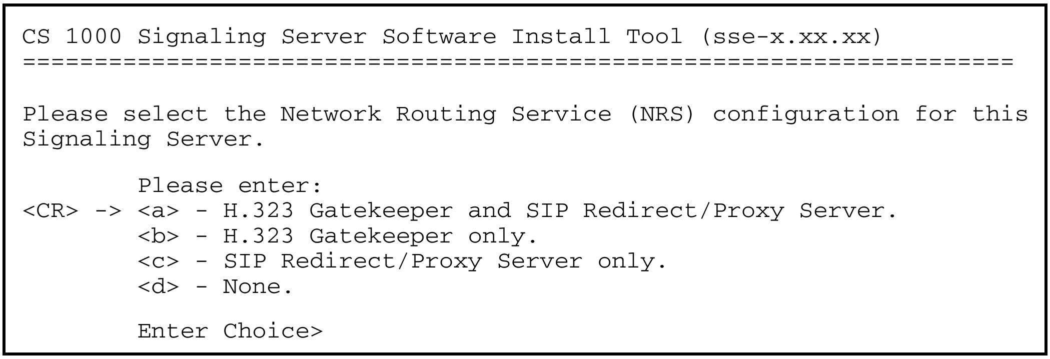
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

Please select the application configuration for this Signaling Server.

        Please enter:
<CR> -> <a> - Co-resident (LTPS + VTRK + NRS).
        <b> - Stand-alone (NRS only - no Call Server).
        <q> - Quit.

        Enter Choice>
```

11 Select the Network Routing Service (NRS) to be provided by this Signaling Server. See Figure 34 for a co-resident Signaling Server or Figure 35 on page 81 for a stand-alone Signaling Server.

- Enter **a** if this Signaling Server will provide an H.323 Gatekeeper and a SIP Redirect/Proxy Server.
- Enter **b** if this Signaling Server will provide only an H.323 Gatekeeper.
- Enter **c** if this Signaling Server will provide only a SIP Redirect/Proxy Server.
- Enter **d** if this Signaling Server is a Leader Signaling Server and will not provide an NRS. Go to step 13 on page 82.

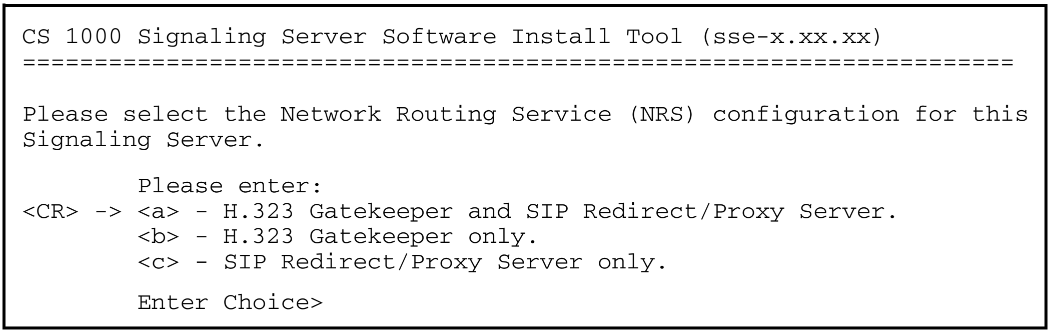
Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for more information on the NRS.

**Figure 34**
**Network Routing Service (NRS) — co-resident 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>
```

**Figure 35**
**Network Routing Service (NRS) — stand-alone Signaling Server**



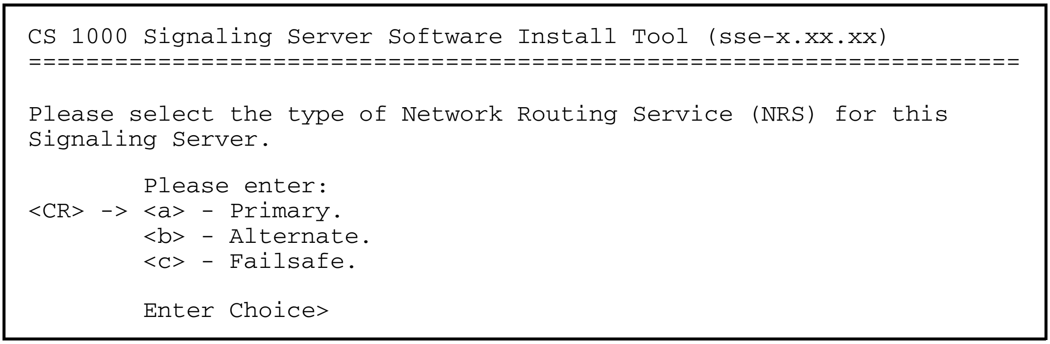
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
======================================================================

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>
```

**12** Select the type of NRS to be provided by this Signaling Server. See Figure 36 for a co-resident Signaling Server. See Figure 37 on page 82 for a stand-alone Signaling Server.

- 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 stand-alone Signaling Server and is to be the Failsafe NRS, enter **c**.

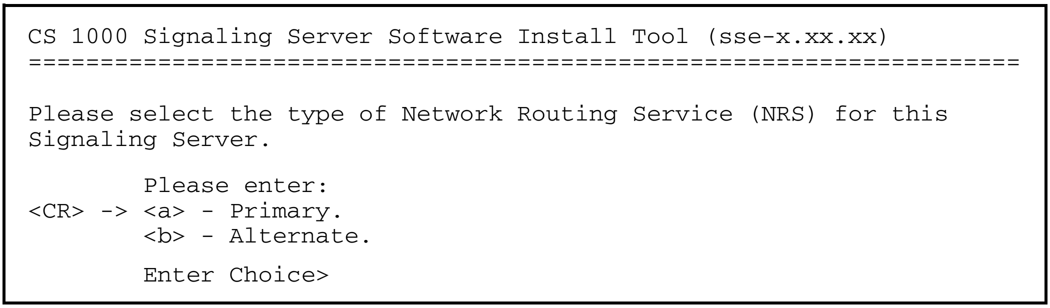
Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for more information on the NRS.

**Figure 36**
**NRS type — co-resident 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 37**
**NRS type — stand-alone 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>
```

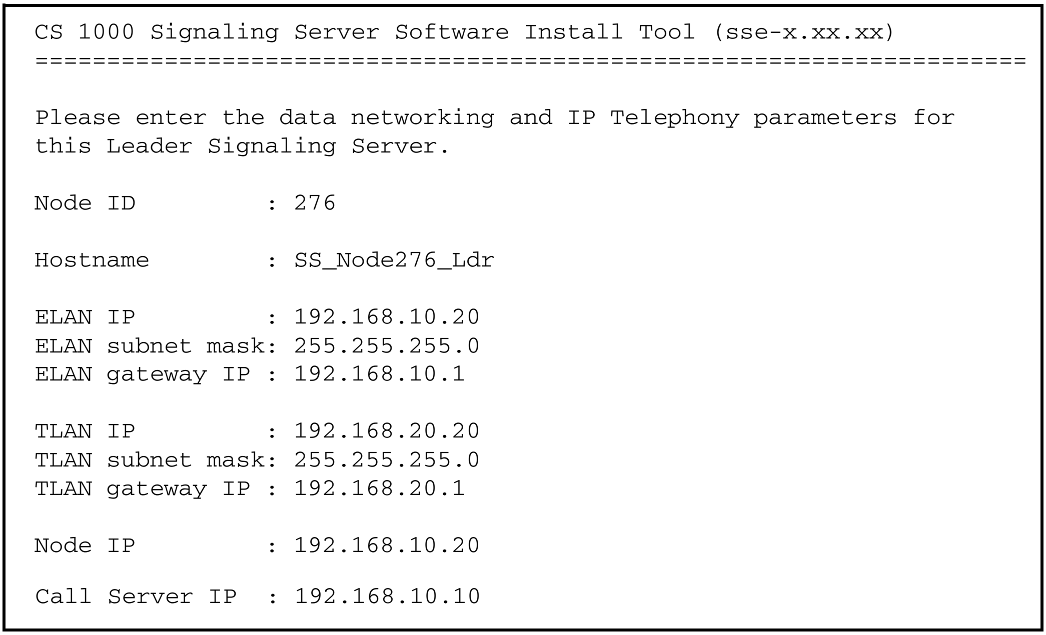
**13** Enter the data networking and IP telephony parameters for the Signaling Server, as prompted.

- If this is a Leader Signaling Server, enter the parameters for the Node, ELAN network interface, TLAN network interface, and Call Server as required. See Figure 38 on page 83. 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.
- If this is a Follower Signaling Server, enter the Hostname of the Leader Signaling Server. See Figure 39 on page 83. Then go to step 15 on page 85.
- If this is a stand-alone Signaling Server and not associated with a Call Server (that is, **b** was selected in step 10 on page 79), enter the TLAN subnet parameters as required. The Call Server IP address is automatically set to 0.0.0.0. See Figure 40 on page 84. Then go to step 14 on page 84.

The IP information applies to a temporary IP Telephony node. This ensures that the existing node is not impacted. This also preconfigures the IP Telephony node files. In “Importing IP Telephony node files” on page 179, the node files are imported to Element Manager for further configuration.

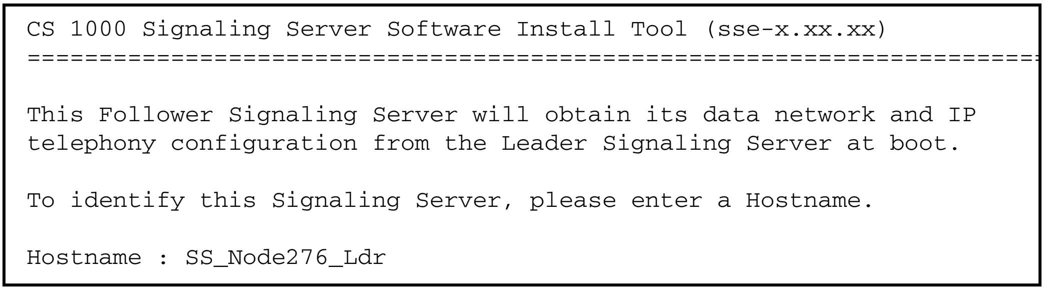
***Note:*** IP addresses shown in Figure 38, Figure 39 on page 83, and Figure 40 on page 84 are examples.

**Figure 38**
**Leader Signaling Server configuration**



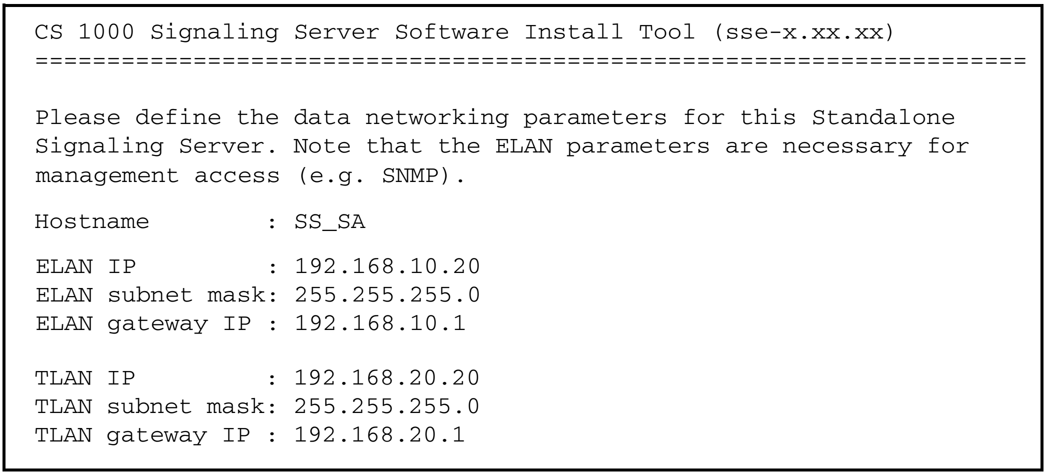
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

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 39**
**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
```

**Figure 40**
**Stand-alone Signaling Server configuration**



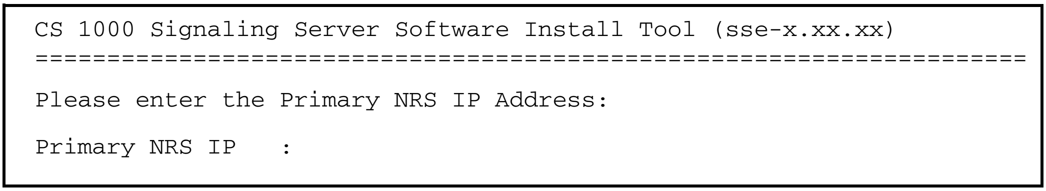
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

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
```

**14** Enter the Primary NRS IP address or the Alternate NRS IP address, depending on the option entered in step 11 on page 80 or step 12 on page 81.

- If **a** was entered in step 12, you can enter the address of the Alternate NRS if you know it, but it is not required. See Figure 42 on page 85.
- If **b** was entered in step 12, enter the address of the Primary NRS. See Figure 41 on page 85.
- If **c** was entered in step 12:
  - — Enter the address of the Primary NRS. See Figure 41.
  - — Enter the address of the Alternate NRS. See Figure 42.
- If **d** was entered in step 11:
  - — Enter the address of the Primary NRS (optional). See Figure 41.
  - — If you did enter the address of the Primary NRS, enter the address of the Alternate NRS (also optional). See Figure 42.

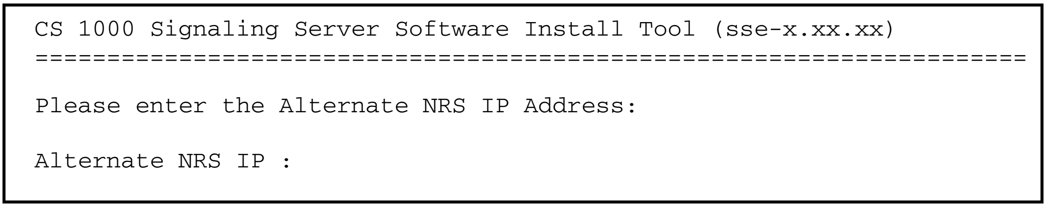
The Gatekeeper configuration can be updated later using Element Manager.

**Figure 41**
**Primary NRS IP address**



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

Please enter the Primary NRS IP Address:

Primary NRS IP   :
```

**Figure 42**
**Alternate NRS IP address**



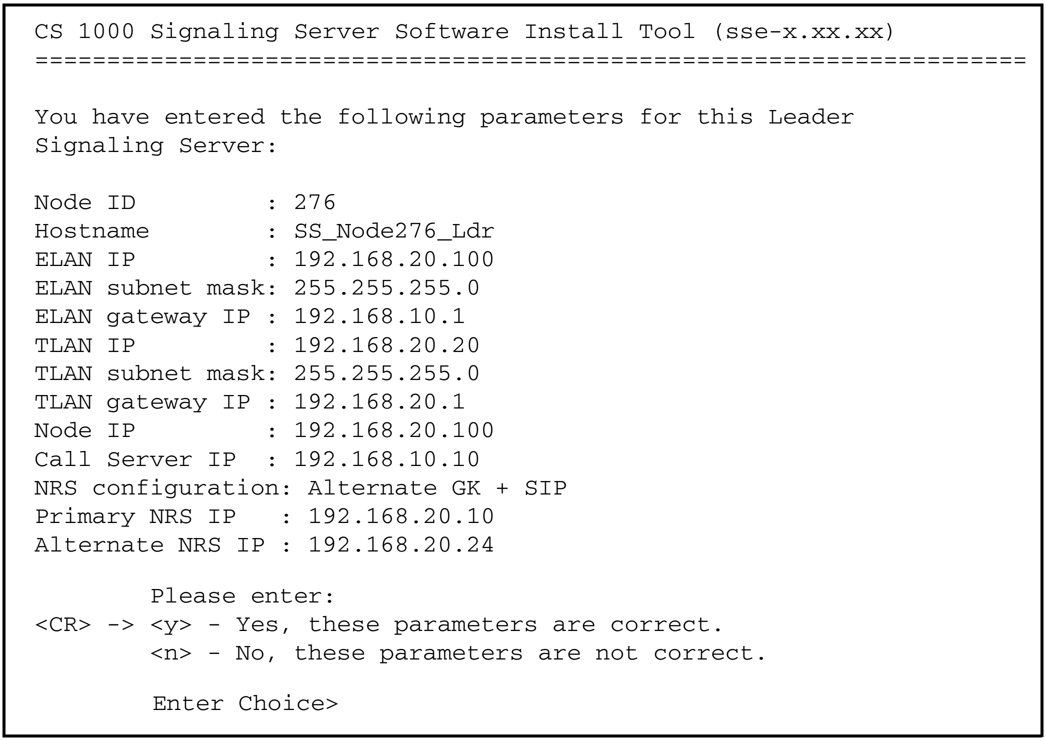
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

Please enter the Alternate NRS IP Address:

Alternate NRS IP :
```

**15** Enter **y** to confirm the parameters. See Figure 43 on page 86.

The example in Figure 43 is for a Leader Signaling Server configured with an Alternate H.323 and SIP NRS. The confirmation screens for a Follower and stand-alone Signaling Server are similar, showing the same list of parameters, specifically:

- The screen for the Follower Signaling Server displays only the value for the Hostname parameter; all other values are blank.
- The screen for the stand-alone Signaling Server displays values for the Hostname, ELAN network interface, TLAN network interface, and NRS parameters. The Node ID field is set to 0. The Call Server IP field is set to 0.0.0.0.

**Figure 43**
**IP Telephony parameter configuration**



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

You have entered the following parameters for this Leader
Signaling Server:

Node ID          : 276
Hostname         : SS_Node276_Ldr
ELAN IP          : 192.168.20.100
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          : 192.168.20.100
Call Server IP   : 192.168.10.10
NRS configuration: Alternate GK + SIP
Primary NRS IP    : 192.168.20.10
Alternate NRS IP : 192.168.20.24

        Please enter:
<CR> -> <y> - Yes, these parameters are correct.
        <n> - No, these parameters are not correct.

        Enter Choice>
```

The system echoes the ELAN network interface MAC address.

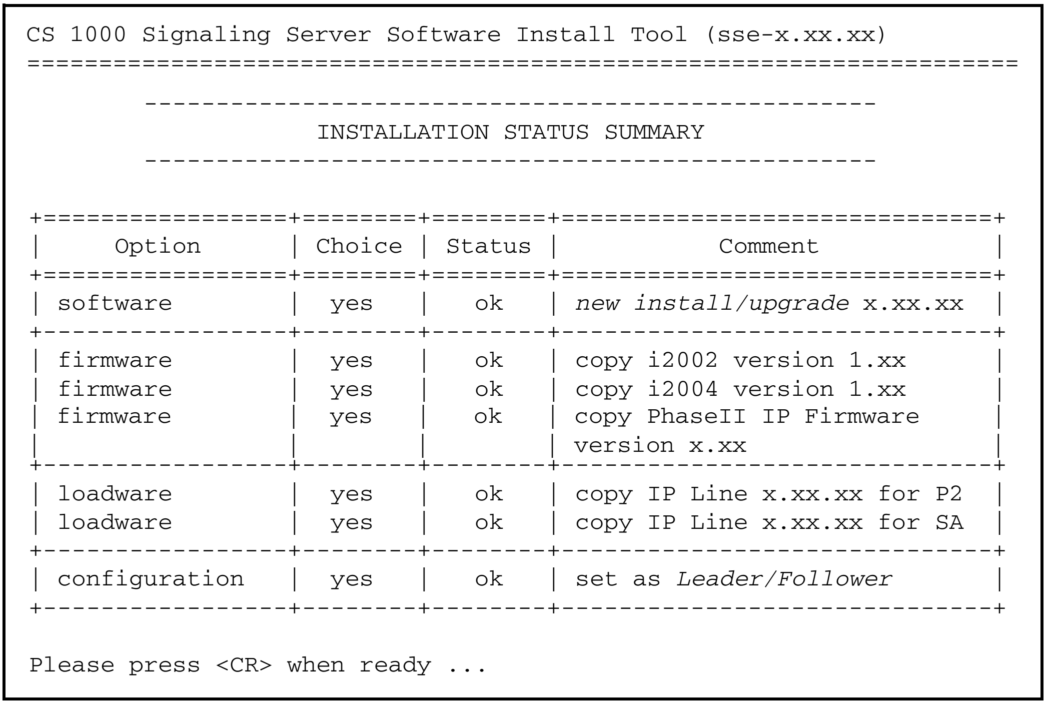
```
For future reference, the ELAN MAC address is:
“00:02:b3:c5:5l:c6”.
```

This address is on the face of the Signaling Server, on the right side when the bezel door is open. See Figure 15 on page 54.

***Note:*** The ELAN network interface MAC address must be configured in the Element Manager node configuration web page.

**16** To complete the installation, the Installation Status Summary screen appears as shown in Figure 44 on page 87.

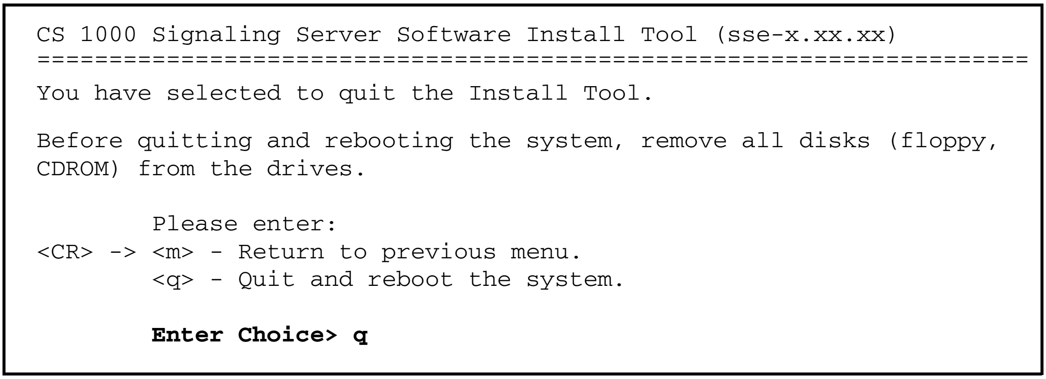
**Figure 44**
**Installation Status Summary**



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

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

+=================+========+========+===============================+
|     Option      | Choice | Status |            Comment            |
+=================+========+========+===============================+
| software        |  yes   |   ok   | new install/upgrade x.xx.xx   |
+-----------------+--------+--------+-------------------------------+
| firmware        |  yes   |   ok   | copy i2002 version 1.xx       |
| firmware        |  yes   |   ok   | copy i2004 version 1.xx       |
| firmware        |  yes   |   ok   | copy PhaseII 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   |
+-----------------+--------+--------+-------------------------------+
| configuration   |  yes   |   ok   | set as Leader/Follower        |
+-----------------+--------+--------+-------------------------------+

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

**17** Press <CR> to exit to the Main Menu (see Figure 26 on page 74). Enter **q** at the Main Menu to quit the installation process. Figure 45 on page 88 appears. Enter **q** again.

**Figure 45**
**Quit**



```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================
You have selected to quit the Install Tool.

Before quitting and rebooting the system, remove all disks (floppy,
CDROM) from the drives.

        Please enter:
<CR> -> <m> - Return to previous menu.
        <q> - Quit and reboot the system.

        Enter Choice> q
```

**18** Remove the CD-ROM from the drive and reboot the system.

> ***Note:*** After software installation and reboot, a Follower Signaling Server sends out BOOTP requests and waits for a response. Since the Follower Signaling Server is not yet configured in an IP Telephony node, there is no BOOTP response. Do not wait for this response; use Procedure 7 on page 89 to add the Follower Signaling Server to a node immediately.

**End of Procedure**

Use Element Manager to add the Follower Signaling Server to the IP Telephony node. Refer to “Adding a Follower Signaling Server to a node”, below.

## Adding a Follower Signaling Server to a node

Use Procedure 7 on page 89 to add a Follower Signaling Server to an IP Telephony node.

> *Note:* The first time the Follower Signaling Server is installed, the FTP fails. The failure occurs because the Follower cannot obtain the system login and password, and does not have the current CONFIG.INI file with the Call Server IP address. In subsequent Follower installations, FTP succeeds.

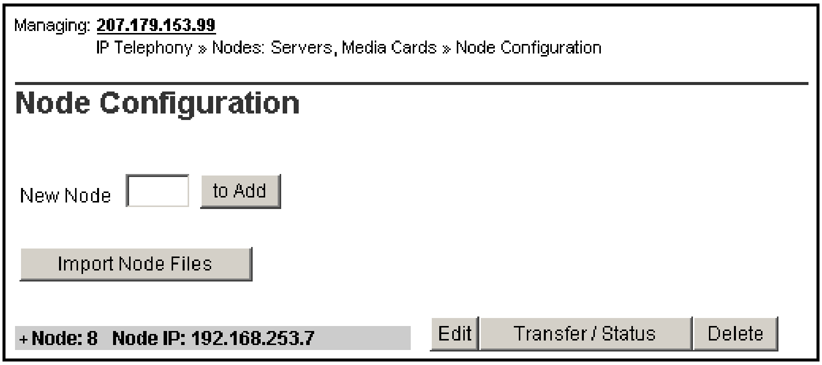
### Procedure 7
### Adding a Follower Signaling Server to an IP Telephony node

1 Log in to Element Manager, using Procedure 32 on page 170.

2 Select **IP Telephony > Nodes: Servers, Media Cards > Configuration** from the navigator.

The **Node Configuration** web page opens, as shown in Figure 46.

**Figure 46**
**Node Configuration web page**



Managing: 207.179.153.99
IP Telephony » Nodes: Servers, Media Cards » Node Configuration

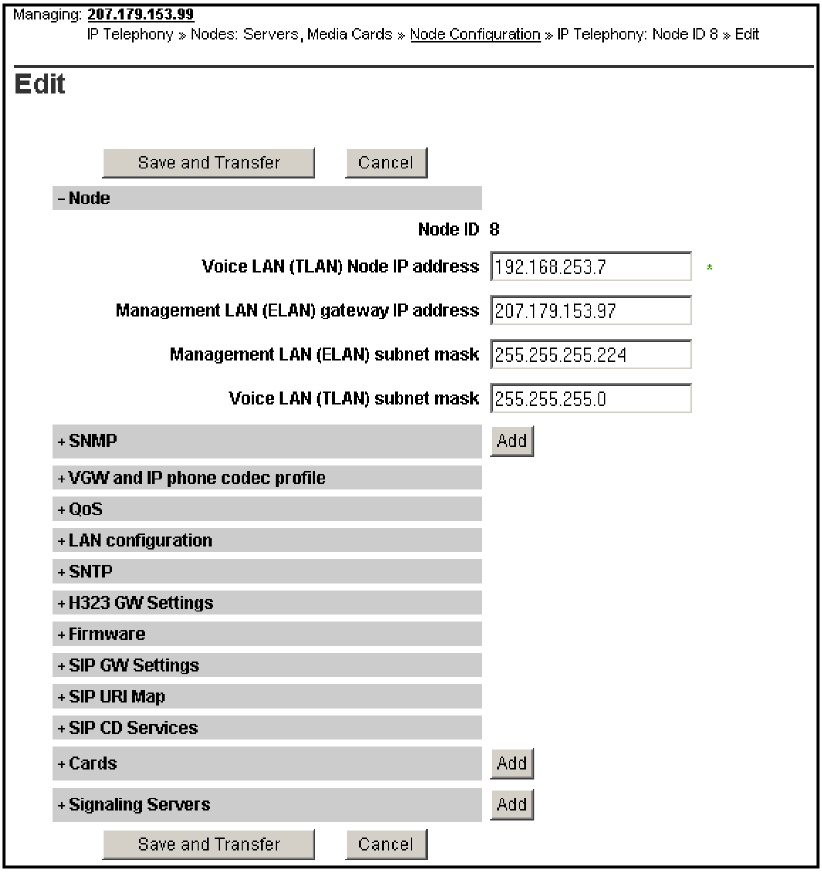
Node Configuration

+ Node: 8 Node IP: 192.168.253.7

3 Click **Edit** next to the node to which the Follower Signaling Server is to be added.

The **Edit** web page opens, as shown in Figure 47 on page 90.

**Figure 47**
**Edit web page**



Managing: **207.179.153.99**
IP Telephony » Nodes: Servers, Media Cards » Node Configuration » IP Telephony: Node ID 8 » Edit

Edit

- Node

Node ID: 8

Voice LAN (TLAN) Node IP address: 192.168.253.7 *

Management LAN (ELAN) gateway IP address: 207.179.153.97

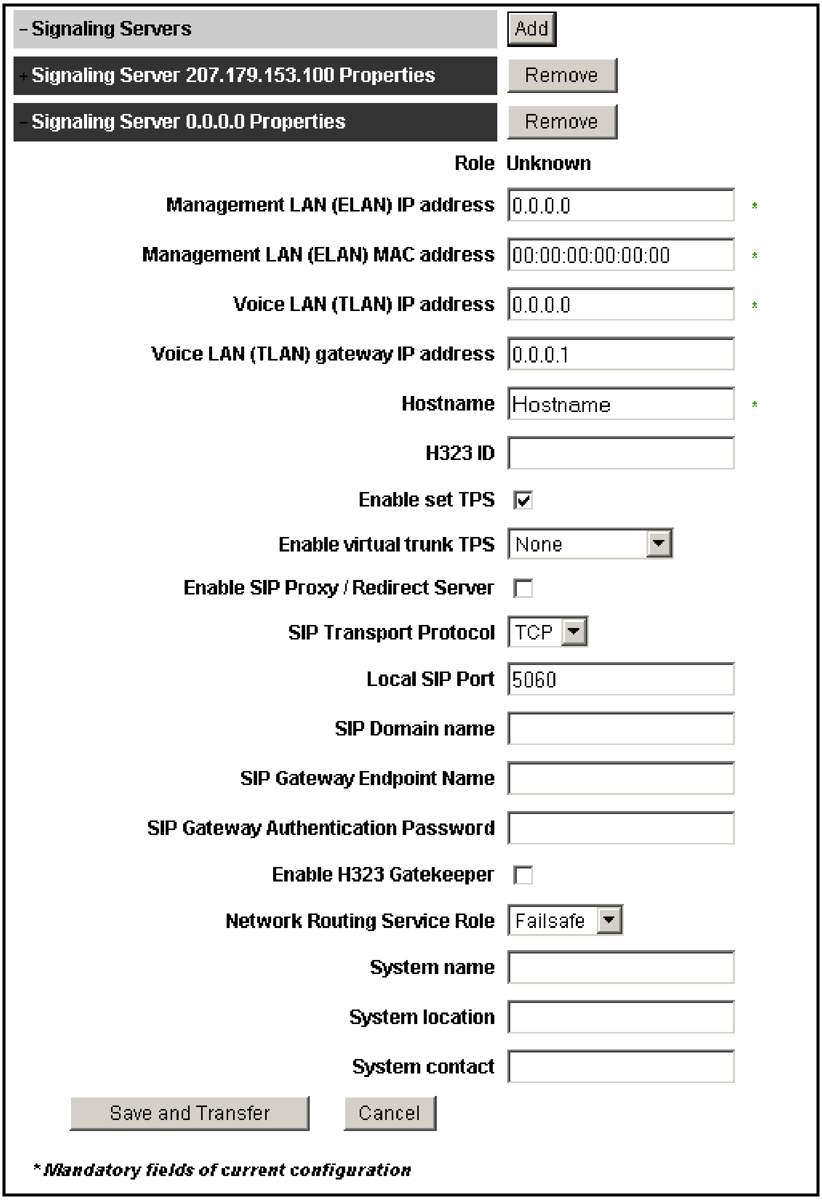
Management LAN (ELAN) subnet mask: 255.255.255.224

Voice LAN (TLAN) subnet mask: 255.255.255.0

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**, as shown in Figure 48 on page 91.

**Figure 48**
**Signaling Server xxx.xxx.xxx.xxx properties**



- Signaling Servers
Add
+ Signaling Server 207.179.153.100 Properties
Remove
- Signaling Server 0.0.0.0 Properties
Remove

| | |
|---|---|
| Role | Unknown |
| Management LAN (ELAN) IP address | 0.0.0.0 * |
| Management LAN (ELAN) MAC address | 00:00:00:00:00:00 * |
| Voice LAN (TLAN) IP address | 0.0.0.0 * |
| Voice LAN (TLAN) gateway IP address | 0.0.0.1 |
| Hostname | Hostname * |
| H323 ID | |
| Enable set TPS | ☑ |
| Enable virtual trunk TPS | None |
| Enable SIP Proxy / Redirect Server | □ |
| SIP Transport Protocol | TCP |
| Local SIP Port | 5060 |
| SIP Domain name | |
| SIP Gateway Endpoint Name | |
| SIP Gateway Authentication Password | |
| Enable H323 Gatekeeper | □ |
| Network Routing Service Role | Failsafe |
| System name | |
| System location | |
| System contact | |

** Mandatory fields of current configuration*

5 Enter the information corresponding to the Follower Signaling Server.

The **Role** field will automatically revert to **Follower** once the Follower Signaling Server has been added.

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

Refer to "Transferring IP Telephony files" on page 180, and *IP Line: Description, Installation, and Operation* (553-3001-365) for detailed instructions on transferring IP Telephony node information.

**End of Procedure**

# Unpacking 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, they can be unpacked at any time after the Signaling Server software is installed. Use Procedure 34 on page 175 to unpack the files.

**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* (553-3001-332) for more information on Element Manager and the Virtual Terminal Emulator.

# Logging in to the Signaling Server

Use Procedure 8 on page 93 to log in to the vxWorks$^{TM}$ shell to access the Signaling Server from a maintenance terminal.

**Procedure 8**
**Logging in to the Signaling Server**

Before you begin, make sure the DTE–DTE null modem cable (supplied with the Signaling Server) runs between the serial port on the back of the Signaling Server and the maintenance terminal.

**1** Make sure the Signaling Server is powered up and connected to the maintenance terminal. Refer to Procedure 3 on page 51.

The Signaling Server must boot successfully before the user can log in.

**2** Press <CR> to invoke the login prompt.

**3** Enter the login credentials by doing one of the following:.

- If the Signaling Server has connected to the Call Server (the startup messages indicate if the PBX link is up), use the PWD1 login to access the Signaling Server.
- If the Signaling Server is not connected to the Call Server:

  **a.** Enter the default Signaling Server Command Line Interface (CLI) login **`admin1`** or **`admin2`**.

  **b.** Enter the Signaling Server Command Line Interface (CLI) password.

  - If this Signaling Server has just been installed and you are logging in for the first time, enter the default password **`0000`**.
  - If this is not the first login to the Signaling Server, enter the appropriate password.

    If you have forgotten the password, reset it from the Tools Menu (see Procedure 36 on page 235).

**End of Procedure**

To log out of the Signaling Server, enter **`exit`** at the command line.

# Verifying a successful configuration

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

**Procedure 9**
**Verifying the Signaling Server Ethernet connection**

**1** Log in to the Signaling Server, using Procedure 8 on page 93.

**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 of Procedure**

# Testing the Leader Signaling Server

Configure two IP Phones to register to the Signaling Server on its temporary node. These IP Phones must be provisioned on the Call Server. Refer to *Communication Server 1000S: Installation and Configuration* (553-3031-210), *Communication Server 1000E: Installation and Configuration* (553-3041-210), *Communication Server 1000M and Meridian 1: Large System Installation and Configuration* (553-3021-210), or *Communication Server 1000M and Meridian 1: Small System Installation and Configuration* (553-3011-210) for the procedure appropriate to the system. After provisioning, the telephones can call each other.

# Software upgrade and reconfiguration

## Contents

This section contains information on the following topics:

## Introduction

This chapter explains how to use the Signaling Server Install Tool to upgrade the Signaling Server software and reconfigure the Signaling Server. It also explains how to reinstall the previous version of Signaling Server software.

# Upgrading from previous releases

## Upgrading from Succession Release 3.0

If you are upgrading from Succession Release 3.0, you must migrate your H.323 Gatekeeper to the NRS as part of the upgrade.

Use the process and procedures in "H.323 Gatekeeper database migration" on page 123 to perform both the migration and the Signaling Server upgrade.

**IMPORTANT!**

If you are upgrading from Succession Release 3.0, do not use the procedures in this section unless directed to do so by the process described in "H.323 Gatekeeper database migration" on page 123.

## Upgrading from CS 1000 Release 4.0

If you are upgrading from CS 1000 Release 4.0 and the Signaling Server hosts an NRS, you must back up the NRS database before you begin the software upgrade.

To verify if the Signaling Server hosts an NRS, use Procedure 10 on page 96.

**Procedure 10**
**Verifying the presence of an NRS**

**1** Logon to Element Manager on the Signaling Server.

- The "Home - System Overview" screen appears. This screen displays information about the connected Call Server, the connected WEB server, and the Signaling Server itself.

**2** Expand the Signaling Server component on the "Home - System Overview" screen.

- Click the "+" symbol in front of the Signaling Server component to see detailed information about this Signaling Server.

**3** View the contents of the “Gatekeeper configuration” item.

- If it contains the words “Primary”, “Alternate” or “Failsafe”, the Signaling Server hosts an NRS. If blank, the Signaling Server does not host an NRS.

**End of Procedure**

If the Signaling Server hosts an NRS, you must back up the NRS database using the backup tool in NRS Manager. Then you must download and save the backup file to your local PC. For instructions, see *IP Peer Networking: Installation and Configuration* (553-3001-213).

**IMPORTANT!**

You must back up the NRS database to your local PC for the database migration to be successful.

After you have upgraded and reconfigured the Signaling Server, you must restore the backed up NRS database from your local PC to the upgraded Signaling Server. Use NRS Manager to restore the database, then cutover and commit the database. For instructions, see *IP Peer Networking: Installation and Configuration* (553-3001-213).

# Upgrading the Signaling Server software

**IMPORTANT!**

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

## Before you begin

Before upgrading the software, you must do the following:

- Connect and power up the Signaling Server — use Procedure 3 on page 51.
- If the Signaling Server hosts an NRS, back up the NRS database to your local PC. See *IP Peer Networking: Installation and Configuration* (553-3001-213) for instructions

- Obtain the latest version of the Signaling Server Software Install CD-ROM — see “Signaling Server Software CD-ROM” on page 62.
- Obtain a DOS-formatted blank diskette.

## Performing the software upgrade

Use Procedure 11 to upgrade the Signaling Server software.

**Procedure 11**
**Upgrading the Signaling Server software**

The Signaling Server requires a minimum of 512 MB of RAM to run CS 1000 Release 4.5. If the Signaling Server must support more than 382 H.323 virtual trunks, a minimum of 768 MB of RAM is required. If necessary, use Procedure 41 on page 246 to upgrade the RAM before beginning this procedure.

If you are upgrading from CS 1000 Release 4.0, you must back up the NRS database. See *IP Peer Networking: Installation and Configuration* (553-3001-213) for instructions.

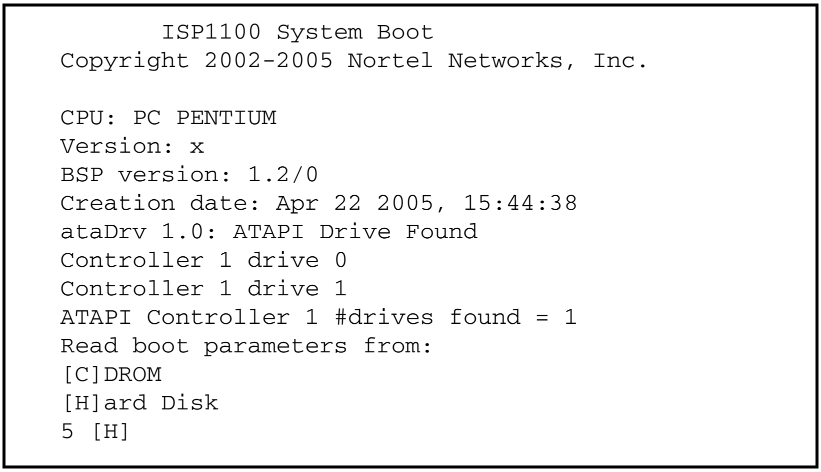
1 Insert the Software CD-ROM into the Signaling Server CD drive, and press the **RST** button on the front panel to cold-reboot the Signaling Server.

*Note:* The Software CD-ROM should be bootable. If not, create a boot floppy using the files in the `/mkboot` directory on the Signaling Server Software CD-ROM.

2 Enter **c** at the boot menu shown in Figure 49 on page 99.

*Note:* Enter **c** within ten seconds to ensure that the Signaling Server boots to the upgraded software on the CD-ROM.

**Figure 49**
**Upgrade boot sequence**



```
       ISP1100 System Boot
Copyright 2002-2005 Nortel Networks, Inc.

CPU: PC PENTIUM
Version: x
BSP version: 1.2/0
Creation date: Apr 22 2005, 15:44:38
ataDrv 1.0: ATAPI Drive Found
Controller 1 drive 0
Controller 1 drive 1
ATAPI Controller 1 #drives found = 1
Read boot parameters from:
[C]DROM
[H]ard Disk
5 [H]
```

The following message appears:

```
tRootTask: Error reading system configuration file
tRootTask: Can't open oml.cfg file

Loading /cd0/load/inst.out
```

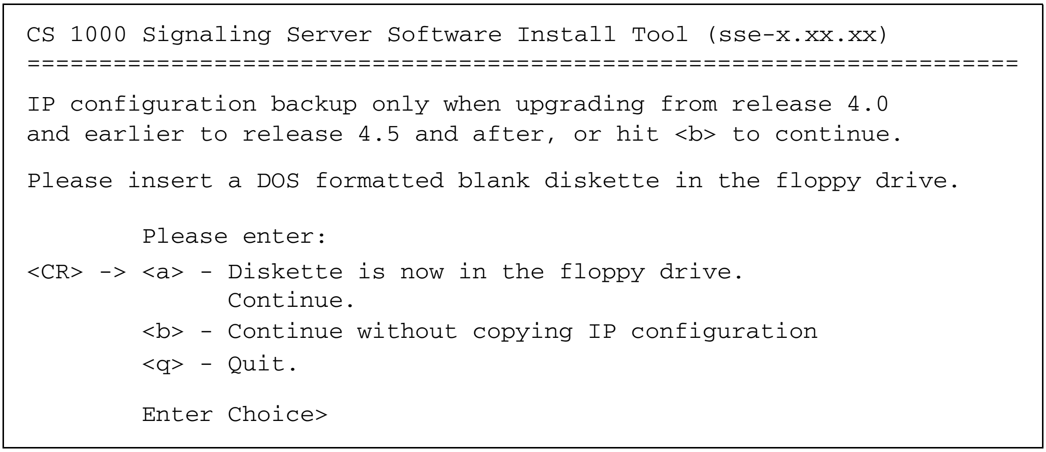
**3** When the Install Tool banner appears (Figure 19 on page 68), press <CR> to perform system checks and begin software installation.

The system verifies the file systems.

The following message appears:

```
WARNING: Make sure the NRS database is already
backed up. At this point, you should quit if you
don't have a NRS database backup. Option <a> will
only allow you to backup the IP configuration, and
the hard disk will be partitioned and all unsaved
data will be lost.
```

**Figure 50**
**Copy IP configuration**



```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================
IP configuration backup only when upgrading from release 4.0
and earlier to release 4.5 and after, or hit <b> to continue.

Please insert a DOS formatted blank diskette in the floppy drive.

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

        Enter Choice>
```

4 Do one of the following:

- If you want to back up the IP configuration, insert a blank floppy disk in the floppy drive (ensure that the floppy is not write-protected) and enter **a** at the menu shown in Figure 50 on page 100.

  Do one of the following:

  — If the following message displays, followed by the menu in Figure 50 on page 100 again, the backup operation failed. Go to step 5 on page 101:

  ```
  Change volume Id from 0x0 to 0x320d2
  Please Wait

  Failed to copy the IP configuration
  The floppy is write-protected.
  ```

  If the following message displays, followed by the menu in Figure 51 on page 102, the backup succeeded. Remove the floppy from the drive and change it to write-protected. Keep the floppy write-protected throughout the rest of the upgrade procedure to ensure the integrity of its data. Go to step 7 on page 102:

```
/p/ - Volume is OK

Please wait

/f0/ - Volume is OK
/u/ - Volume is OK

Change volume Id from 0x0 to 0x125b

Done backing up IP configuration to the floppy
```

- If you want to continue without backing up the IP configuration, enter **b** at the menu shown in Figure 50 on page 100.

  The system asks for confirmation:

  ```
  IP configuration will be lost. Are you sure you
  want to continue?
  ```

  Enter **b** at the menu shown in Figure 50 on page 100 to confirm that you want to continue. Go to step 6 on page 101.

- If you want to quit the upgrade and restore the previous release of software, remove the Install Tool CD and the floppy from the drives and enter **q** at the menu shown in Figure 50 on page 100. Go to step 14 on page 107.

**5** Reset the write permission on the floppy and try again:

**a.** Remove the floppy from the drive and slide the permission tab up and down.

**b.** Go back to step 4 on page 100.

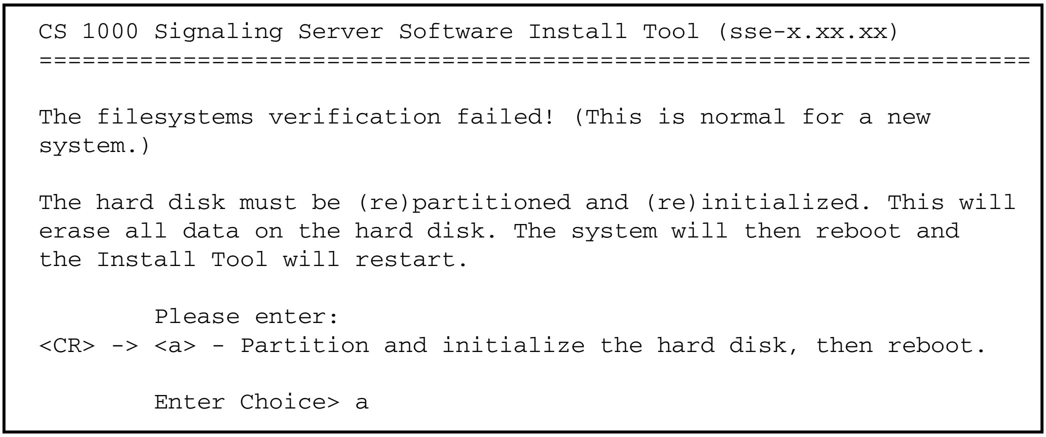
**6** When the Install Tool banner appears (Figure 19 on page 68), press <CR> to perform system checks and begin software installation.

The system verifies the file systems. The disk check reports:

```
Filesystems verification succeeded.
```

The menu shown in Figure 51 on page 102 appears.

**Figure 51**
**First boot of a new system**



```
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
```

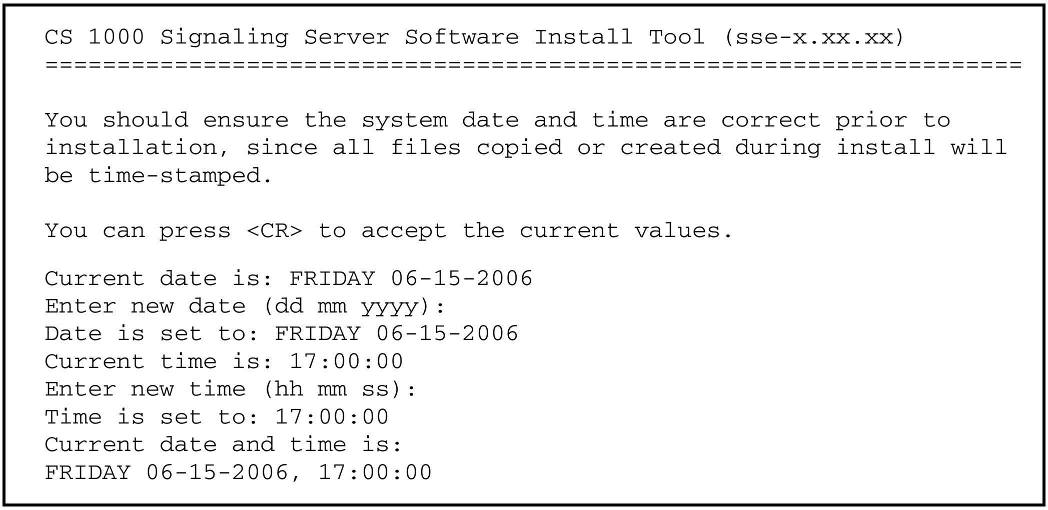
**7** Enter **a** at the menu shown in Figure 51 on page 102 to partition and initialize the hard disk.

The following messages appear:

```
Partitioning hard disk ...
Clearing partitions on hda
Hard disk partitioning succeeded.

Creating filesystems ...

/boot/ - Volume is OK
/p/ - Volume is OK
/u/ - Volume is OK
/e/ - Volume is OK

Filesystems creation succeeded.

Rebooting system ...
```

The system reboots and the Install Tool banner (Figure 19 on page 68) appears. Press <CR> to continue. The screen shown in Figure 52 on page 103 appears.

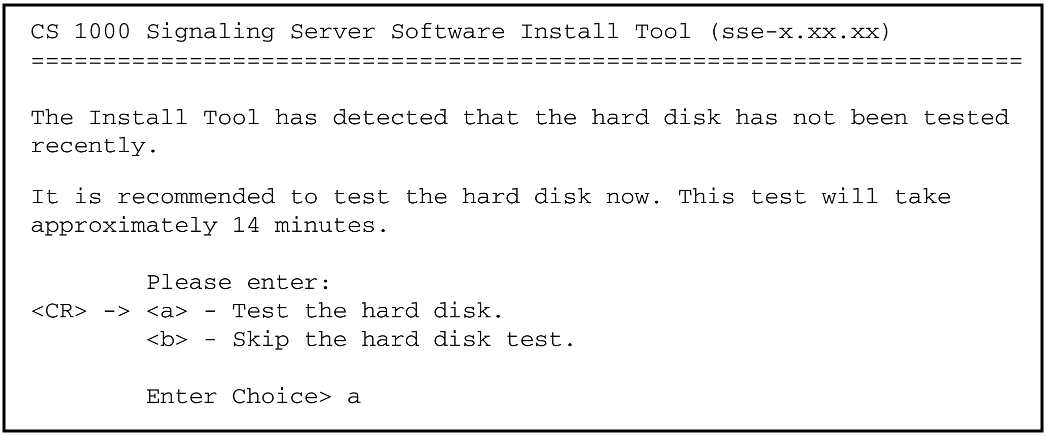
**Figure 52**
**Date and time**



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

You should ensure 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 06-15-2006
Enter new date (dd mm yyyy):
Date is set to: FRIDAY 06-15-2006
Current time is: 17:00:00
Enter new time (hh mm ss):
Time is set to: 17:00:00
Current date and time is:
FRIDAY 06-15-2006, 17:00:00
```

8 Confirm or enter the current date and time. Press <CR> to continue. The screen shown in Figure 53 on page 103 appears.

**Figure 53**
**Not recently tested**



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

The Install Tool has detected that the hard disk has not been tested
recently.

It is recommended to test the hard disk now. This test will take
approximately 14 minutes.

        Please enter:
<CR> -> <a> - Test the hard disk.
        <b> - Skip the hard disk test.

        Enter Choice> a
```

9 Determine whether or not you want to test the hard disk.

- If you have not checked the hard disk recently, enter option **a**.

The following messages are displayed:

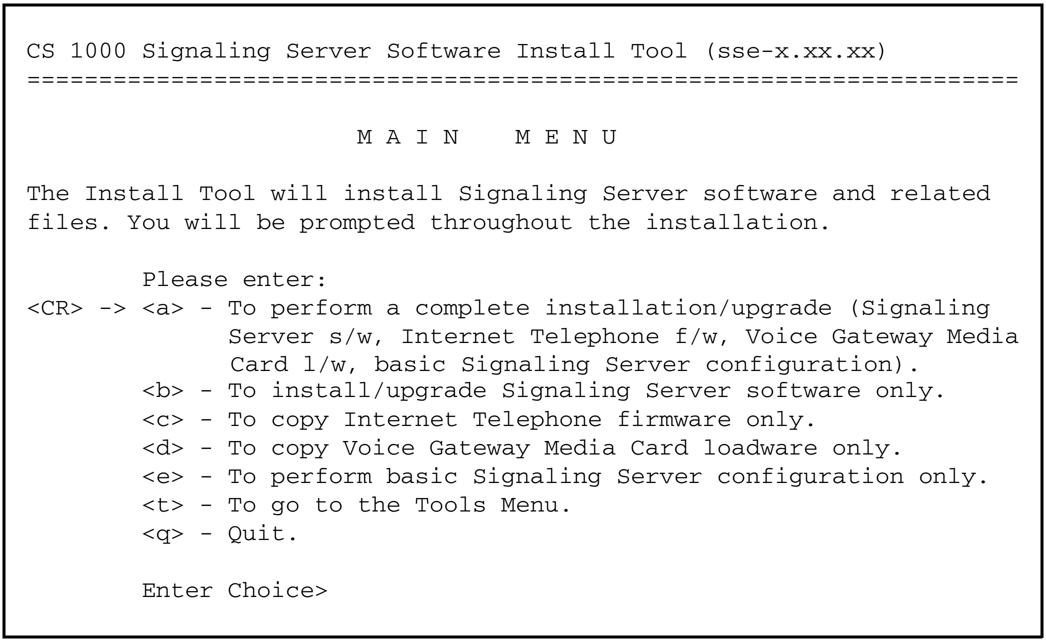
```
Testing hard disk ...
Testing partition /u (4194241 blocks) ...
xxx% complete

Testing partition /p (4194241 blocks) ...
xxx% complete

Hard disk testing succeeded.

Where xxx = 0 to 100.
```

If the physical check did not pass, contact your technical support group.

- If you have checked the hard disk recently, enter option **b**.

Regardless of which option is chosen, the next screen that appears is shown in Figure 54 on page 105.

**Figure 54**
**Install 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.
        <t> - To go to the Tools Menu.
        <q> - Quit.

        Enter Choice>
```

**10** Do one of the following:

- Enter **a** to upgrade the Signaling Server software, IP Phone firmware, and Voice Gateway Media Card loadware.
- Enter **b** to upgrade only the Signaling Server software.

The following sample lines appear:

```
Copying “/cd0/sse30047.p3/disk.sys” to “/u/disk.sys”.
Processing the install control file ...
“/cd0/sse30047.p3/install.dat” parsed.
```

**11** Enter **y** to start the upgrade.

A series of screens show the progress of the upgrade. The system then echoes the ELAN network interface MAC address.

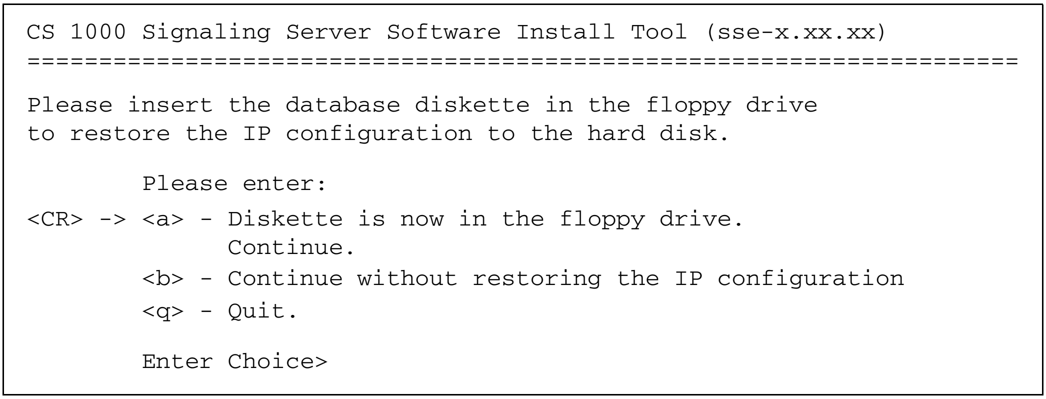
```
For future reference, the ELAN MAC address is:
"00:02:b3:c5:51:c6".
```

This address is found on the face of the Signaling Server, on the right-hand side when the bezel door is open. See Figure 15 on page 54.

When the upgrade is complete, one of the following occurs:

- If the IP configuration was not backed up prior to the upgrade, the Status Summary screen appears. Go to step 12.
- If the IP configuration was backed up prior to the upgrade, the menu shown in Figure 55 on page 106 is displayed. Go to step 13.

**Figure 55**
**Restore IP configuration**



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

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

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

        Enter Choice>
```

**12** Press <CR> to exit to the Main Menu, then go to step 14 on page 107.

**13** Do one of the following:

- To restore the IP configuration from the floppy, insert the write-protected floppy in the floppy drive, and enter **a** at the menu shown in Figure 55.
- To continue the upgrade without restoring the IP configuration, enter **b** or **q** at the menu shown in Figure 55. You will have to manually re-enter the IP configuration.

14 Enter **q** at the Main Menu to exit the upgrade process.

15 Enter **q** to exit the Install Tool.

16 Remove the CD-ROM from the drive and reboot the system.

**End of Procedure**

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. Use the steps in Procedure 12 to reconfigure the Signaling Server.

If you are upgrading from CS 1000 Release 4.0, and you did not back up your original IP configuration, either when upgrading the software (see Procedure 11 on page 98) or directly from the Tools menu (see Procedure 36 on page 235), you must manually reconfigure the Signaling Server. Use the steps in Procedure 12 to reconfigure the Signaling Server.

## Unpacking 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, they can be unpacked at any time after the Signaling Server software is installed. Use Procedure 34 on page 175 to unpack the files.

**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* (553-3001-332) for more information on Element Manager and the Virtual Terminal Emulator.

# Reconfiguring the Signaling Server

Use the Signaling Server Install Tool to reconfigure the Signaling Server.

**Procedure 12**
**Reconfiguring the Signaling Server**

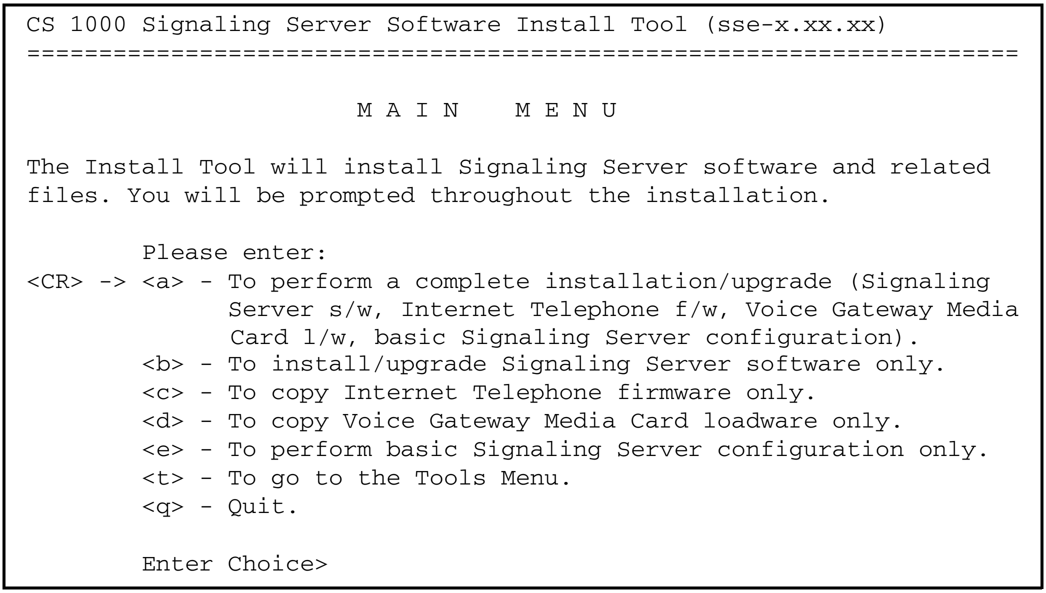
**1** From your Planning and Engineering group, obtain the following network and IP Telephony data for this Signaling Server:

- node ID for the IP Telephony node
- node IP address for the IP Telephony node
- hostname 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 Configuration* (553-3001-213) for details on the Gatekeeper)
- primary and alternate Gatekeeper IP addresses for this networked system (refer to *IP Peer Networking: Installation and Configuration* (553-3001-213))
- NRS role (refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for details on NRS

**2** At the Main Menu (Figure 56), enter **e** to reconfigure the Signaling Server.

- If the nrsconf.xml file does not exist (and the nrsdflt.xml file does exist), the menu shown in Figure 57 on page 110 is displayed. Go to step 3 on page 109.
- If the nrsconf.xml file does exist, go to step 5 on page 111.

**Figure 56**
**Install Tool Main Menu**



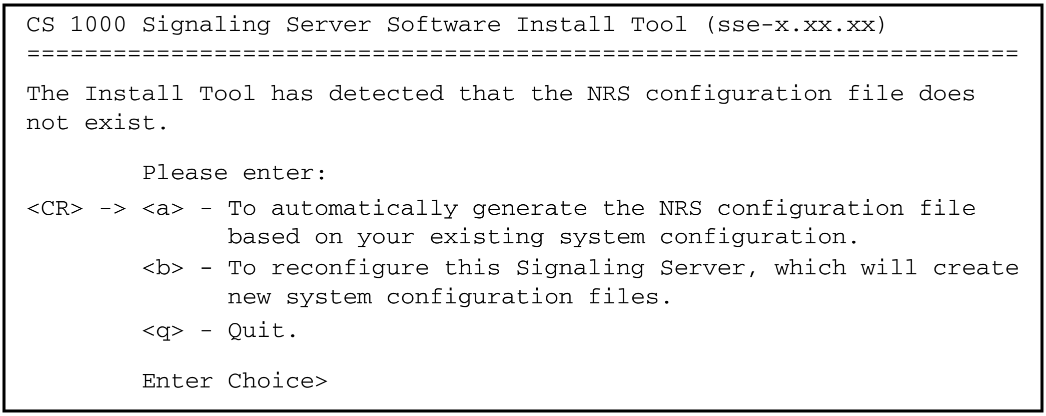
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

                       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.
        <t> - To go to the Tools Menu.
        <q> - Quit.

        Enter Choice>
```

**3** Create the NRS configuration file (nrsconf.xml) using the menu shown in Figure 57 on page 110.

- Select **a** to have the system automatically generate the NRS configuration file (nrsconf.xml) based on the existing configuration of the Signaling Server.

- Select **b** to create the new configuration file by reconfiguring the Signaling Server. Go to step 5 on page 111.

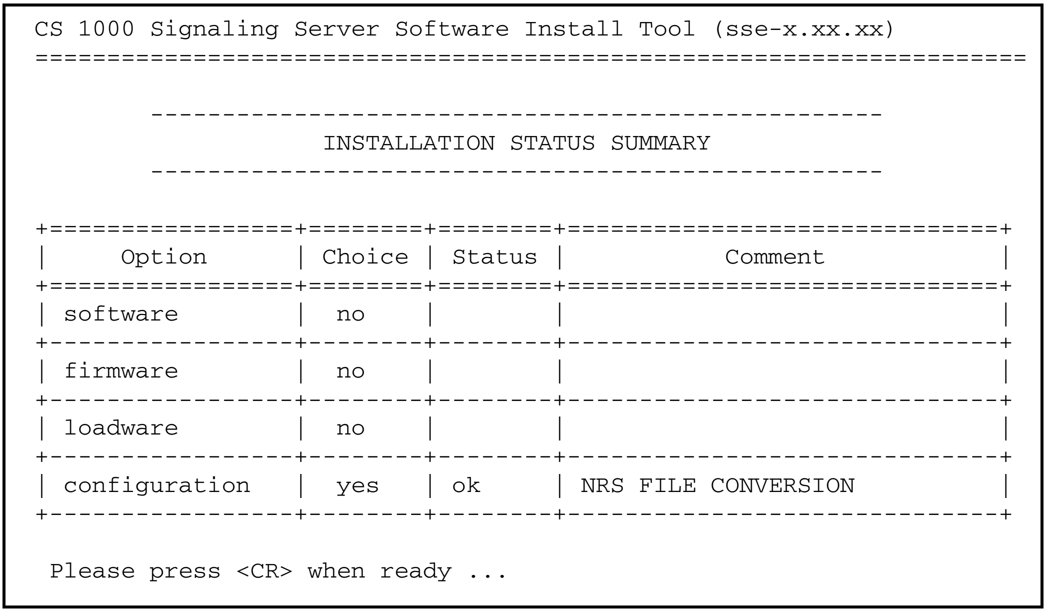
**Figure 57**
**NRS configuration file**



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

The Install Tool has detected that the NRS configuration file does
not exist.

        Please enter:

<CR> -> <a> - To automatically generate the NRS configuration file
              based on your existing system configuration.
        <b> - To reconfigure this Signaling Server, which will create
              new system configuration files.
        <q> - Quit.

        Enter Choice>
```

4 Press <CR> at the Installation Status screen (Figure 58) to return to the Main Menu, and then go to step 13 on page 120.

**Figure 58**
**Installation Status**

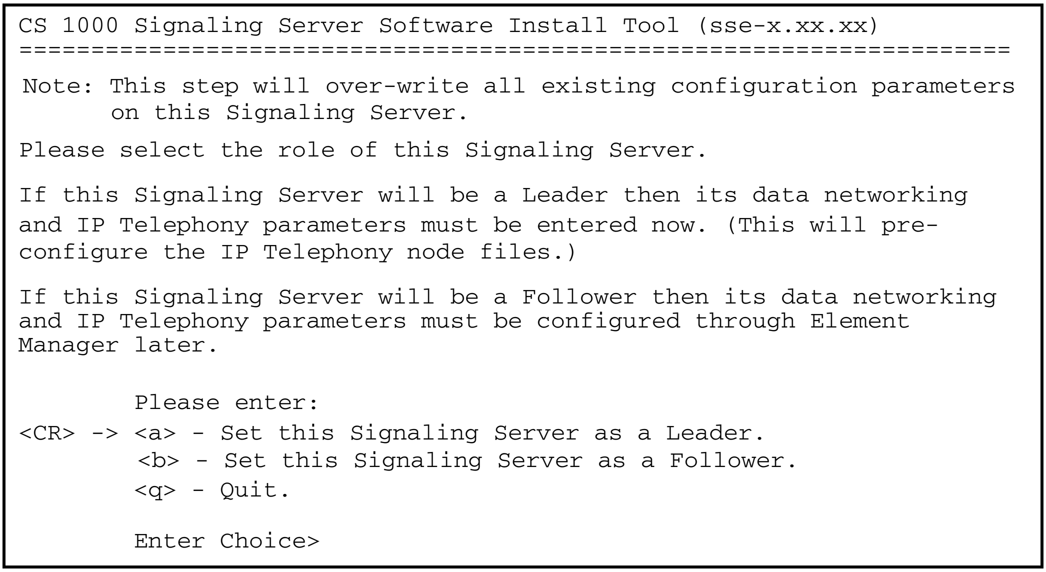


```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
====================================================================


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


+==================+========+========+===============================+
|     Option       | Choice | Status |           Comment             |
+==================+========+========+===============================+
| software         |  no    |        |                               |
+------------------+--------+--------+-------------------------------+
| firmware         |  no    |        |                               |
+------------------+--------+--------+-------------------------------+
| loadware         |  no    |        |                               |
+------------------+--------+--------+-------------------------------+
| configuration    |  yes   | ok     | NRS FILE CONVERSION           |
+------------------+--------+--------+-------------------------------+

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

**5** Configure the Signaling Server as Leader or Follower. See Figure 59.

- Enter **a** at the prompt to set this Signaling Server as Leader.
- Enter **b** at the prompt to set this Signaling Server as Follower. Go to step 9 on page 115.

**Figure 59**
**Leader/Follower Signaling Server configuration**

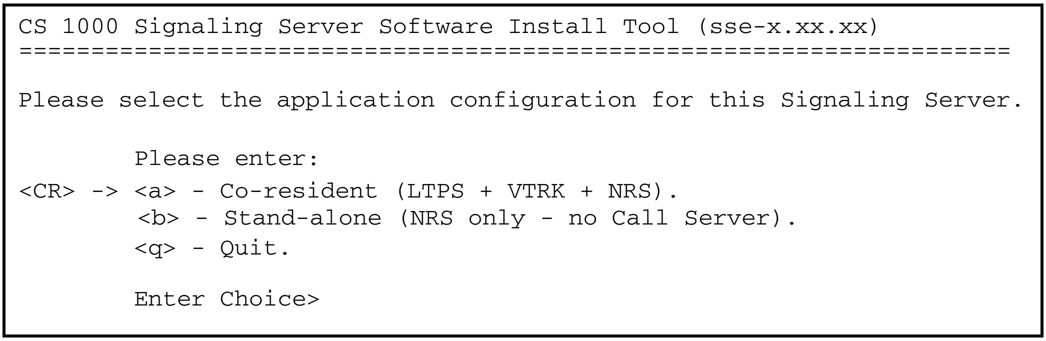


```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================
Note: This step will over-write all existing configuration parameters
      on this Signaling Server.
Please select the role of this Signaling Server.

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>
```

**6** Configure the application configuration for this Signaling Server. See Figure 60.

- If the Set TPS, Virtual Trunk TPS, and optional Network Routing Service (NRS) applications are to be enabled on this Signaling Server, enter **a** at the prompt to configure this Signaling Server as a co-resident 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 co-resident Signaling Server. After you finished installing the Signaling Server software, you can disable the Line TPS and Virtual Trunk TPS in Element Manager (refer to *Element Manager: System Administration* (553-3001-332)).
  - — If this Signaling Server is not to be associated with a Call Server, enter **b** at the prompt to set this Signaling Server as a stand-alone Signaling Server.

**Figure 60**
**Application configuration**



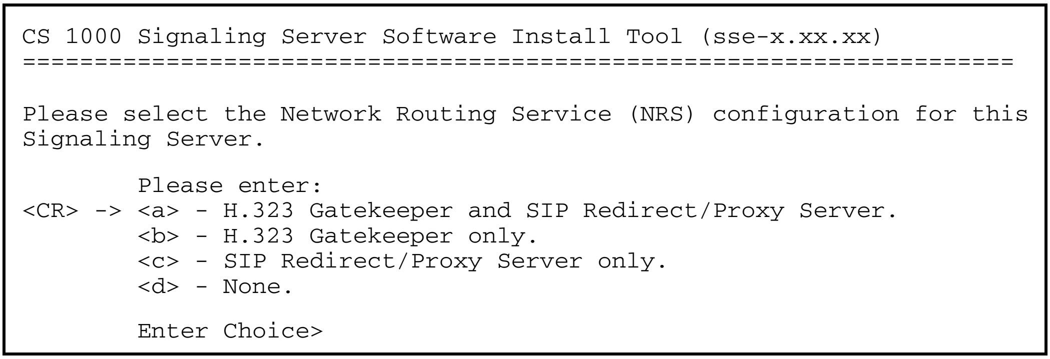
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

Please select the application configuration for this Signaling Server.

        Please enter:
<CR> -> <a> - Co-resident (LTPS + VTRK + NRS).
        <b> - Stand-alone (NRS only - no Call Server).
        <q> - Quit.

        Enter Choice>
```

7 Select the NRS to be provided by this Signaling Server. See Figure 61 for a co-resident Signaling Server or Figure 62 on page 114 for a stand-alone Signaling Server.

- Enter **a** if this Signaling Server will provide an H.323 Gatekeeper and a SIP Redirect/Proxy Server.
- Enter **b** if this Signaling Server will provide only an H.323 Gatekeeper.
- Enter **c** if this Signaling Server will provide only a SIP Redirect/Proxy Server.
- Enter **d** if this Signaling Server is a Leader Signaling Server and will not provide an NRS. Go to step 9 on page 115.

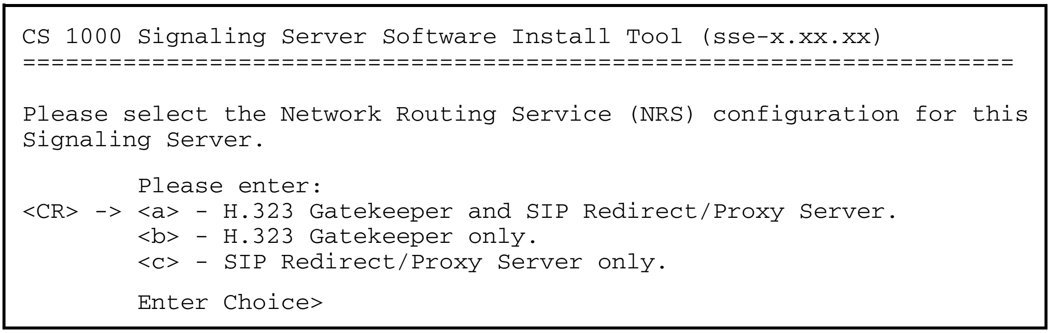
Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for more information on the NRS.

**Figure 61**
**Network Routing Service (NRS) — co-resident 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>
```

**Figure 62**
**Network Routing Service (NRS) — stand-alone Signaling Server**



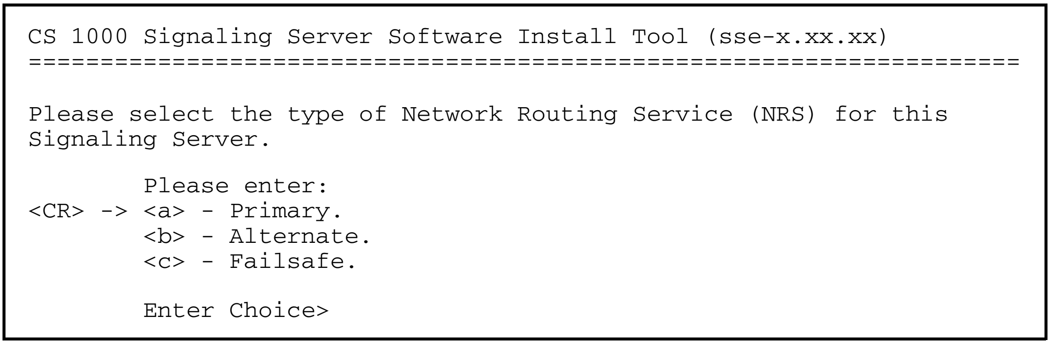
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

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>
```

**8** Select the type of NRS to be provided by this Signaling Server. See Figure 63 for a co-resident Signaling Server. See Figure 64 on page 115 for a stand-alone Signaling Server.

- 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 stand-alone Signaling Server and is to be the Failsafe NRS, enter **c**.

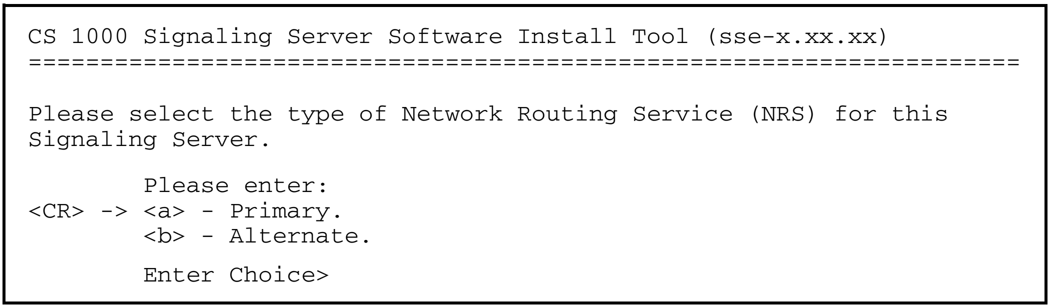
Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for more information on the NRS.

**Figure 63**
**NRS type — co-resident 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 64**
**NRS type — stand-alone 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>
```

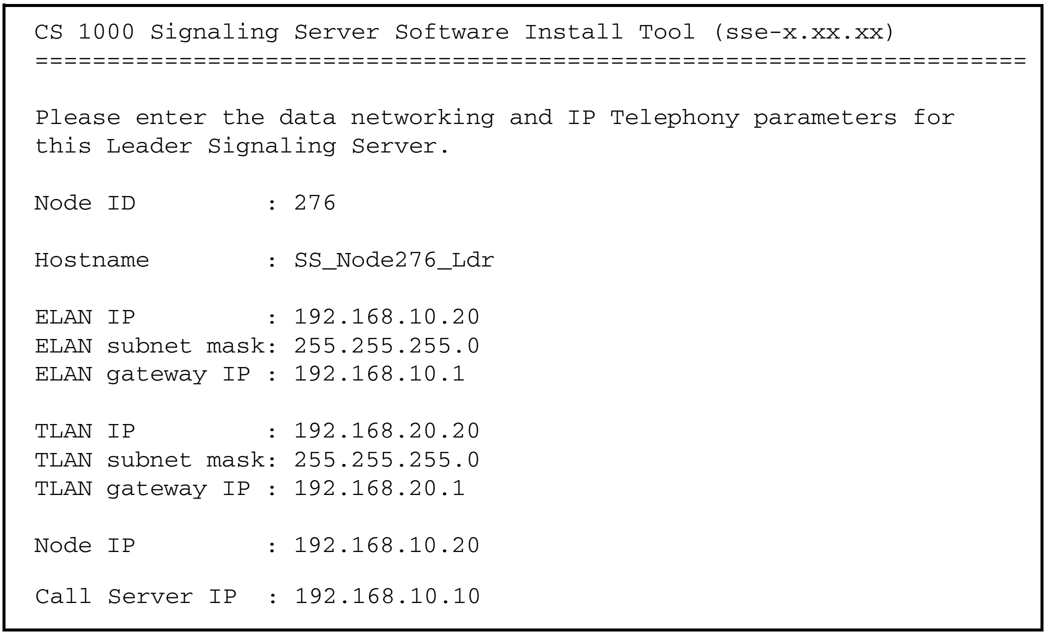
**9** Enter the data networking and IP telephony parameters for the Signaling Server as prompted.

- If this is a Leader Signaling Server, enter the parameters for the Node, ELAN network interface, TLAN network interface, and Call Server as required. See Figure 65 on page 116. 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.
- If this is a Follower Signaling Server, enter the Hostname of the Leader Signaling Server. See Figure 66 on page 116. Then go to step 11 on page 118.
- If this is a stand-alone Signaling Server and not associated with a Call Server (that is, **b** was selected in step 6 on page 112), enter the TLAN network interface parameters as required. The Call Server IP address is automatically set to 0.0.0.0. See Figure 67 on page 117. Then go to step 10 on page 117.

The IP information applies to a temporary IP Telephony node. This ensures that the existing node is not impacted. This also preconfigures the IP Telephony node files. In “Importing IP Telephony node files” on page 179, the node files are imported to Element Manager for further configuration.

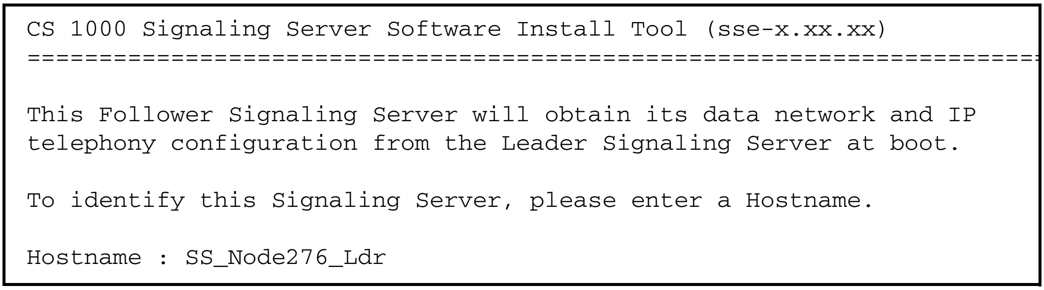
***Note:*** IP addresses shown in Figures 65 to 67 starting on page 116 are examples.

**Figure 65**
**Leader Signaling Server**



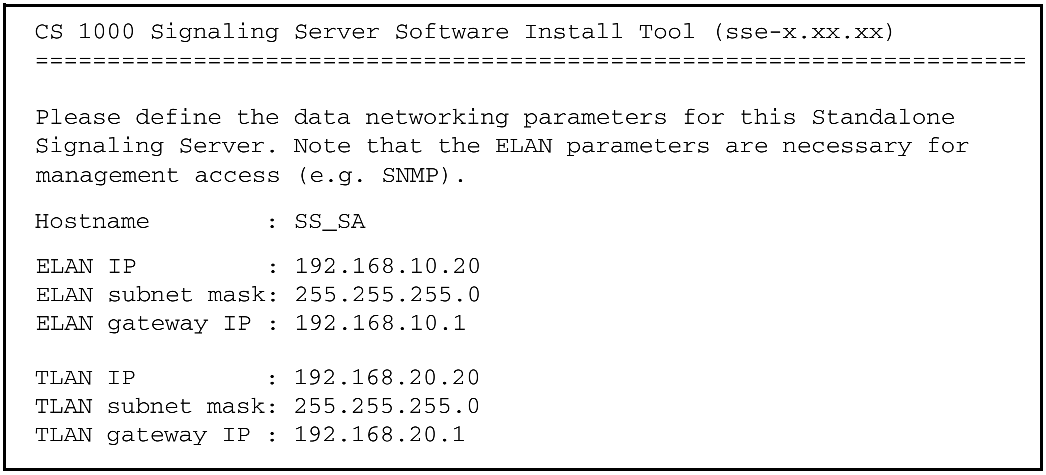
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

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 66**
**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
```

**Figure 67**
**Stand-alone Signaling Server**



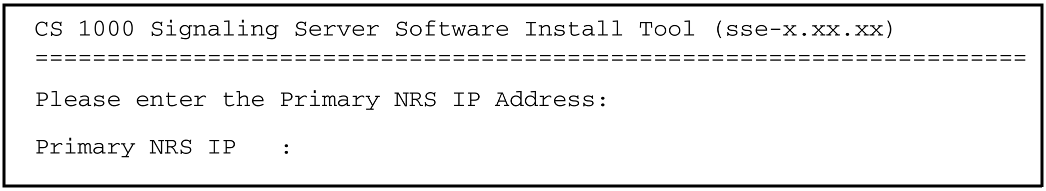
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

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
```

**10** Enter the Primary NRS IP address or the Alternate NRS IP address depending on the option entered in step 7 on page 113 or step 8 on page 114.

- If **a** was entered in step 8, you can enter the address of the Alternate NRS if you know it, but it is not required. See Figure 69 on page 118.
- If **b** was entered in step 8, enter the address of the Primary NRS. See Figure 68 on page 118.
- If **c** was entered in step 8:
    - — Enter the address of the Primary NRS. See Figure 68 on page 118.
    - — Enter the address of the Alternate NRS. See Figure 69 on page 118.
- If **d** was entered in step 7:
    - — Enter the address of the Primary NRS (optional). See Figure 68 on page 118.
    - — If you did enter the address of the Primary NRS, enter the address of the Alternate NRS (also optional). See Figure 69 on page 118.

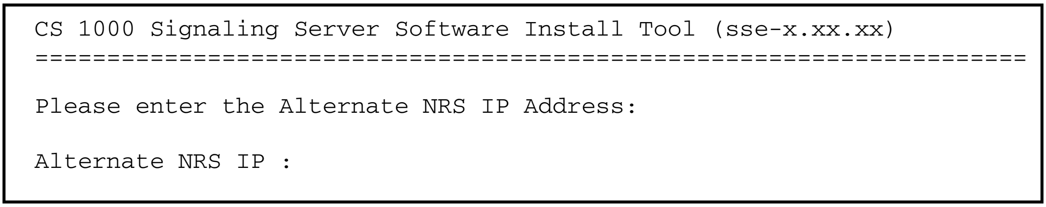
The Gatekeeper configuration can be updated later using Element Manager.

**Figure 68**
**Primary NRS IP address**



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

Please enter the Primary NRS IP Address:

Primary NRS IP   :
```

**Figure 69**
**Alternate NRS IP address**



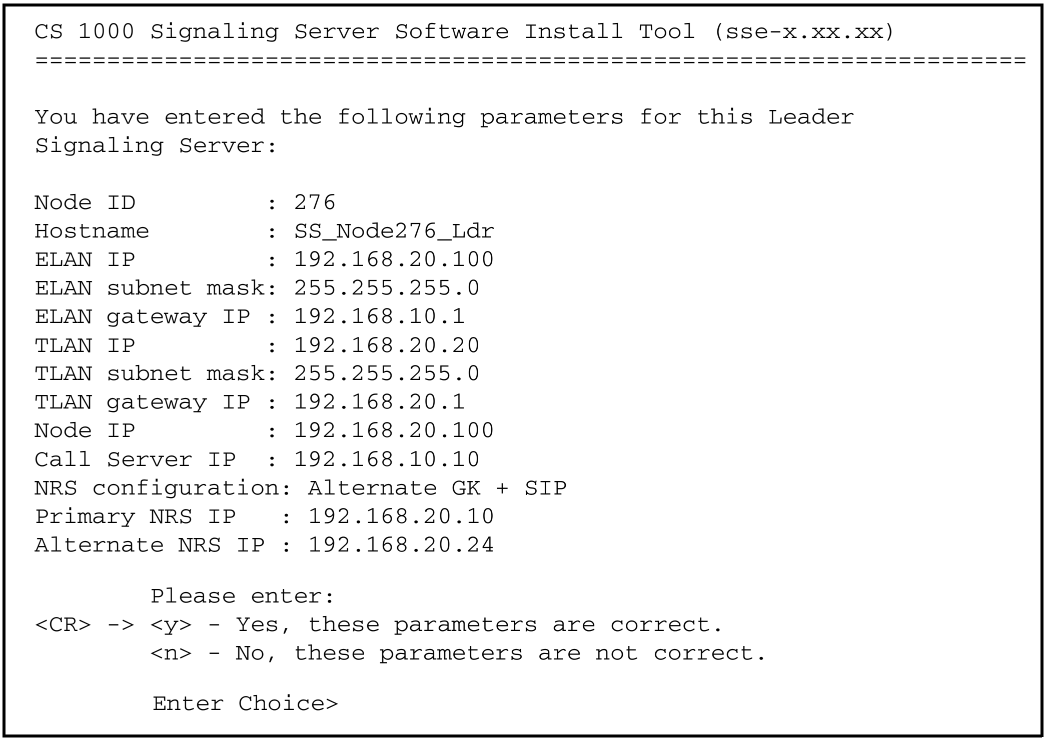
```
CS 1000 Signaling Server Software Install Tool (sse-x.xx.xx)
=====================================================================

Please enter the Alternate NRS IP Address:

Alternate NRS IP :
```

**11** Enter **y** to confirm the parameters. See Figure 70 on page 119.

The example in Figure 70 is for a Leader Signaling Server configured with an Alternate H.323 and SIP NRS. The confirmation screens for a Follower and stand-alone Signaling Server are similar, showing the same list of parameters, specifically:

- The screen for the Follower Signaling Server displays only the value for the Hostname parameter; all other values are blank.
- The screen for the stand-alone Signaling Server displays values for the Hostname, ELAN network interface, TLAN network interface, and NRS parameters. The Node ID field is set to 0. The Call Server IP field is set to 0.0.0.0.

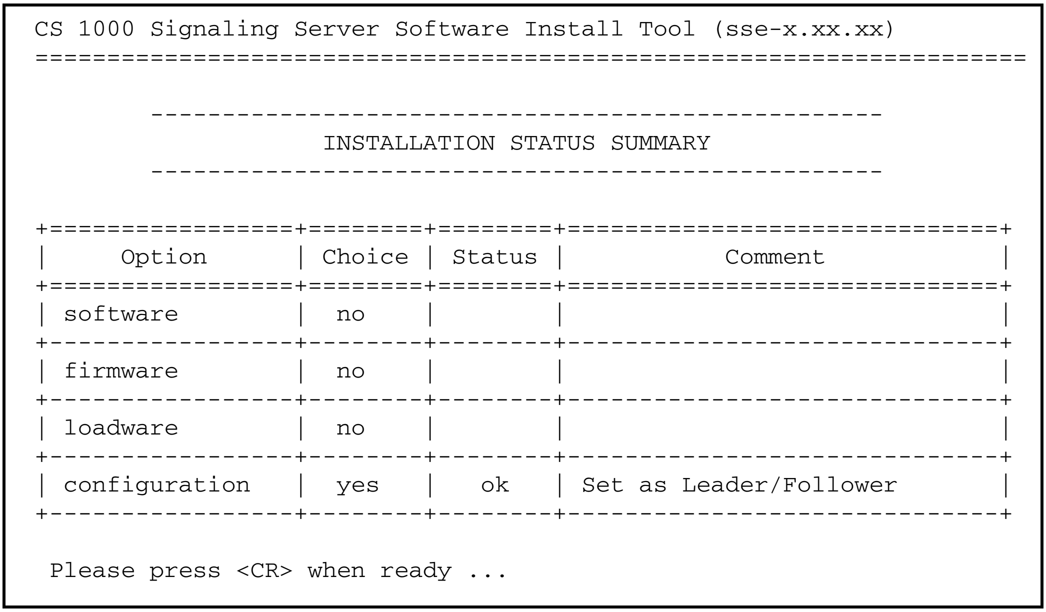
**Figure 70**
**IP Telephony parameter configuration**



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

You have entered the following parameters for this Leader
Signaling Server:

Node ID          : 276
Hostname         : SS_Node276_Ldr
ELAN IP          : 192.168.20.100
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          : 192.168.20.100
Call Server IP   : 192.168.10.10
NRS configuration: Alternate GK + SIP
Primary NRS IP    : 192.168.20.10
Alternate NRS IP : 192.168.20.24

        Please enter:
<CR> -> <y> - Yes, these parameters are correct.
        <n> - No, these parameters are not correct.

        Enter Choice>
```

12 Press <CR> at the Installation Status screen (Figure 71 on page 120) to return to the Main Menu.

**Figure 71**
**Installation Status**



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

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

+=================+========+========+==============================+
|     Option      | Choice | Status |           Comment            |
+=================+========+========+==============================+
| software        |  no    |        |                              |
+-----------------+--------+--------+------------------------------+
| firmware        |  no    |        |                              |
+-----------------+--------+--------+------------------------------+
| loadware        |  no    |        |                              |
+-----------------+--------+--------+------------------------------+
| configuration   |  yes   |   ok   | Set as Leader/Follower       |
+-----------------+--------+--------+------------------------------+

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

13 Enter **q** at the Main Menu to quit the installation process.

14 Remove all disks from the disk drives.

15 Enter **q** to Quit the Install Tool and reboot the system.

**End of Procedure**

# Reinstalling the previous release of software

Use Procedure 13 on page 121 to reinstall the previous release of software.

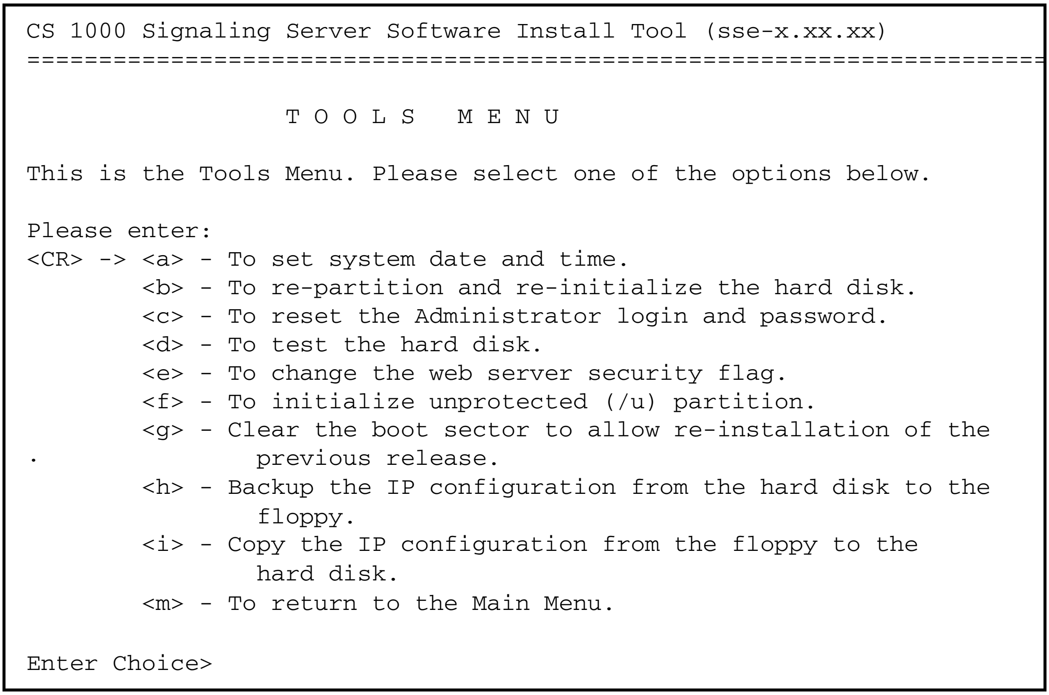
> ***Note:*** , You must first clear the boot sector. A utility in the Tools Menu is provided to do this (see “Signaling Server tools menu” on page 234).

### Procedure 13
### Reinstalling the previous software release

1 Enter **t** at the Install Tool **Main Menu** (see Figure 26 on page 74).

The **Tools Menu** opens, as shown in Figure 72.

**Figure 72**
**Tools menu**



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


                  T O O L S   M E N U

This is the Tools Menu. Please select one of the options below.

Please enter:
<CR> -> <a> - To set system date and time.
        <b> - To re-partition and re-initialize the hard disk.
        <c> - To reset the Administrator login and password.
        <d> - To test the hard disk.
        <e> - To change the web server security flag.
        <f> - To initialize unprotected (/u) partition.
        <g> - Clear the boot sector to allow re-installation of the
.                 previous release.
        <h> - Backup the IP configuration from the hard disk to the
                  floppy.
        <i> - Copy the IP configuration from the floppy to the
                  hard disk.
        <m> - To return to the Main Menu.

Enter Choice>
```

2 Enter **g** to **Clear the boot sector to allow the re-installation of the previous release.**

When the boot sector is cleared, the following message displays:

```
The boot sector is cleared.
Insert the installation CD and restart the system.
```

**3** Insert the Signaling Server Install Tool CD for the previous release, and install the software accordingly.

**End of Procedure**

# H.323 Gatekeeper database migration

## Contents

This chapter contains information on the following topics:

## Introduction

This chapter describes the procedures required to migrate an H.323 Gatekeeper database to a CS 1000 Release 4.5 NRS database.

It also describes the procedures required to migrate the database from one Signaling Server to another.

For detailed information on NRS configuration and management, see *IP Peer Networking: Installation and Configuration* (553-3001-213).

> ***Note:*** You can contact Nortel Global Professional Services to assist you with the migration and upgrade procedures.

## Networking Routing Service (NRS)

CS 1000 Release 4.0 and later supports both H.323 and the Session Initiation Protocol (SIP) on the same Signaling Server platform. NRS enables customers to manage a single network dialing plan for SIP, H.323, and mixed H.323/SIP networks.

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

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

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

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

# Browser configuration

You must properly configure your web browser before using NRS Manager. Refer to “Configuring the Internet Explorer browser” on page 166 for instructions on how to configure your web browser.

# Enabling and configuring the NRS server

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

You can configure the NRS server in two modes:

- Stand-alone mode — The host Signaling Server is not attached to a Call Server. During installation of the Signaling Server, ensure that the Call Server IP address is set to 0.0.0.0.

  ***Note:*** During installation of the Signaling Server in stand-alone mode (using the Signaling Server Software Install Tool), the administrator is not prompted to enter the Call Server IP address. Instead, the Call Server IP address defaults to 0.0.0.0. During the installation, the parameter confirmation screen displays the IP address as 0.0.0.0.

- Co-resident mode — The NRS is co-resident on the Signaling Server that is attached to a Call Server. The Signaling Server can run other applications. The applications include the IP Line TPS and the Virtual Trunk applications.

## Stand-alone mode

**Procedure 14**
**Enabling and configuring the NRS server in stand-alone mode**

**1** Enable the NRS using the Signaling Server Software Install Tool.

The following is a summary of the tasks required for the installation of a stand-alone Signaling Server; however, follow the detailed procedures given in “Software installation and configuration” on page 65 or “Software upgrade and reconfiguration” on page 95 for complete instructions.

- Perform the introductory steps for the Signaling Server installation.
- Set the Signaling Server as a Leader, when prompted.

- Set stand-alone mode (NCS only, no Call Server) for the Signaling Server.
- Select whether the NRS supports the SIP Redirect Server, the H.323 Gatekeeper, or both.
- Select the type of NRS (Primary or Alternate).
- Enter the hostname, the ELAN network interface parameters, and the TLAN network interface parameters. These parameters include the IP address, subnet mask, and gateway IP address.
- The Call Server IP address defaults to 0.0.0.0. for a stand-alone Signaling Server.
- Enter the IP address of the NRS (Primary or Alternate NRS IP address).

**2** Reboot the Signaling Server, after proper configuration of the Signaling Server.

If the Signaling Server reboots successfully, the NRS is configured with the default settings.

**3** Log in to NRS Manager using the default user ID and password. See Procedure 20 on page 147.

**4** Configure the NRS Server Settings in NRS Manager. See *IP Peer Networking: Installation and Configuration* (553-3001-213).

**5** Log out of the NRS. See Procedure 26 on page 159.

**6** Reboot the Signaling Server.

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

**End of Procedure**

## Co-resident mode

**Procedure 15**
**Enabling and configuring the NRS server in co-resident mode**

> ***Note:*** If the Signaling Server is configured in co-resident mode, proceed directly to step 3 on page 127.

**1** Enable the NRS using the Signaling Server Software Install Tool.

The following is a summary of the tasks required for the installation of a co-resident Signaling Server; however, follow the detailed procedures given in “Software installation and configuration” on page 65 or “Software upgrade and reconfiguration” on page 95 for complete instructions.

- Perform the introductory steps for the Signaling Server installation.
- Set the Signaling Server as a Leader, when prompted.
- Select co-resident mode (LTPS + VTRK + NRS) for the Signaling Server.
- Select whether the NRS supports the SIP Redirect Server, the H.323 Gatekeeper, or both. (The option to configure no NRS is also available.)
- Select the type of NRS (Primary, Alternate or Failsafe).
- Enter the node ID, hostname, 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 of the Signaling Server.

**3** Log in to Element Manager.

**4** Select **Configuration > IP Telephony** from the navigation tree.

The **IP Telephony Configuration** web page opens.

**5** Click **Node Summary**.

The **Node Summary** web page opens.

6 Click **Edit** for the appropriate node.

The **Edit** web page opens.

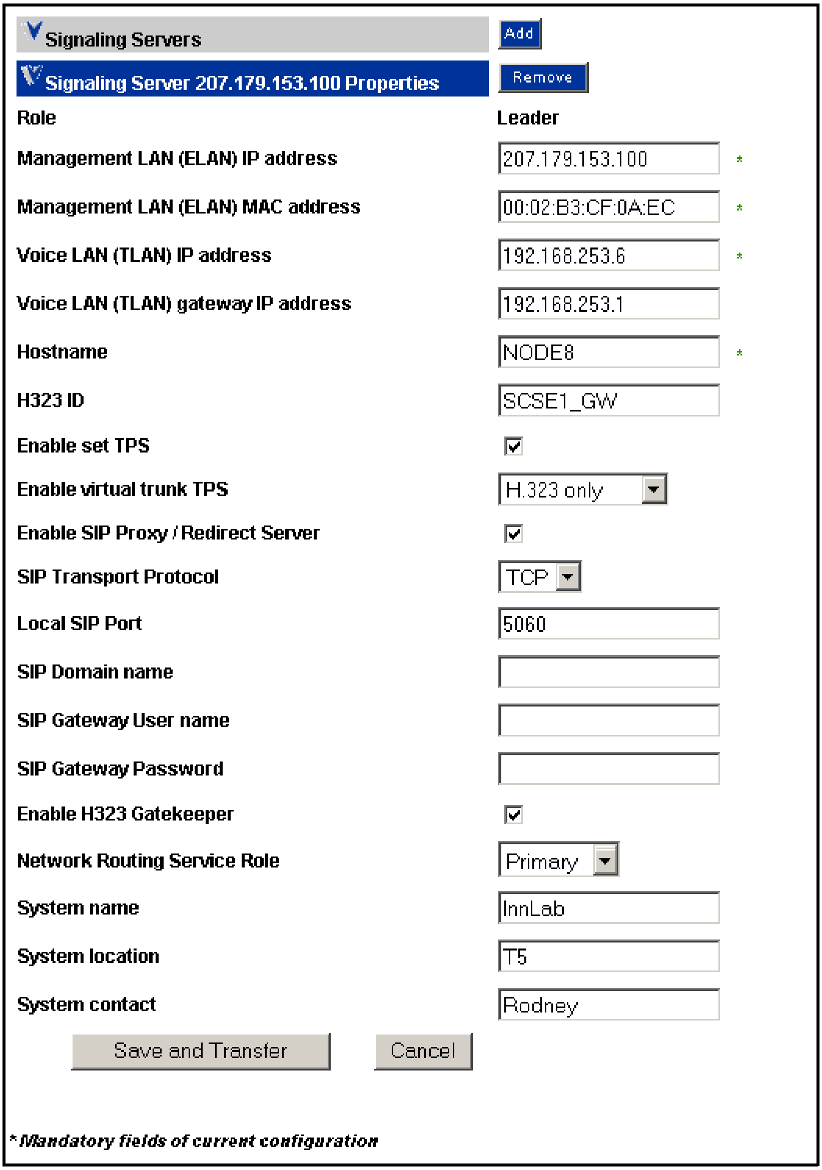
7 Select **Signaling Servers** to expand the section.

A list of Signaling Servers displays.

8 Select the appropriate **Signaling Server xxx.xxx.xxx.xxx Properties**.

The properties for that Signaling Server display (see Figure 73 on page 129).

**Figure 73**
**Signaling Server xxx.xxx.xxx.xxx properties**



| | | |
|---|---|---|
| Role | Leader | |
| Management LAN (ELAN) IP address | 207.179.153.100 | * |
| Management LAN (ELAN) MAC address | 00:02:B3:CF:0A:EC | * |
| Voice LAN (TLAN) IP address | 192.168.253.6 | * |
| Voice LAN (TLAN) gateway IP address | 192.168.253.1 | |
| Hostname | NODE8 | * |
| H323 ID | SCSE1_GW | |
| Enable set TPS | ☑ | |
| Enable virtual trunk TPS | H.323 only | |
| Enable SIP Proxy / Redirect Server | ☑ | |
| SIP Transport Protocol | TCP | |
| Local SIP Port | 5060 | |
| SIP Domain name | | |
| SIP Gateway User name | | |
| SIP Gateway Password | | |
| Enable H323 Gatekeeper | ☑ | |
| Network Routing Service Role | Primary | |
| System name | InnLab | |
| System location | T5 | |
| System contact | Rodney | |

** Mandatory fields of current configuration*

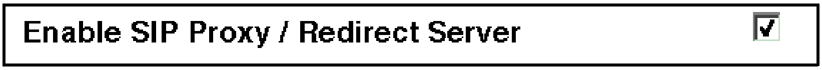
**9** To enable the NRS, do the following:

- Enable the SIP Proxy/Redirect Server and/or the H.323 Gatekeeper:
  - — To enable the SIP Proxy Server, SIP Redirect Server, or both, do step a.
  - — To enable the H.323 Gatekeeper, do step b.
  - — To enable the H.323 Gatekeeper, and the SIP Proxy Server, SIP Redirect Server, or both, do step a and step b.
- Set the role of the NRS (see step c on page 131).
- Ensure that the other required Signaling Server properties are also properly configured.

**a.** Select the **Enable SIP Proxy / Redirect Server** check box to enable the SIP Redirect Server (see Figure 74).

***Note:*** CS 1000 Release 4.5 does not support the SIP Proxy Server.

**Figure 74**
**Enabling the SIP Redirect Server**

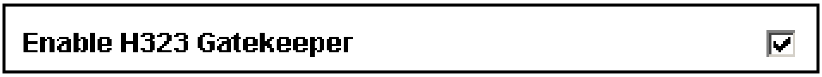


Enable SIP Proxy / Redirect Server ☑

***Note:*** You must also configure the SIP Gateway. See *IP Peer Networking: Installation and Configuration* (553-3001-213).

**b.** Select the **Enable H.323 Gatekeeper** check box to enable the H.323 Gatekeeper (see Figure 75).

**Figure 75**
**Enabling the H.323 Gatekeeper**



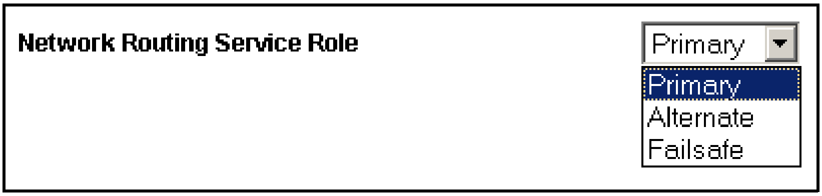
Enable H323 Gatekeeper ☑

***Note:*** You must also configure the H.323 Gateway. See *IP Peer Networking: Installation and Configuration* (553-3001-213).

**c.** Select the role of the NRS from the **Network Routing Service Role** drop-down list (see Figure 76 on page 131).

The three options are Primary, Alternate, and Failsafe.

**Figure 76**
**Network Routing Service Role**



Network Routing Service Role

Primary

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

**11** Click **Logout** at the bottom of the navigation tree to log out of Element Manager.

**12** Reboot the Signaling Server.

**13** After a successful reboot of the Signaling Server, log in to NRS Manager using the default user ID and password. See Procedure 20 on page 147.

**14** Configure the NRS Server Settings in NRS Manager. See *IP Peer Networking: Installation and Configuration* (553-3001-213).

**15** Log out of the NRS. See Procedure 26 on page 159.

**16** Reboot the Signaling Server.

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

**End of Procedure**

## Changing a Co-resident NRS server to a Stand-alone NRS server

Use the Signaling Server Software Install Tool to change a co-resident NRS server to a stand-alone NRS.

# Migration overview

To migrate your system, you must convert the H.323 Gatekeeper database into a CS 1000 Release 4.5 NRS database. This involves the following tasks:

- backing up the H.323 Gatekeeper database
- upgrading the Signaling Server software to CS 1000 Release 4.5
- reconfiguring the Signaling Server
- copying the backed up H.323 Gatekeeper database to the upgraded Signaling Server
- converting the H.323 Gatekeeper database to the CS 1000 Release 4.5 NRS database

## Redundancy

Redundancy in the network can be provided by three types of H.323 Gatekeepers:

- Primary H.323 Gatekeeper
- Alternate H.323 Gatekeeper
- Failsafe H.323 Gatekeeper

If these H.323 Gatekeepers exist in your network, you must upgrade each Gatekeeper database, because the NRS cannot use the existing H.323 Gatekeeper data directly.

Nortel Network recommends that you upgrade the Alternate H.323 Gatekeeper before you upgrade the Primary H.323 Gatekeeper.

**IMPORTANT!**

Nortel recommends that you migrate the databases to CS 1000 Release 4.5 as soon as possible after upgrading the software.

The Primary and Alternate H.323 Gatekeepers can coexist with mixed software releases; however, when a mixture exists, the Alternate and Primary databases cannot synchronize their data. This would require manual provisioning of the database. For example, if the Primary H.323 Gatekeeper runs CS 1000 Release 4.0 software while the Alternate H.323 Gatekeeper runs CS 1000 Release 4.5 software, no database synchronization occurs between the databases.

If a Failsafe H.323 Gatekeeper exists in the network, you must also upgrade it to CS 1000 Release 4.5. Nortel allows a 45-day period where the Failsafe can coexist with Primary and Alternate Gatekeepers that have been upgraded to Release 4.5.

**WARNING**

Failing to upgrade the Failsafe H.323 Gatekeeper within 45 days jeopardizes your network's system redundancy.

The new NRS database will respond to Keepalive messages from the Failsafe H.323 Gatekeeper to facilitate a smooth upgrade path. This allows you to upgrade the Primary and Alternate H.323 Gatekeepers to CS 1000 Release 4.5. It also allows you to upgrade the Failsafe H.323 Gatekeeper as time permits over the 45-day period. After 45 days, the Alternate NRS (CS 1000 Release 4.5) database will not recognize the Failsafe H.323 Gatekeeper.

If the Failsafe H.323 Gatekeeper is not upgraded to CS 1000 Release 4.5, then the Failsafe H.323 Gatekeeper cannot synchronize its database with the CS 1000 Release 4.5 NRS. The Failsafe H.323 Gatekeeper also cannot synchronize with the Release 4.5 dynamic database that contains registration information (which is essential for its operation). In this case, the Failsafe H.323 Gatekeeper maintains the old dynamic database to resolve queries (if the Failsafe becomes active).

# Task summary list

The following summarizes the tasks required to upgrade the H.323 Gatekeeper database to the new NRS database (CS 1000 Release 4.5).

**WARNING**

Complete each of these tasks in the order specified.

Failure to complete all of these tasks in the specified order will cause problems (see "Potential consequences" on page 135).

## Backing up the H.323 Database to your local PC

**1** Log in to the Gatekeeper web pages in the Succession 3.0 version of Element Manager (see Procedure 16 on page 138).

**2** Back up the existing H.323 Gatekeeper database to your local PC using the backup functionality in Succession 3.0 Element Manager (see Procedure 17 on page 141).

**IMPORTANT!**

Procedure 17 on page 141 provides instructions on backing up the database to the Signaling Server and to the local PC. You must back up the database to your local PC for the migration to be successful.

**3** Log out of the Gatekeeper web pages (see Procedure 18 on page 143).

## Upgrading and reconfiguring the Signaling Server

**1** Upgrade the Signaling Server from to CS 1000 Release 4.5 software. This includes the following tasks:

- **a** Download the Signaling Server CD image from the Nortel web site (see Procedure 4 on page 62).
- **b** Create a Signaling Server software CD-ROM (see Procedure 5 on page 63).

- **c** Upgrade the Signaling Server software (see Procedure 11 on page 98).

**2** Reconfigure the Signaling Server (see Procedure 12 on page 108).

### Copying the backed up H.323 Gatekeeper database to the upgraded Signaling Server

See Procedure 19 on page 145.

### Converting the H.323 Gatekeeper database to an NRS database using the NRS web interface

**1** Log in to the NRS Manager web interface (see Procedure 20 on page 147).

**2** Under the Configuration tab:

- **a** Add a new Service Domain (see Procedure 21 on page 151).
- **b** Add a new Level 1 Domain (L1 Domain) (see Procedure 22 on page 153).

**3** Under the Tools tab:

- **a** Use the GK/NRS Data Upgrade link to convert the backed-up H.323 Gatekeeper to an NRS database (see Procedure 23 on page 155).
- **b** View the conversion log file. This procedure is optional (see Procedure 24 on page 157).
- **c** Use the Database Actions link to cutover and commit the database (see Procedure 25 on page 158).

**4** Log out of NRS Manager (see Procedure 26 on page 159).

## Potential consequences

### Scenario 1

User fails to back up the H.323 Gatekeeper database and also unsuccessfully upgrades the Signaling Server software.

### Impact: Severe

Customer must downgrade the system to previous release software. This 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. The user does not realize that part of the conversion process did not proceed smoothly. If the user places the converted database into active service, then performance can degrade.
2. The user starts the conversion and does not watch the complete conversion process. When the user returns, it is possible to have missed informative error information.

## Scenario 3

The user mistypes the names of the Service Domain or Level 1 Domain.

### Impact: Minor

The user can access the Standby database and edit the names.

## Scenario 4

The user upgrades the Signaling Server to CS 1000 Release 4.5 software, but does not upgrade the database.

### Impact: Minor

The existing H.323 Gatekeeper database is not responding. The user interface has also been upgraded from the "old" H.323 Gatekeeper web pages to the "new" NRS interface. Therefore, if the user tries to use the H.323 Gatekeeper interface, the user cannot to see the active database (as the interface no longer exists). If the user tries to use the NRS interface, the user cannot read any data because the database has not been converted.

### Scenario 5

The user does not enter the Service Domain and Level 1 Domain, and proceeds directly to database conversion.

#### Impact: None

The NRS interface prevents the user from performing the database conversion upgrade if the Service Domain and Level 1 Domain names have not been entered. The user is informed that they have missed steps in the conversion process.

## Backing up the H.323 Gatekeeper database

### Description

You must back up the H.323 Gatekeeper database using the Gatekeeper web pages in the Succession 3.0 version of Element Manager. Two backup options are provided in the Gatekeeper web pages: Automatic Backup and Manual Backup (see Figure 79 on page 141). The Automatic Backup option allows you to schedule the backup at a later time and date. Use the Manual Backup option to back up the H.323 Gatekeeper database immediately.

The Manual Backup saves the database files to a directory on the Signaling Server. This location is later accessed by the NRS conversion tool to convert the H.323 Gatekeeper database to the NRS database.

### Backup procedures

Use the following procedures to backup the H.323 Gatekeeper database:

- Procedure 16 — Log in to the H.323 Gatekeeper web pages in Element Manager.
- Procedure 17 on page 141 — Back up the H.323 Gatekeeper database.
- Procedure 18 on page 143 — Log out of the H.323 Gatekeeper web pages.

**Procedure 16**
**Logging in to the H.323 Gatekeeper web pages in Element Manager**

**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, the 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 Sever platform with other applications.

The **Enter Network Password** login dialog box opens (see Figure 77).

***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.

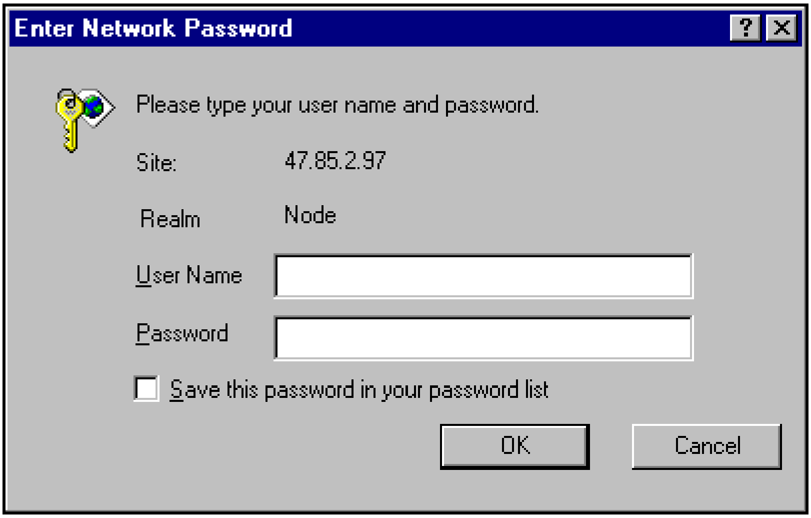
— Enter the **Gatekeeper IP Address**.

— Click **Next**.

— When the login window opens (see Figure 77), enter the **User Name** and **Password**.

— Click **OK**.

**Figure 77**
**Enter Network Password login dialog box**



Enter Network Password

Please type your user name and password.

Site: 47.85.2.97

Realm Node

User Name

Password

□ Save this password in your password list

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

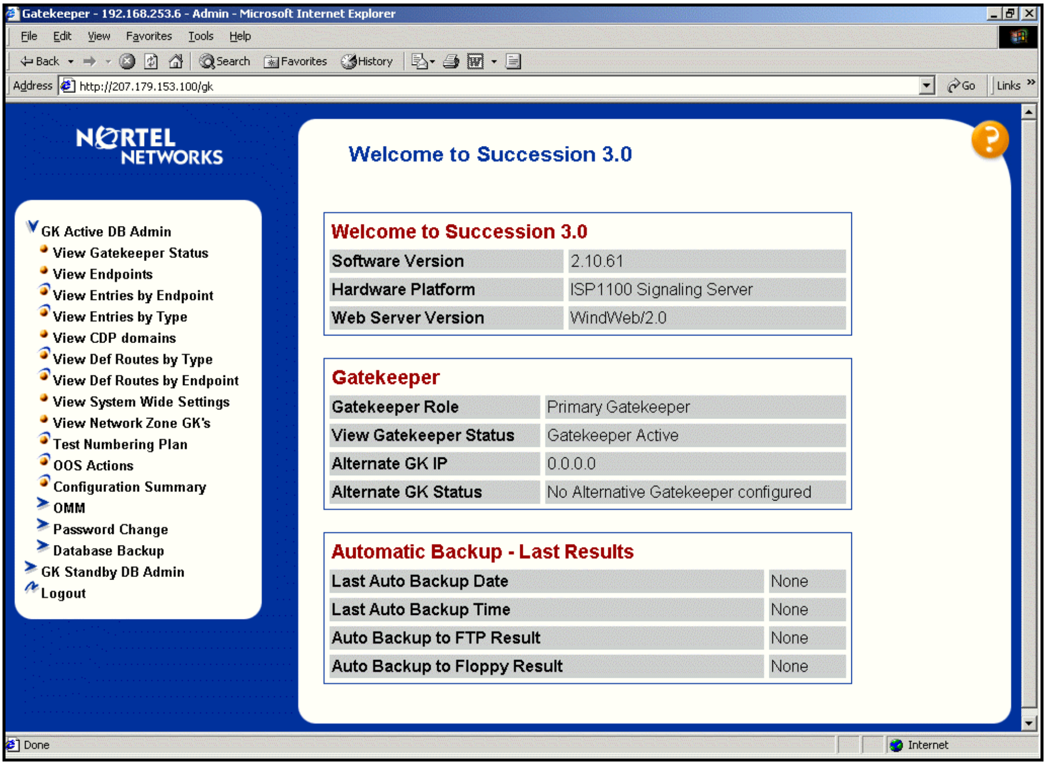
3 Enter your password in the **Password** text box (the default password is *gkadmin*).

4 Click **OK**.

If login is successful, the **Welcome** web page opens (see Figure 78).

If login is unsuccessful, an error message opens, and then the **Enter Network Password** dialog box reopens.

**Figure 78**
**Welcome web page**



Welcome to Succession 3.0

| Welcome to Succession 3.0 | |
|---|---|
| Software Version | 2.10.61 |
| Hardware Platform | ISP1100 Signaling Server |
| Web Server Version | WindWeb/2.0 |

| Gatekeeper | |
|---|---|
| Gatekeeper Role | Primary Gatekeeper |
| View Gatekeeper Status | Gatekeeper Active |
| Alternate GK IP | 0.0.0.0 |
| Alternate GK Status | No Alternative Gatekeeper configured |

| Automatic Backup - Last Results | |
|---|---|
| Last Auto Backup Date | None |
| Last Auto Backup Time | None |
| Auto Backup to FTP Result | None |
| Auto Backup to Floppy Result | None |

**End of Procedure**

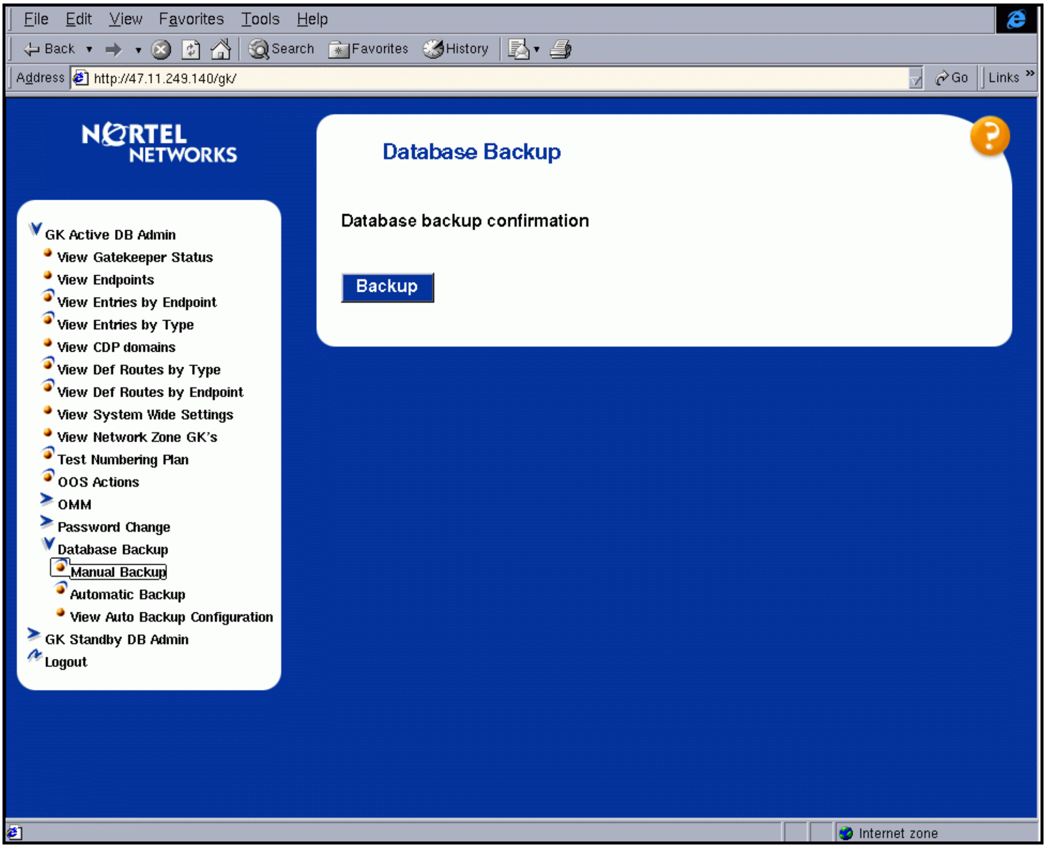
### Procedure 17
### Backing up the H.323 Gatekeeper database

You must back up the database to your local PC to ensure a successful database migration.

1 Select **GK Active DB Admin > Database Backup > Manual Backup** from the navigation tree to perform a manual backup of the database.

The Database Backup web page opens as in Figure 79.

**Figure 79**
**Manual database backup**



Database Backup

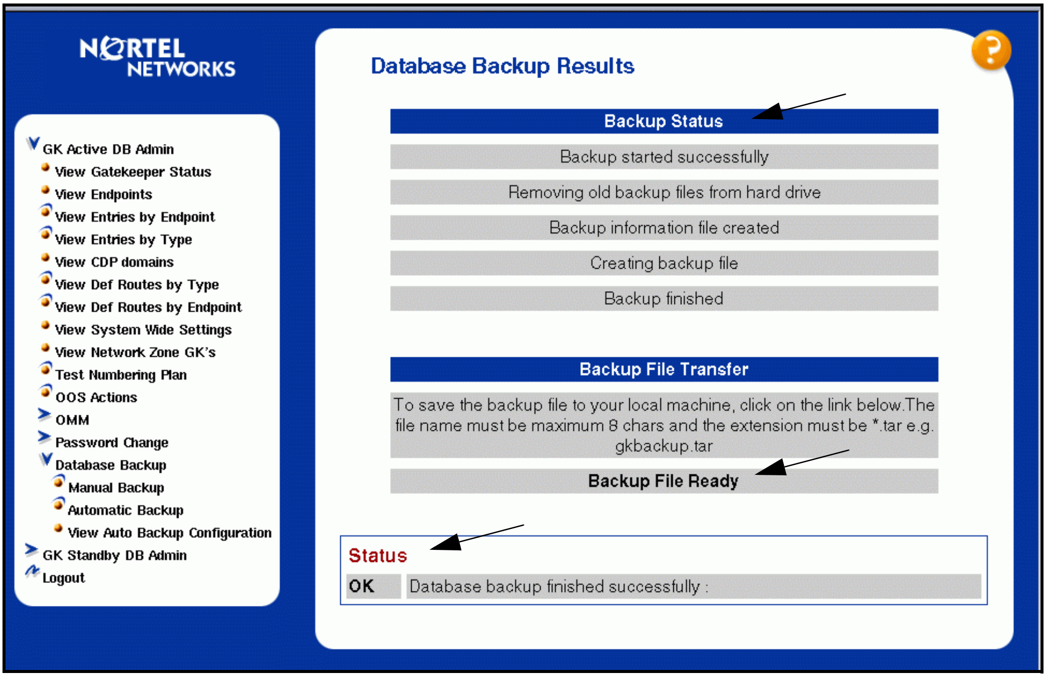
Database backup confirmation

Backup

**2** Click **Backup**.

The **Database Backup Results** web page opens as shown in Figure 80. The results display under the Backup Status area at the top of the web page and also in the Status area at the bottom of the web page.

**Figure 80**
**Manual Database Backup Results**



Database Backup Results

Backup Status

Backup started successfully

Removing old backup files from hard drive

Backup information file created

Creating backup file

Backup finished

Backup File Transfer

To save the backup file to your local machine, click on the link below.The file name must be maximum 8 chars and the extension must be *.tar e.g. gkbackup.tar

**Backup File Ready**

Status

OK Database backup finished successfully :

**IMPORTANT!**

You must save the backup file to your local PC. Use step 3 to step 5 on page 143.

**3** Click the Backup File Ready link (see Figure 80) in the middle of the Database Backup Results web page.

A download window opens.

**4** Select the folder location on your local PC to which to download and save the file.

**5** Click Save.

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

**7** 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.

- 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 17).

**End of Procedure**

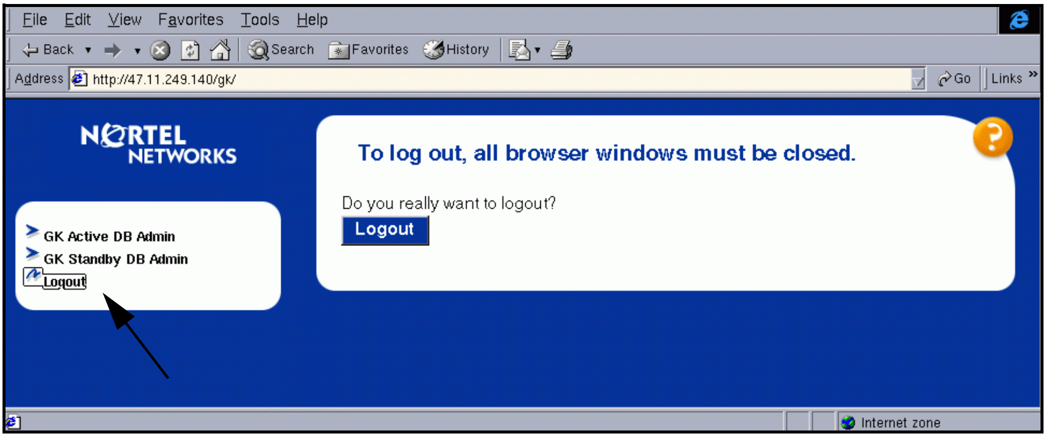
**Procedure 18**
**Logging out of the H.323 Gatekeeper web pages**

**1** Click **Logout** at the bottom of the navigation tree to log out of the H.323 Gatekeeper web pages Element Manager.

The Logout web page opens (see Figure 81 on page 144).

***Note:*** You must close all browser windows to log out.

**Figure 81**
**Logout web page**



To log out, all browser windows must be closed.

Do you really want to logout?

Logout

2 Click **Logout**.

3 Click **Yes**.

The browser window closes.

**End of Procedure**

# Upgrading and reconfiguring the Signaling Server

## Upgrading the Signaling Server software

Follow the procedures given in "Upgrading the Signaling Server software" on page 97.

**IMPORTANT!**

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

**IMPORTANT!**

When a Signaling Server is upgraded, its disk is completely erased. Therefore, it is critical that you back up your H.323 database to your local PC before beginning the upgrade (see Procedure 17 on page 141).

## Reconfiguring the Signaling Server

After upgrading the Signaling Server to CS 1000 Release 4.5, you must reconfigure the Signaling Server to obtain and configure the NRS. If you do not reconfigure the Signaling Server, you will not be able to use a SIP Redirect Server.

Follow the procedures given in "Reconfiguring the Signaling Server" on page 108.

# Copying the backed up H.323 Gatekeeper database to the upgraded Signaling Server

The H.323 Gatekeeper database must be copied back onto the upgraded Signaling Server before it can be converted for use by the NRS.

**Procedure 19**
**Copying the backed up H.323 Gatekeeper database to the upgraded Signaling Server**

1 Log into the upgraded Signaling Server.

2 FTP the backed up H.323 database file (gkbackup.tar) to the Signaling Server, in the following subdirectory:

```
/u/gk/database/
```

**End of Procedure**

The H.323 Gatekeeper database is now ready to be converted to an NRS database.

# Converting the H.323 Gatekeeper database to the NRS database

## Description

The existing H.323 Gatekeeper backup data cannot be directly used by the NRS.

NRS Manager provides a conversion tool called the "Gatekeeper/NRS Data Upgrade". This tool allows for conversion of the existing H.323 Gatekeeper backup data into an XML format, which then can be imported into the NRS database.

You must create a Service Domain and Level 1 Domain, as these two domains do not exist in the Gatekeeper. Once you create the Service and Level 1 Domains, the user must select these configured domains before converting the databases. The user must select the source location of the H.323 Gatekeeper data before database conversion begins.

The data is converted only to the standby database in the NRS. You must cutover and commit the database before the NRS can properly use the data.

## Conversion procedures

Use the following procedures to convert the H.323 Gatekeeper database to an NRS database:

- Procedure 20 — Log in to NRS Manager.
- Procedure 21 on page 151 — Add a Service Domain.
- Procedure 22 on page 153 — Add Level 1 Domain.
- Procedure 23 on page 155 — Convert the H.323 database to the NRS database.
- Procedure 24 on page 157 — View the conversion log file. This procedure is optional.
- Procedure 25 on page 158 — Save the conversion and to make the NRS database active.

- Procedure 26 on page 159 — Log out of the NRS.

### Procedure 20
### Logging in to NRS Manager

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/

3. The NRS Manager Login web page displays (see Figure 82 on page 149).

   You must enable the H.323 Gatekeeper or SIP Redirect Server before you can log in to NRS Manager. If you do not enable the H.323 Gatekeeper or the SIP Redirect Server, the web page turns white and the following error message displays:

   ```
   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 application(s).
   Reboot the Signaling Server, then access NRS Manager
   again.
   ```

   To enable the H.323 Gatekeeper or SIP Redirect Server, refer to *IP Peer Networking: Installation and Configuration* (553-3001-213)

4. Enter the **User ID** and **Password** to log in.

   You must use a username and password to prevent unauthorized access.

**IMPORTANT!**

Nortel recommends that you use the default User ID and Password when configuring the NRS server. When 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`**

CS 1000 Release 4.5 provides improved security through authentication and database access privileges. CS 1000 Release 4.5 introduces a username and password for accessing the NRS database. The username and password are stored (in encrypted format) in the same database as the SIP Redirect Server or Proxy Server data. NRS performs authentication, and authentication parameters are configurable in Element Manager.

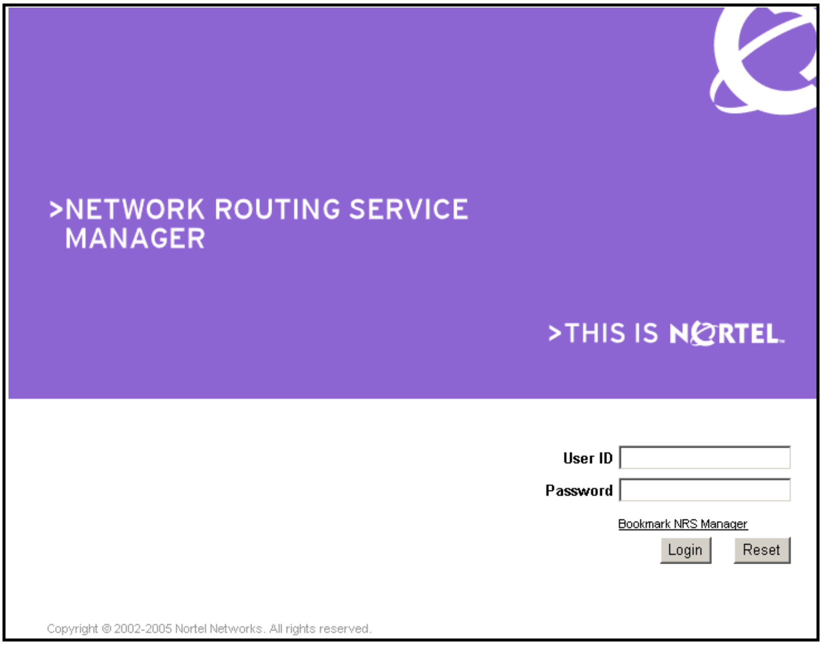
Two types of access privileges are supported:

- 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 1:*** Once you log in as an administrator, you can create new users. See *IP Peer Networking: Installation and Configuration* (553-3001-213).

**5** 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; however, this is configurable using the CLI.

**Figure 82**
**NRS Manager login web page**

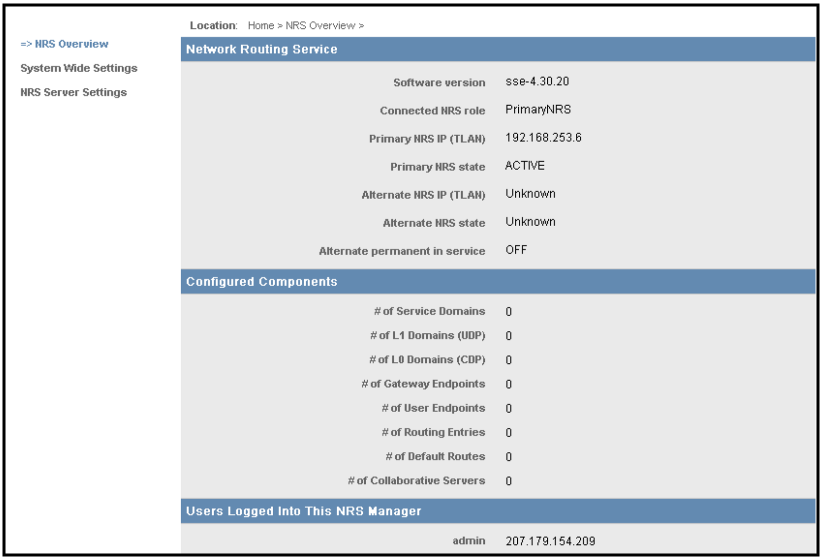


>NETWORK ROUTING SERVICE MANAGER
>THIS IS NORTEL
User ID
Password
Bookmark NRS Manager
Login
Reset
Copyright © 2002-2005 Nortel Networks. All rights reserved.

6 Click **Login**.

The **NRS Overview** page opens, as shown in Figure 83 on page 150.

**Figure 83**
**NRS Overview page**



Location: Home > NRS Overview >

Network Routing Service

| | |
|---|---|
| Software version | sse-4.30.20 |
| Connected NRS role | PrimaryNRS |
| Primary NRS IP (TLAN) | 192.168.253.6 |
| Primary NRS state | ACTIVE |
| Alternate NRS IP (TLAN) | Unknown |
| Alternate NRS state | Unknown |
| Alternate permanent in service | OFF |

Configured Components

| | |
|---|---|
| # of Service Domains | 0 |
| # of L1 Domains (UDP) | 0 |
| # of L0 Domains (CDP) | 0 |
| # of Gateway Endpoints | 0 |
| # of User Endpoints | 0 |
| # of Routing Entries | 0 |
| # of Default Routes | 0 |
| # of Collaborative Servers | 0 |

Users Logged Into This NRS Manager

| | |
|---|---|
| admin | 207.179.154.209 |

If the login is successful, then the User ID and Password are securely transferred from the web client to the NRS web server. The web server verifies the User ID and Password and if the login is valid, then the **NRS Overview** web page opens.

NRS Manager allows you to navigate to specific components of the NRS and allows you to configure and maintain these components.

If the login is not successful, then you may have entered an incorrect User ID or Password.

***Note 1:*** The **Reset** button clears the User ID and Passwords text boxes.

To add an bookmark to your Internet Explorer Favorites list, click the **Bookmark NRS Manager** link on the login page.

**End of Procedure**

### Procedure 21
### Adding a Service Domain

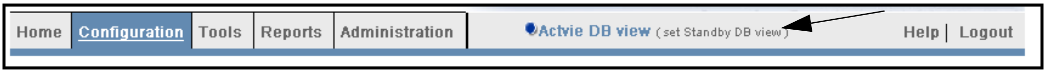
1 Click **set Standby DB view** to switch to the standby database (see Figure 84).

To the right of the tabs is an area for switching between the active and standby databases (see Figure 84). The database has two schemas: active and standby.

- The active database is used for runtime queries.
- The standby database is used for administrator modifications.

The database must be in Standby DB view to be modified. By default, the database is in Active DB view when the NRS is launched.

**Figure 84**
**Active DB view selected**

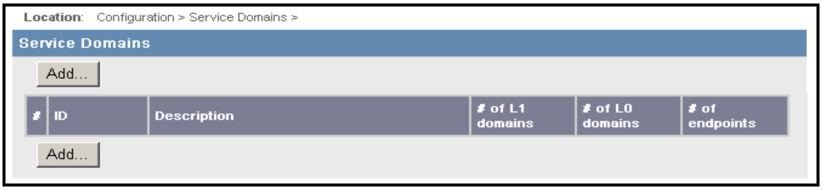


2 Click the **Configuration** tab.

3 Click **Service Domains** from the navigation tree.

The Service Domains web page opens (see Figure 85).

**Figure 85**
**Service Domains**

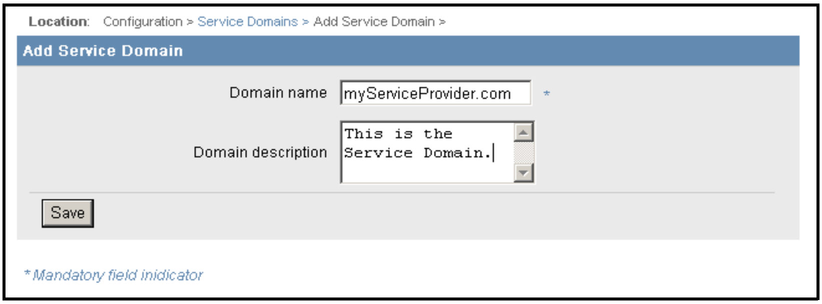


| # | ID | Description | # of L1 domains | # of L0 domains | # of endpoints |
|---|---|---|---|---|---|

4 Click **Add**.

The **Add Service Domain** web page opens (see Figure 86 on page 152).

**Figure 86**
**Add Service Domain**



Location: Configuration > Service Domains > Add Service Domain >

Add Service Domain

Domain name: myServiceProvider.com *

Domain description: This is the Service Domain.

* Mandatory field indicator

5 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.

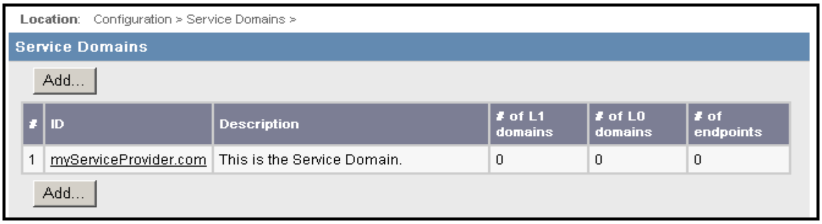
6 Enter a **Domain description** for the Service Domain.

7 Click **Save**.

Clicking Save updates the Standby database. The data is visible only in the Standby database (see Procedure 25 on page 158).

The Service Domains web page opens showing the newly added Service Domain (see Figure 87).

**Figure 87**
**Added Service Domain**



Location: Configuration > Service Domains >

Service Domains

| # | ID | Description | # of L1 domains | # of L0 domains | # of endpoints |
|---|---|---|---|---|---|
| 1 | myServiceProvider.com | This is the Service Domain. | 0 | 0 | 0 |

**End of Procedure**

### Procedure 22
### Adding an L1 Domain

1 Click **set Standby DB view** to switch to the standby database (see Figure 84 on page 151).

2 Click the **Configuration** tab.

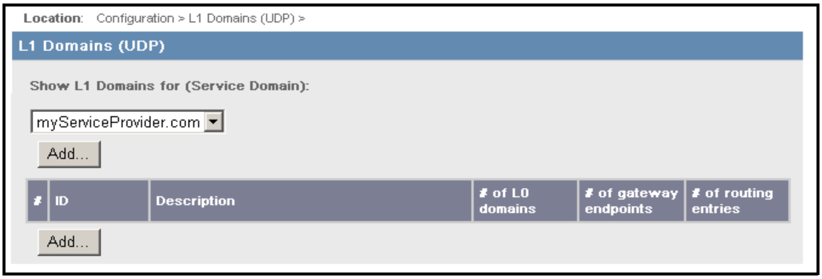
3 Click **L1 Domains** from the navigation tree.

The **L1 Domains** web page opens (see Figure 88). There is a drop-down list containing any available Service Domains.

4 Select the Service Domain from the drop-down list.

This is the Service Domain where the new L1 subdomain will be added.

**Figure 88**
**L1 Domains**



Location: Configuration > L1 Domains (UDP) >

L1 Domains (UDP)

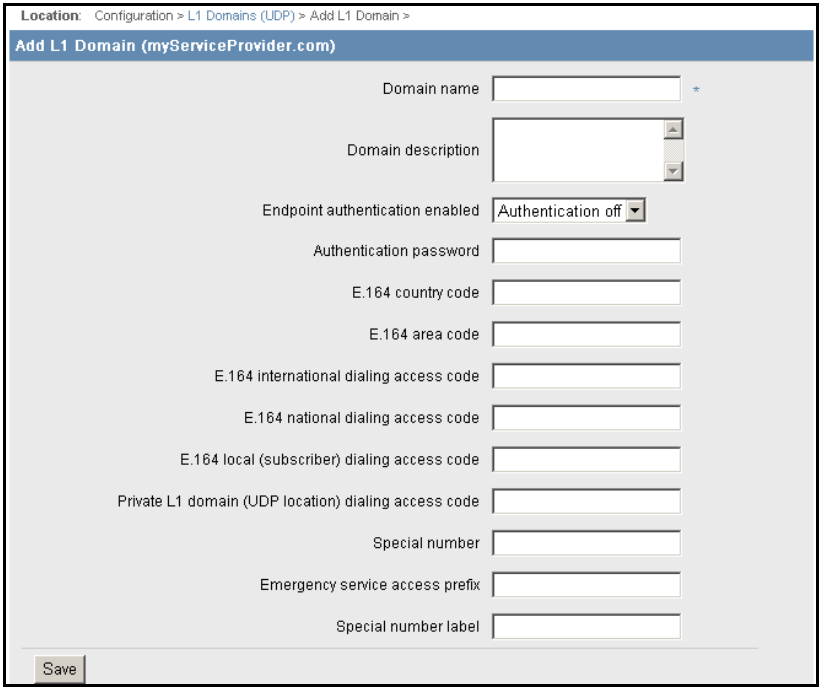
Show L1 Domains for (Service Domain): myServiceProvider.com

| # | ID | Description | # of L0 domains | # of gateway endpoints | # of routing entries |
|---|---|---|---|---|---|

5 Click **Add**.

The **Add L1 Domain** web page opens (see Figure 89 on page 154).

**Figure 89**
**Add L1 Domain**



Location: Configuration > L1 Domains (UDP) > Add L1 Domain >

Add L1 Domain (myServiceProvider.com)

| | |
|---|---|
| Domain name | * |
| Domain description | |
| Endpoint authentication enabled | Authentication off |
| Authentication password | |
| E.164 country code | |
| E.164 area code | |
| E.164 international dialing access code | |
| E.164 national dialing access code | |
| E.164 local (subscriber) dialing access code | |
| Private L1 domain (UDP location) dialing access code | |
| Special number | |
| Emergency service access prefix | |
| Special number label | |

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

7 Enter the **Domain description**.

8 Select whether authentication is on or off from the **End point authentication enabled** drop-down list.

If **Authentication on** is selected, then 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**.

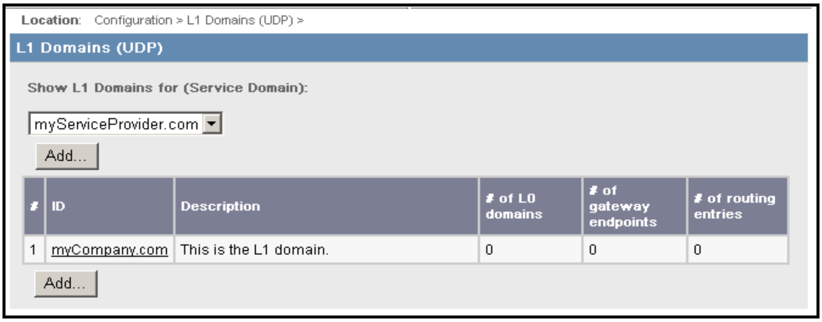
**17** Enter the **Emergency service access prefix**.

**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 opens showing the newly added domain in the Service Domain (see Figure 90).

**Figure 90**
**Added L1 Domain**



Location: Configuration > L1 Domains (UDP) >

L1 Domains (UDP)

Show L1 Domains for (Service Domain):

myServiceProvider.com

| # | ID | Description | # of L0 domains | # of gateway endpoints | # of routing entries |
|---|---|---|---|---|---|
| 1 | myCompany.com | This is the L1 domain. | 0 | 0 | 0 |

**End of Procedure**

### Procedure 23
### Converting the H.323 Gatekeeper database to the NRS database

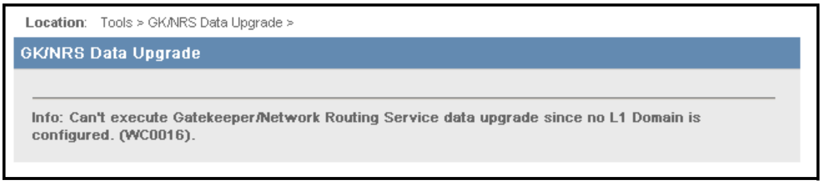
**1** Click the **Tools** tab.

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

If you have configured the Service Domain and Level 1 Domain, then the GK/NRS Data Upgrade web page opens (see Figure 92 on page 156).

If you have not configured the Service Domain or Level 1 Domain, a message appears indicating that the Gatekeeper-to-Networking Routing Service data upgrade cannot execute since a Level 1 Domain has not been configured. Ensure that Procedure 21 on page 151 and Procedure 22 on page 153 are completed before starting Procedure 23.

**Figure 91**
**Domains not configured**

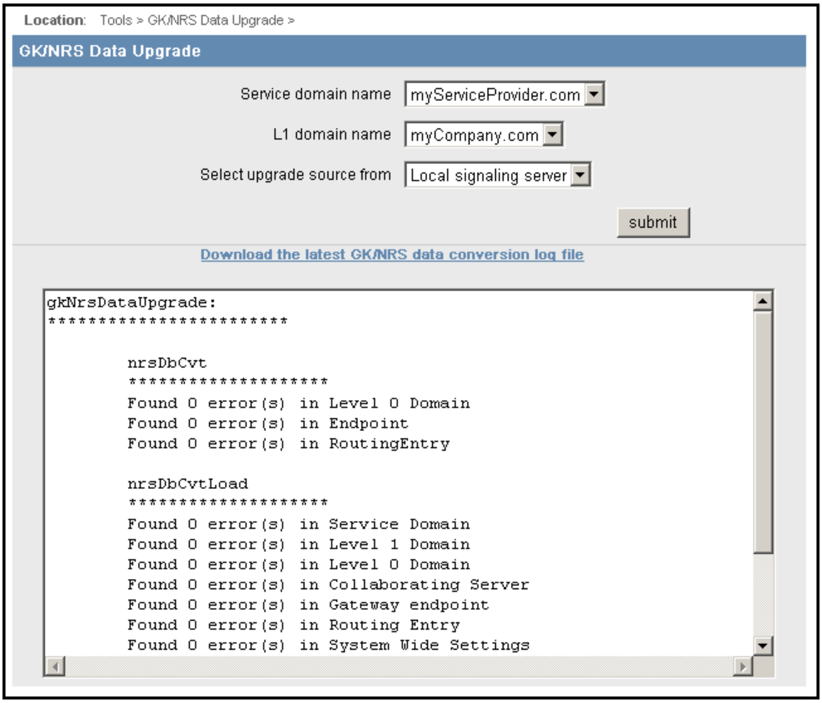


Location: Tools > GK/NRS Data Upgrade >

GK/NRS Data Upgrade

Info: Can't execute Gatekeeper/Network Routing Service data upgrade since no L1 Domain is configured. (WC0016).

**Figure 92**
**GK/NRS Data Upgrade**



Location: Tools > GK/NRS Data Upgrade >

GK/NRS Data Upgrade

Service domain name: myServiceProvider.com

L1 domain name: myCompany.com

Select upgrade source from: Local signaling server

```
gkNrsDataUpgrade:
************************


        nrsDbCvt
        ********************
        Found 0 error(s) in Level 0 Domain
        Found 0 error(s) in Endpoint
        Found 0 error(s) in RoutingEntry

        nrsDbCvtLoad
        ********************
        Found 0 error(s) in Service Domain
        Found 0 error(s) in Level 1 Domain
        Found 0 error(s) in Level 0 Domain
        Found 0 error(s) in Collaborating Server
        Found 0 error(s) in Gateway endpoint
        Found 0 error(s) in Routing Entry
        Found 0 error(s) in System Wide Settings
```

**3** Select the Service Domain (configured in Procedure 21 on page 151) from the **Service domain name** drop-down list.

4 Select the correct Level 1 Domain (configured in Procedure 22 on page 153) from the **L1 domain name** drop-down list.

5 Select **Local signaling server** from the **Select Upgrade source from** drop-down list.

6 Click **Submit**.

Once the H.323 Gatekeeper database is converted to an NRS database, the NRS database is loaded in Standby view.

**End of Procedure**

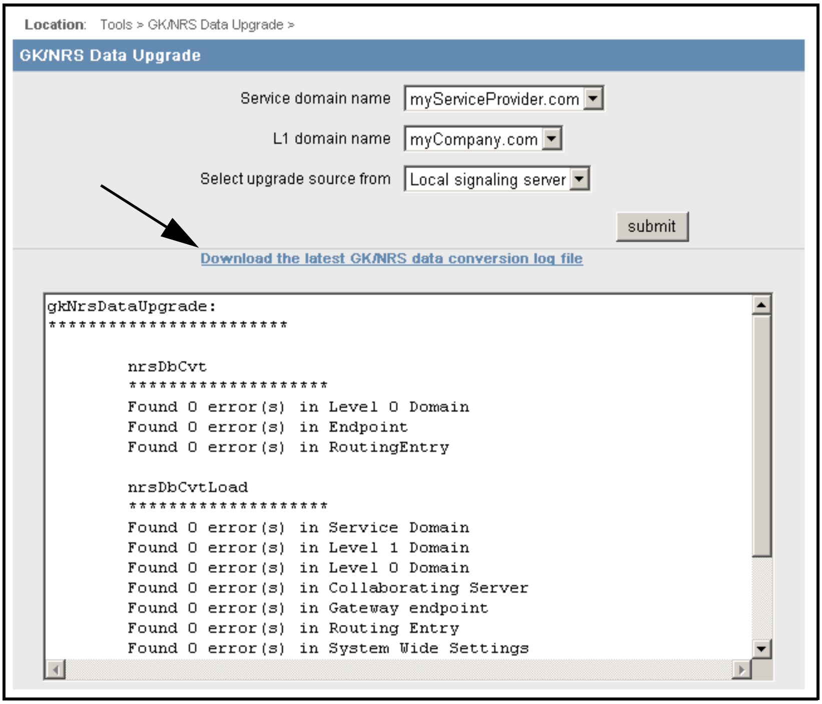
### Procedure 24
### Viewing the conversion log file

This procedure is optional.

1 Click the **Download the latest GK/NRS conversion log file** link to view the log file (see Figure 93 on page 158).

The conversion log file opens. The log file is an XML file named cvtLog.xml. Any conversion errors are written to this file.

### Figure 93
### Conversion log file link


Location: Tools > GK/NRS Data Upgrade >
GK/NRS Data Upgrade
submit
Download the latest GK/NRS data conversion log file

Service domain name: myServiceProvider.com

L1 domain name: myCompany.com

Select upgrade source from: Local signaling server

```
gkNrsDataUpgrade:
************************


        nrsDbCvt
        ********************
        Found 0 error(s) in Level 0 Domain
        Found 0 error(s) in Endpoint
        Found 0 error(s) in RoutingEntry

        nrsDbCvtLoad
        ********************
        Found 0 error(s) in Service Domain
        Found 0 error(s) in Level 1 Domain
        Found 0 error(s) in Level 0 Domain
        Found 0 error(s) in Collaborating Server
        Found 0 error(s) in Gateway endpoint
        Found 0 error(s) in Routing Entry
        Found 0 error(s) in System Wide Settings
```

2 Close the conversion log file window when you finish viewing the log file.

**End of Procedure**

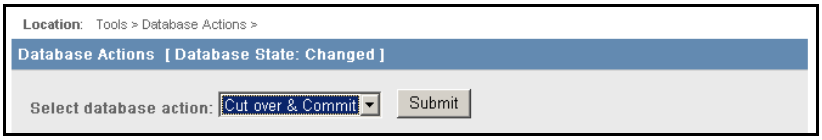
### Procedure 25
### Saving changes to the database

1 Click the **Tools** tab.

2 Select **Database Actions** from the navigation tree.

3 Select **Cut over & Commit** from the **Select database action** drop-down list (see Figure 94 on page 159).

**Figure 94**
**Database Actions – cutover and commit**

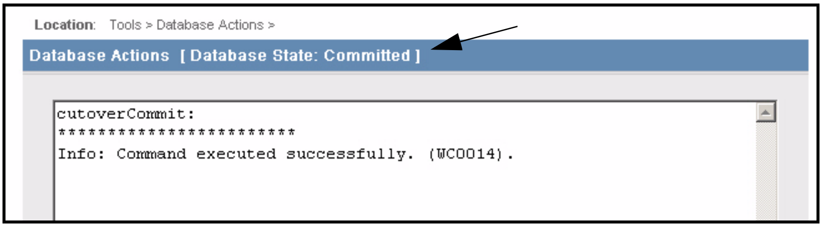


Location: Tools > Database Actions >
Database Actions [ Database State: Changed ]
Select database action: Cut over & Commit
Submit

4 Click **Submit**.

A message displays in the text box indicating that the cutover and commit operation was successful (see Figure 95). Figure 95 also shows the status of the database.

**Figure 95**
**Database Actions – cutover and commit (successful)**



Location: Tools > Database Actions >
Database Actions [ Database State: Committed ]

```
cutoverCommit:
************************
Info: Command executed successfully. (WC0014).
```

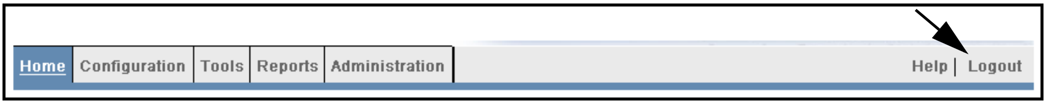
The NRS database is saved and is in Active DB view.

**End of Procedure**

**Procedure 26**
**Logging out of NRS Manager**

1 Click **Logout** (see Figure 96).

**Figure 96**
**Logout**



The Networking Routing Service Manager logout screen opens.

2 Close the browser window.

**End of Procedure**

## Migrating from one Signaling Server to another

The following section describes the procedures used to migrate an NRS database from a ***source*** Signaling Server running CS 1000 Release 4.5 software to a ***target*** Signaling Server running CS 1000 Release 4.5 software.

The following summarizes the tasks required to perform the database migration:

- "Preparing for migration" on page 160
- "Uploading the database" on page 162
- "Restoring the database file" on page 163
- "Activating the target NRS database" on page 163

**Procedure 27**
**Preparing for migration**

1 Log in to the source Signaling Server.

2 Verify that the source Signaling Server is running CS 1000 Release 4.5 software. If it is not, complete the upgrade and conversion procedures described in "Software upgrade and reconfiguration" on page 95 to upgrade the source Signaling Server to CS 1000 Release 4.5 software.

At this point, verify that the backup file generated in the correct directory on the source Signaling Server by completing the following steps:

3 Look for the compressed tar file (nrsback.tar) in the appropriate directory (/u/db/backup/tar/).

4 Check the list of files contained within the backup tar file:

- bootp.tab
- config.ini
- csr.xml
- dbv.xml
- gep.xml
- l0d.xml
- l1d.xml
- rey.xml
- sdm.xml
- sws.xml
- usr.xml

5 If the list of files within the backup tar file is not exactly as above, repeat the entire backup procedure on the source Signaling Server. (Procedure 17 on page 141).

6 Log in to the target Signaling Server verifying that it is running the same software load version as the source Signaling Server.

If the software version on the target Signaling Server does not match the software version running on the source Signaling Server, perform "Upgrading the Signaling Server software" on page 97 on the target Signaling Server.

***Note:*** To back up the data from the database on the target Signaling Server, perform "Backing up the H.323 Gatekeeper database" on page 141 on the target Signaling Server.

7 Choose one of the following steps to preserve the tar file (nrsback.tar of the target Signaling Server in the process of migration:

- Save the backup file under a different name.
- Transfer the file to another server or workstation.
- Move or copy the file to a different directory.

**End of Procedure**

**Procedure 28**
**Uploading the database**

1 Establish an FTP connection to the source Signaling Server.

- Type: **FTP x** (at the Windows command line)
  - — where "**x**" is the ELAN IP address of the *source* Signaling Server
- Enter your level 1 username and password at the prompts.
  - — userid/password = admin1/0000

2 Navigate to the directory /u/db/backup/tar.

- Type: **cd /u/db/backup/tar**

3 Download the database backup file (nrsback.tar) from the source Signaling Server to the local drive.

- Type: **get nrsback.tar**
  - — This downloads the file to a default location on the local hard drive.

4 Establish an FTP connection to the target Signaling Server.

- Type: **FTP x** (at the Windows command line)
  - — where "**x**" is the ELAN IP address of the *target* Signaling Server
- Enter your level 1 username and password at the prompts.
  - — userid/password = admin1/0000

5 Navigate to the directory /u/db/backup/tar.

- Type: **cd /u/db/backup/tar**

6 Upload the database backup file you downloaded in step 3 (nrsback.tar).

- Type: **put nrsback.tar**
  - — This uploads the file from the default location on the local hard drive to the /u/db/backup/tar directory on the target Signaling Server.

7 Check the size of the transferred file, ensuring it is the same size as the original.

8 Close all FTP connections.

**End of Procedure**

**Procedure 29**
**Restoring the database file**

1 Log in to NRS Manager on the target Signaling Server.

2 Go to **Tools**.

3 Click **Database Restore**.

4 Monitor log messages displayed 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 has to 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.

Data from the old StandBy database is replaced with data from the new NRS database. The new NRS database is loaded in standby view. You must perform database activation (Procedure 30) to complete the migration process.

**End of Procedure**

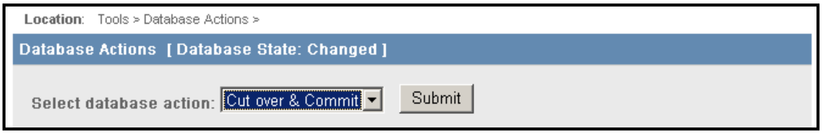
**Procedure 30**
**Activating the target NRS database**

1 Click the **Tools** tab.

2 Select **Database Actions** from the navigation tree.

3 Select **Cut over & Commit** from the **Select database action** drop-down list (see Figure 97 on page 164).

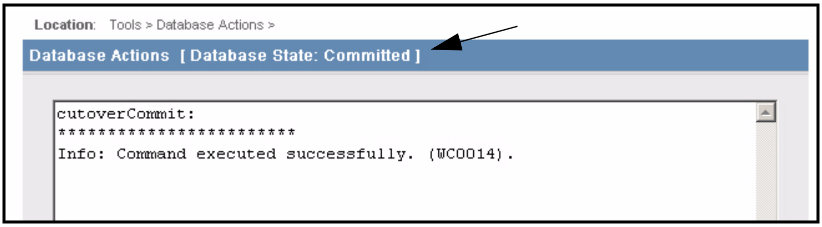
**Figure 97**
**Database Actions – cutover and commit**


Location: Tools > Database Actions >
Database Actions [ Database State: Changed ]
Select database action: Cut over & Commit
Submit

**4** Click **Submit**.

A message displays in the text box indicating that the cutover and commit command was executed successfully (see Figure 98). Figure 98 also shows the status of the database.

**Figure 98**
**Database Actions – cutover and commit (successful)**


Location: Tools > Database Actions >
Database Actions [ Database State: Committed ]

```
cutoverCommit:
************************
Info: Command executed successfully. (WC0014).
```

The NRS database is saved and is in Active DB view.

**End of Procedure**

# 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 Optivity Telephony Manager (OTM). The OTM 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* (553-3001-332).

# 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 is 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.

**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 Procedure 31 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.

- Set empty session information.
- Deselect the AutoComplete options.

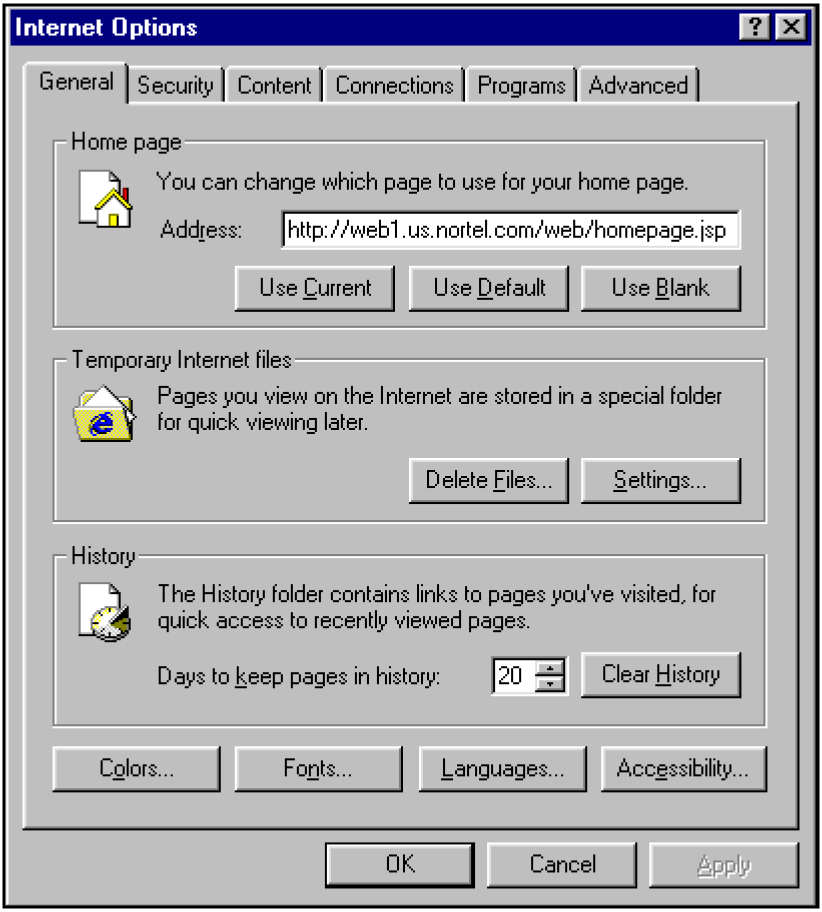
**Procedure 31**
**Configure the Internet Explorer browser settings**

1 Select **View** > **Text Size** > **Medium** to set the text size in the browser.

2 Select **Tools** > **Internet Options** In the Internet Explorer browser window.

The **Internet Options** window opens, as shown in Figure 99.

**Figure 99**
**Internet Options window**



You can change which page to use for your home page.

Address: http://web1.us.nortel.com/web/homepage.jsp

Pages you view on the Internet are stored in a special folder for quick viewing later.

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

Days to keep pages in history: 20

**3** Turn off Internet Explorer caching:

- **a.** On the **General** tab under the **Temporary Internet files** section, click **Settings**.

  The **Settings** window opens.

- **b.** Under the **Check for newer versions of stored pages** section, select the **Every visit to the page** option.

- **c.** Click **OK**.

**4** Set empty session information:

- **a.** Select the **Advanced** tab.

  The Advanced Settings window opens.

- **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 opens.

- **c.** Under the **Use AutoComplete for** section, deselect **Forms** and **User names and passwords on forms**.

**6** (Optional) Set the Windows display settings.

- **a.** Select **Start > Settings > Control Panel > Display**.

  The **Display Settings** window opens.

- **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 of Procedure**

# Logging in to Element Manager

Before logging in to Element Manager, obtain the IP address of:

- the Signaling Server
- the Call Server (or MG 1000B Core if at a branch office)

### Procedure 32
### Logging in to Element Manager

Before beginning this procedure, be sure that you have configured the browsers properly, using Procedure 31 on page 168.

1 Open Internet Explorer.

2 Enter the ELAN or TLAN network interface IP Address of the primary Signaling Server as the URL.

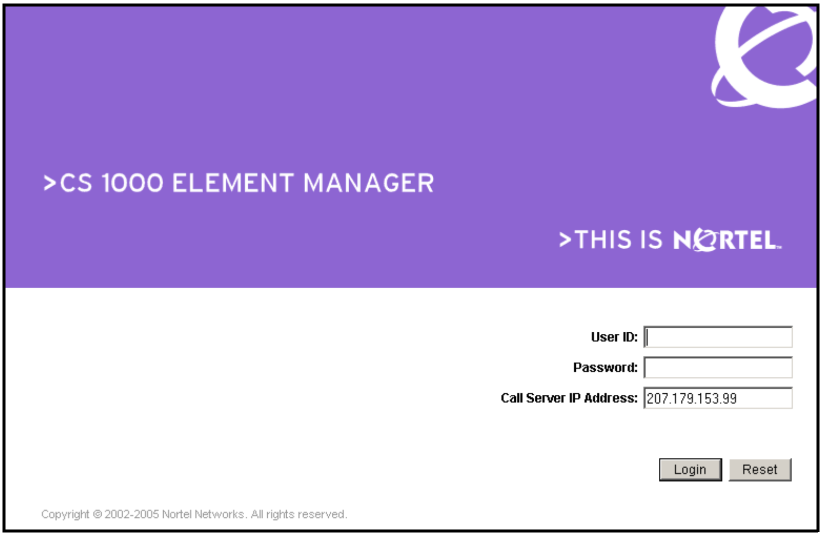
***Note:*** Do not assign the same IP address for the Node ID and the TLAN network interface IP address. This must be verified manually. The Node IP address must be on the same subnet as the TLAN network interface IP addresses of the Media Cards. In addition, the TLAN and ELAN network interfaces of the 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 login page opens (see Figure 100 on page 171).

Initially, you may be prompted to enter the Call Server IP address. This is because the Call Server is used for web login authorization. This is a requirement, since 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.

**Figure 100**
**Element Manager login page**



User ID:

Password:

Call Server IP Address: 207.179.153.99

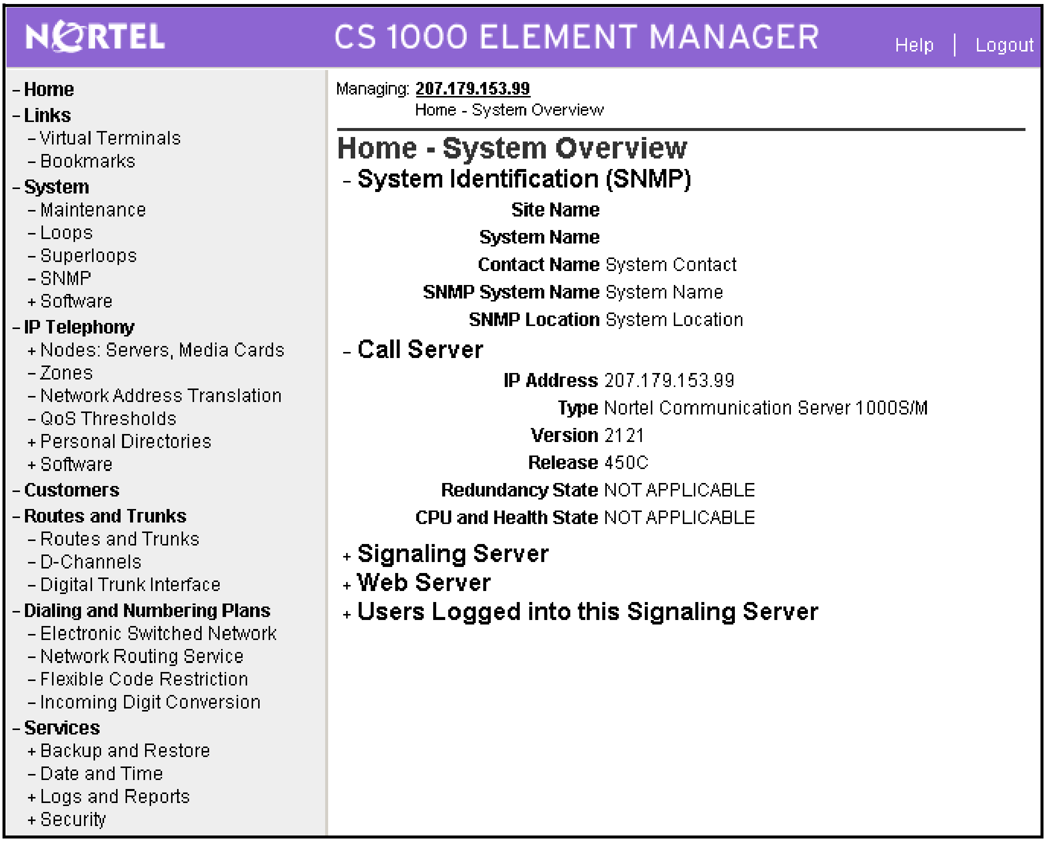
Copyright © 2002-2005 Nortel Networks. All rights reserved.

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 has been accessed, the login user IDs and passwords will not have been changed. The default Level 1 or Level 2 user ID and password are used.

If login is successful, the Element Manager **System Overview** web page (with the navigator) opens. See Figure 101 on page 172.

**Figure 101**
**Element Manager — System Overview web page with navigator**



Managing: 207.179.153.99
Home - System Overview

Home - System Overview

- System Identification (SNMP)

**Site Name**
**System Name**
**Contact Name** System Contact
**SNMP System Name** System Name
**SNMP Location** System Location

- Call Server

**IP Address** 207.179.153.99
**Type** Nortel Communication Server 1000S/M
**Version** 2121
**Release** 450C
**Redundancy State** NOT APPLICABLE
**CPU and Health State** NOT APPLICABLE

+ Signaling Server
+ Web Server
+ Users Logged into this Signaling Server

Now you can begin to configure the Call Server or IP telephony node. For more information, see *IP Line: Description, Installation, and Operation* (553-3001-365) and *Element Manager: System Administration* (553-3001-332).

**End of Procedure**

**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.

**Procedure 33**
**Changing the web server security flag**

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.

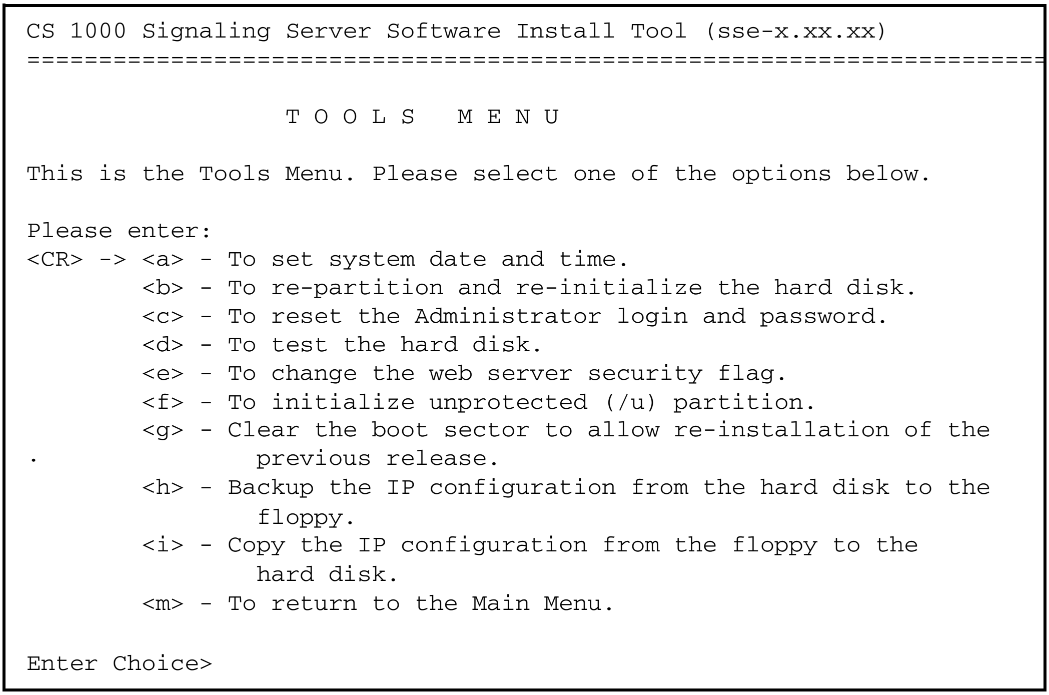
**1** Open the Tools Menu in the Signaling Server Install Tool.

**a.** Load the Signaling Server Install Tool.

**b.** At the Main Menu, enter **t** to open the **Tools Menu**.

The **Tools Menu** is displayed, as shown in Figure 102 on page 174.

**Figure 102**
**Tools menu**



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

                  T O O L S   M E N U

This is the Tools Menu. Please select one of the options below.

Please enter:
<CR> -> <a> - To set system date and time.
        <b> - To re-partition and re-initialize the hard disk.
        <c> - To reset the Administrator login and password.
        <d> - To test the hard disk.
        <e> - To change the web server security flag.
        <f> - To initialize unprotected (/u) partition.
        <g> - Clear the boot sector to allow re-installation of the
.                 previous release.
        <h> - Backup the IP configuration from the hard disk to the
                  floppy.
        <i> - Copy the IP configuration from the floppy to the
                  hard disk.
        <m> - To return to the Main Menu.

Enter Choice>
```

2 Enter **e** to change the web server security flag. The current value of the flag displays:

```
Currently, the flag is set to: DISABLED
```

3 Change the flag:

   **a.** To disable the web server security flag, enter **a**. The new value of the flag displays.

   **b.** To enable the web server security flag, enter **b**. The new value of the flag displays.

   **c.** To exit this menu without changing the web server security flag, enter **q**.

4 Enter **m** to exit the Signaling Server Install Tool.

**5** Import the IP Telephony node files for the web security flag change to take effect. Refer to "Importing IP Telephony node files" on page 179.

If this is a first-time Signaling Server or node installation, the preconfigured IP Telephony node files are imported. If this is an upgrade of the Signaling Server, the web server security flag change is saved to the master copy of the node files on the Call Server.

**End of Procedure**

## 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. However, they can be unpacked at any time after the Signaling Server software is installed. Use Procedure 34 to unpack the Help files.

**IMPORTANT!**

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

**Procedure 34**
**Unpacking Help files for Virtual Terminal Emulator**

Before you begin this procedure, ensure that the Signaling Server software is already installed.

**1** Reboot the Signaling Server.

**2** Log in to the Signaling Server CLI. Use Procedure 8 on page 93.

**3** Enter the following command at the prompt:

```
unpackVTHelp
```

**End of Procedure**

Refer to *Element Manager: System Administration* (553-3001-332) 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 OTM or Element Manager, and are fully described in *IP Line: Description, Installation, and Operation* (553-3001-365).

## 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, which 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, by using the EDD command in LD 43. Refer to *Software Input/Output: Maintenance* (553-3001-511) 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" on page 181.

When a Leader Signaling Server is first installed, the IP Telephony nodes are preconfigured during software installation. The node configuration files are then imported into Element Manager for further configuration of the nodes. 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

**IMPORTANT!**

Do not attempt to alter the above database files manually or by importing to IP Trunk or IP Telephony management in OTM. Use Element Manager.

IP Telephony nodes are configured in Element Manager. Therefore, a Signaling Server, which hosts Element Manager, must be installed. See "Element Manager configuration" on page 165.

For more information about IP Telephony nodes and their configuration, refer to *IP Line: Description, Installation, and Operation* (553-3001-365). For more information about Element Manager, refer to *Element Manager: System Administration* (553-3001-332).

# IP Telephony configuration procedures

> **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 (see “Backing up IP Telephony node configuration files” on page 181).

This section summarizes procedures used to configure IP Telephony. For more information, and detailed procedures using OTM or Element Manager, refer to *IP Line: Description, Installation, and Operation* (553-3001-365).

For information about upgrading IP Trunk nodes, refer to *Communication Server 1000S: Upgrade Procedures* (553-3031-258), *Communication Server 1000E: Upgrade Procedures* (553-3041-258), *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures* (553-3021-258), or *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures* (553-3011-258).

## Importing IP Telephony node files

Use this procedure to import existing IP Telephony nodes, including those that have been preconfigured during software installation of a Signaling Server (see Procedure 6 on page 66).

## Adding a Follower Signaling Server to a node

Use Procedure 7 on page 89 to add a follower Signaling Server to an IP Telephony node.

After software installation and reboot, the Follower Signaling Server sends out BOOTP requests, and waits for a response. Since the Follower Signaling Server has not booted successfully before, it waits for a BOOTP response that will not arrive. Do not wait for this response; perform this procedure immediately.

*Note:* The first time the Follower Signaling Server is installed, the FTP fails. The failure occurs because the Follower cannot obtain the system login and password, and does not have the current CONFIG.INI file with the Call Server IP address. In subsequent Follower installations, FTP 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 1000S: Upgrade Procedures* (553-3031-258), *Communication Server 1000E: Upgrade Procedures* (553-3041-258), *Communication Server 1000M and Meridian 1: Large System Upgrade Procedures* (553-3021-258), or *Communication Server 1000M and Meridian 1: Small System Upgrade Procedures* (553-3011-258).

## 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.

**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 at 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$^{TM}$ 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 in to the Signaling Server to use the CLI. See Procedure 8 on page 93.

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”.

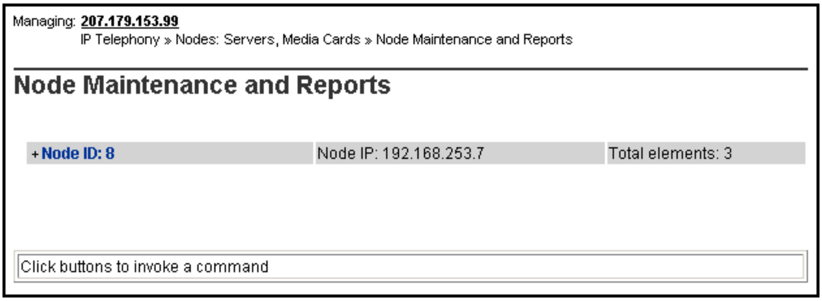
Use Procedure 35 to access the commands in Element Manager.

**Procedure 35**
**Accessing CLI commands in Element Manager**

1. Log in to Element Manager, using Procedure 32 on page 170.
2. Select **IP Telephony > Nodes: Servers, Media Cards > Maintenance and Reports** from the navigator.

   The **Node Maintenance and Reports** web page opens, listing the configured nodes. See Figure 103 on page 186.

**Figure 103**
**Node Maintenance and Reports web page**



Managing: **207.179.153.99**
IP Telephony » Nodes: Servers, Media Cards » Node Maintenance and Reports

Node Maintenance and Reports

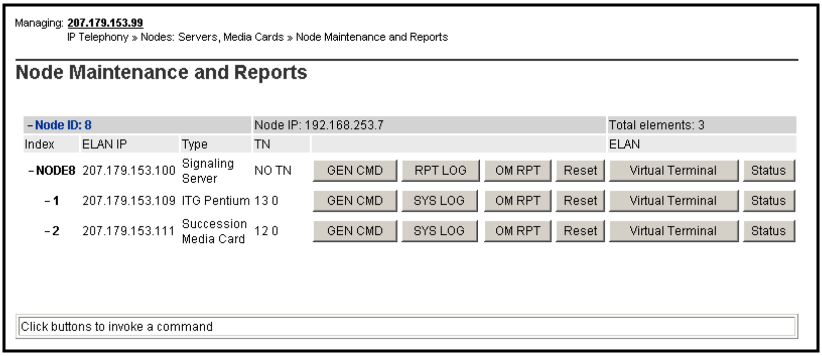
| + Node ID: 8 | Node IP: 192.168.253.7 | Total elements: 3 |
|---|---|---|

Click buttons to invoke a command

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. See Figure 104.

**Figure 104**
**Expanded IP Telephony node**



Managing: **207.179.153.99**
IP Telephony » Nodes: Servers, Media Cards » Node Maintenance and Reports

Node Maintenance and Reports

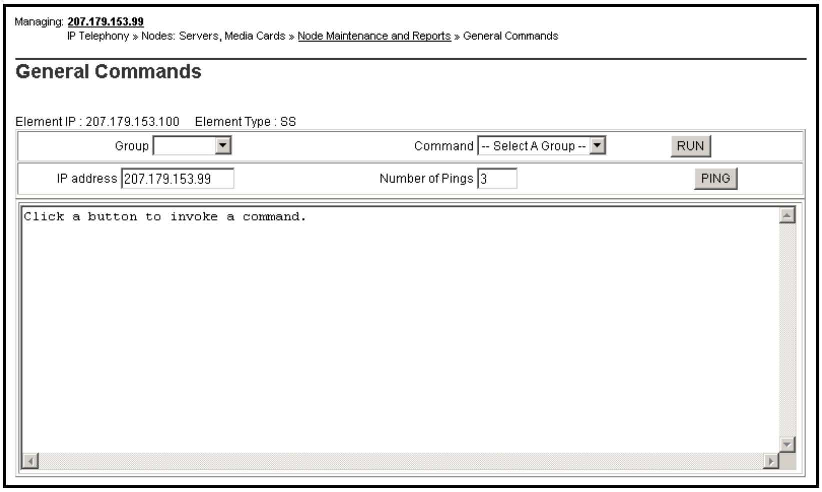
| - Node ID: 8 | | | Node IP: 192.168.253.7 | | | | | Total elements: 3 | |
|---|---|---|---|---|---|---|---|---|---|
| Index | ELAN IP | Type | TN | | | | | ELAN | |
| - NODE8 | 207.179.153.100 | Signaling Server | NO TN | GEN CMD | RPT LOG | OM RPT | Reset | Virtual Terminal | Status |
| - 1 | 207.179.153.109 | ITG Pentium | 13 0 | GEN CMD | SYS LOG | OM RPT | Reset | Virtual Terminal | Status |
| - 2 | 207.179.153.111 | Succession Media Card | 12 0 | GEN CMD | SYS LOG | OM RPT | Reset | Virtual Terminal | Status |

Click buttons to invoke a command

4 Click **GEN CMD** for the Signaling Server element.

The **General Commands** web page opens, as shown in Figure 105 on page 187.

**Figure 105**
**General Commands web page**



Managing: 207.179.153.99
IP Telephony » Nodes: Servers, Media Cards » Node Maintenance and Reports » General Commands

General Commands

Element IP : 207.179.153.100 Element Type : SS

Group Command -- Select A Group --

IP address 207.179.153.99 Number of Pings 3

```
Click a button to invoke a command.
```

**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 of Procedure**

For more information on Element Manager, refer to "Element Manager configuration" on page 165 and *Element Manager: System Administration* (553-3001-332).

## 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

Table 11 lists the OAM CLI command groups. The commands in each group are described in the following sections.

**Table 11**
**OAM CLI command groups (Part 1 of 2)**

| Command group | Description | Commands |
|---|---|---|
| **DLOG** | Firmware download log file commands | Table 12 on page 190 |
| **GK** | Gatekeeper module commands | Table 13 on page 190 |
| **Network** | Remote access commands | Table 14 on page 192 |
| **RID** | Remote iset diagnostics commands | Table 15 on page 193 |
| **UFTP** | UFTP IP Phone firmware download commands. | Table 16 on page 194 |
| **cds** | Converged Desktop Service module commands | Table 17 on page 195 |
| **election** | Election module commands | Table 18 on page 196 |
| **elm** | ELM module commands | Table 19 on page 196 |
| **iset** | iset module commands | Table 20 on page 197 |

**Table 11**
**OAM CLI command groups (Part 2 of 2)**

| Command group | Description | Commands |
|---|---|---|
| **mam** | MAM module commands | Table 21 on page 199 |
| **ncs** | Network Connection Service module commands | Table 22 on page 203 |
| **npm** | Network Protocol Module commands | Table 23 on page 204 |
| **nrsDB** | Network Routing Service commands | Table 24 on page 205 |
| **nrsomm** | Network Routing Service operational measurement commands | Table 25 on page 207 |
| **pbxlink** | PBX link commands | Table 26 on page 207 |
| **securityShell** | Security shell commands | Table 27 on page 208 |
| **sipnpm** | SIP Network Protocol Module commands | Table 28 on page 209 |
| **system** | System administration commands | Table 29 on page 210 |
| **tps** | TPS module commands | Table 30 on page 212 |
| **trace** | General trace tools | Table 31 on page 213 |
| **uipc** | Universal ISDN module commands | Table 32 on page 215 |
| **ums** | UMS module commands | Table 33 on page 215 |
| **usi** | RUDP timeout and retry commands | Table 34 on page 217 |
| **vte** | Virtual Terminal Emulator commands | Table 35 on page 217 |
| **vtrk** | Virtual Trunk module commands | Table 36 on page 218 |

## DLOG commands — Firmware download log file

Table 12 lists the OAM firmware download log file commands in the DLOG command group.

**Table 12**
**OAM DLOG commands**

| Command | Description | Element Manager |
|---|---|---|
| **activeDlogShow** | Displays the current used firmware download file. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **inactiveDlogShow** | Displays the inactive firmware download log file. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **dnldFailShow** | Displays failed results in the active firmware download log file. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

## GK commands — Gatekeeper

Table 13 lists the OAM Gatekeeper commands in the GK command group.

**Table 13**
**OAM GK commands (Part 1 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **gkDiscoveryTrace** | Traces Gatekeeper discovery messages for a specified endpoint. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **gkRegTrace** | Traces endpoint registration messages and unregistration messages for a specified endpoint. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |

**Table 13**
**OAM GK commands (Part 2 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **gkCallTrace** | Traces endpoint call-associated messages (admission, bandwidth, disengage, and location messages). See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **gkProtocolTrace** | Traces any message for any message type. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **gkTraceOff** | Turns off the trace for the specified endpoint for all protocol types. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **gkTraceOutput** | Sets the output destination for all Gatekeeper protocol traces. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **gkTraceSettings** | Displays the trace output destination as well as the endpoint types being traced. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **gkTraceTblClear** | Clears the calling/called number table associated with the NUM trace filter(s). See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **gkTraceTblShow** | Displays the calling/called number table associated with the NUM trace filter(s). See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |

## Network commands — remote access

Table 14 lists the OAM remote access commands in the Network command group.

**Table 14**
**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.<br>Where:<br>• server = IP address<br>• username = host name | N/A |
| **rlogin [server] [-l username]** | Remotely logs in to a server. The address can be either an IP address or host name.<br>Where:<br>• server = IP address<br>• username = host name | N/A |
| **cslogin** | Logs in to the Call Server overlays. | N/A |

## RID commands — remote iset diagnostics

Table 15 lists the OAM remote iset diagnostic commands in the RID command group.

**Table 15**
**OAM RID commands**

| Command | Description | Element Manager |
|---|---|---|
| **rPing** | Pings an IP address. See *Converging the Data Network with VoIP* (553-3001-160). | QoS |
| **rPingStop** | Stops pinging an IP address. See *Converging the Data Network with VoIP* (553-3001-160). | N/A |
| **rTraceRoute** | Traces the route of an IP address. See *Converging the Data Network with VoIP* (553-3001-160). | QoS |
| **rTraceRouteStop** | Stops tracing the route of an IP address. See *Converging the Data Network with VoIP* (553-3001-160). | N/A |
| **RUDPStatShow** | Displays RUDP/UNIStim statistics for an IP Phone. See *Converging the Data Network with VoIP* (553-3001-160). | N/A |
| **eStatShow** | Displays Ethernet statistics for an IP Phone. See *Converging the Data Network with VoIP* (553-3001-160). | N/A |
| **isetInfoShow** | Displays DHCP configurations and iset information for an IP Phone. See *Converging the Data Network with VoIP* (553-3001-160). | QoS |

## UFTP commands — UFTP IP Phone firmware download

Table 16 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: Description, Installation, and Operation* (553-3001-365).

**Table 16**
**OAM UFTP commands (Part 1 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **uftpShow** | Displays IP Phone firmware download information. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **uftpNodeShow** | Displays IP Phone firmware download summary for the node. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **uftpRunTimeDataReset** | Resets the run time data field in the UFTP data block. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **uftpTurboMode** | Configures maintenance mode. See *IP Line: Description, Installation, and Operation* (553-3001-365). | Uftp |
| **uftpTurboModeTimeoutSet** | Configures the idle timeout timer for maintenance mode. See *IP Line: Description, Installation, and Operation* (553-3001-365). | Uftp |

**Table 16**
**OAM UFTP commands (Part 2 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **uftpTurboModeShow** | Displays current status of maintenance mode. See *IP Line: Description, Installation, and Operation* (553-3001-365). | 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: Description, Installation, and Operation* (553-3001-365). | Uftp |

## cds commands — Converged Desktop Service Module

Table 17 lists the OAM Converged Desktop Service (CDS) commands in the cds command group.

**Table 17**
**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* (553-3001-521). | 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* (553-3001-521). | N/A |

## election commands — election module

Table 18 lists the OAM election module commands in the election command group.

**Table 18**
**OAM election commands**

| Command | Description | Element Manager |
|---|---|---|
| **electShow** | Displays the card TPS state, current master, and a list of online TPS. See *IP Line: Description, Installation, and Operation* (553-3001-365). | Election |

## elm commands — ELM module

Table 19 lists the OAM ELM module command in the elm command group.

**Table 19**
**OAM elm commands**

| Command | Description | Element Manager |
|---|---|---|
| **elmShow** | Displays a list of supported languages. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

## iset commands — iset module

Table 20 lists the OAM iset module commands in the iset command group.

**Table 20**
**OAM iset commands (Part 1 of 3)**

| Command | Description | Element Manager |
|---|---|---|
| **isetShow** | Displays general information for all registered IP Phones. See *IP Line: Description, Installation, and Operation* (553-3001-365). | Iset |
| **isetNATShow** | Displays information about registered telephones behind a NAT router. See *IP Line: Description, Installation, and Operation* (553-3001-365). | Iset |
| **isetShowByTN** | Displays general information for all registered IP Phones, sorted by TN. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **isetShowByIP** | Displays general information for all registered IP Phones, sorted by IP. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **isetReset** | Resets the registered IP Phone. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **isetResetAll** | Resets all registered IP Phones. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **isetCount** | Displays total number of registered IP Phones. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **isetGet** | Displays a list of IP Phones based on a specified query. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

**Table 20**
**OAM iset commands (Part 2 of 3)**

| Command | Description | Element Manager |
|---|---|---|
| **itgPLThreshold** | Sets the IP Phone 2004 telephone and gateway alarm packet threshold (in units of 0.1%). See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **nodePwdSet** | Sets the password for the current node. See *IP Line: Description, Installation, and Operation* (553-3001-365). | NodePwd |
| **nodePwdShow** | Displays the settings for the node password. See *IP Line: Description, Installation, and Operation* (553-3001-365). | NodePwd |
| **nodePwdEnable** | Enables the node password setting. See *IP Line: Description, Installation, and Operation* (553-3001-365). | NodePwd |
| **nodePwdDisable** | Disables the node password settings. See *IP Line: Description, Installation, and Operation* (553-3001-365). | NodePwd |
| **nodeTempPwdSet** | Sets the temporary password for the current node. See *IP Line: Description, Installation, and Operation* (553-3001-365). | NodePwd |
| **nodeTempPwdClear** | Clears the temporary password for the current node. See *IP Line: Description, Installation, and Operation* (553-3001-365). | NodePwd |
| **clearLockout** | Clears the Branch User Config lockout. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **isetFWShow** | Displays the status of the firmware for IP Phones. See *IP Line: Description, Installation, and Operation* (553-3001-365). | Iset |

**Table 20**
**OAM iset commands (Part 3 of 3)**

| Command | Description | Element Manager |
|---|---|---|
| **isetFWGet** | Filters the output of the isetFWShow command by one of that command's output field names. See *IP Line: Description, Installation, and Operation* (553-3001-365). | Iset |

## mam commands — MAM module

Table 21 lists the OAM MAM module commands in the mam command group.

**Table 21**
**OAM mam commands (Part 1 of 4)**

| Command | Description | Element Manager |
|---|---|---|
| **firmwareVersionShow** | Displays firmware version number. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **IPInfoShow** | Displays IP address information. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) and *IP Line: Description, Installation, and Operation* (553-3001-365). | Mam |
| **itgCardShow** | Displays Voice Gateway Media Card information. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | Mam |
| **itgMemShow** | Displays memory usage. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

**Table 21**
**OAM mam commands (Part 2 of 4)**

| Command | Description | Element Manager |
|---|---|---|
| **resetOM** | Resets the operational measurement file timer. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **bootPFileGet** | Sends an updated bootptab file from the MAT to the ITG. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **bootPFilePut** | Sends the bootptab file to the specified host. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **configFileGet** | Sends an undated config.ini file from the MAT to the ITG. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **omFilePut** | Sends the current OM file to the specified host. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **currOMFilePut** | Sends the current OM file to the specified host. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **prevOMFilePut** | Sends the previous OM file to the specified host. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

**Table 21**
**OAM mam commands (Part 3 of 4)**

| Command | Description | Element Manager |
|---|---|---|
| **hostFileGet** | Transfers any file from the MAT to the ITG. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **hostFilePut** | Transfers any file from the ITG to the specified host. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **swDownload** | Loads new version of software from the FTP host to the ITG card. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **itgAlarmTest** | Generates **ITGxxxx** test alarms. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **itgPLThreshold** | Sets the IP Phone 2004 telephone and gateway alarm packet threshold (in units of 0.1%). See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **disiAll** | Gracefully disables the LTPS and voice gateway. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **enaAll** | Enables the LTPS and voice gateway. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

**Table 21**
**OAM mam commands (Part 4 of 4)**

| Command | Description | Element Manager |
|---|---|---|
| **disServices** | Gracefully switches the registered resources to the other services. See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | Mam |
| **forcedisServices** | Forces the server to switch the registered resources to the other services in the same node. See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | Mam |
| **enlServices** | Enables all services to accept registration of resources. See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | Mam |
| **servicesStatusShow** | Displays the status of services. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | 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 Configuration* (553-3001-213). | N/A |
| **lossPlanPrt** | Displays the offsets and current values for the handset, headset, and handsfree RLR and SLR. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

## ncs commands — Network Connection Service module

Table 22 lists the OAM Network Connection Service (NCS) module commands in the ncs command group.

**Table 22**
**OAM ncs commands (Part 1 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **tpsARTrace** | Enables tracing for the Network Connection Server (NCS). See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **tpsARTraceOff** | Disables tracing for the Network Connection Server (NCS). See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **tpsARTraceAllOff** | Turns off the trace for all tpsAR trace identifiers. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **tpsAROutput** | Modifies the destination for the traced output of the NCS. See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **tpsARTraceSettings** | Displays the trace settings and items being traced for the NCS trace. See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

**Table 22**
**OAM ncs commands (Part 2 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **tpsARTraceHelp** | Displays help on the tpsARTrace commands. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |

## npm commands — Network Protocol Module

Table 23 lists the OAM Network Protocol Module (NPM) commands in the npm command group.

**Table 23**
**OAM npm commands**

| Command | Description | Element Manager |
|---|---|---|
| **H323CallTrace** | Traces H.323 incoming and outgoing call setup messages for selected channels. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **H323TraceShow** | Displays input and output display settings for **H323CallTrace** and **H323Output** commands. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **H323Output** | Directs H323Trace output to TTY or syslog file. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **H323GwShow** | Displays information about the H.323 Network Protocol Module. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |

## nrsDB commands — Network Routing Service

Table 24 lists the OAM Network Routing Service (NRS) commands in the nrsDB command group.

**Table 24**
**OAM nrsDB commands (Part 1 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **nrsGWEndpointShow** | Lists all the endpoints in the database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsUserEPShow** | Lists all the NRS users with corresponding IP addresses. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsCollaboratingServerShow** | Lists all the Collaborating Servers in the database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsL0DomainShow** | Lists all the Level 0 domains in the database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsL1DomainShow** | Lists all the Level 1 domains in the database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsRoutingEntryShow** | Lists all the Routing Entries in the database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsServiceDomainShow** | Lists all the Service Domains in the database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |

**Table 24**
**OAM nrsDB commands (Part 2 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **nrsCollaboratingServerQuery** | | N/A |
| | Queries one Collaborating Server from the database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | |
| **nrsGWEndpointQuery** | Queries one Endpoint from the database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsUserEPQuery** | Queries an NRS endpoint with IP and protocol information. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsL0DomainQuery** | Queries one L 0 Domain from the database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsL1DomainQuery** | Queries one L 1 Domain from the database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsServiceDomainQuery** | Queries one Service Domain from the database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsDefaultRouteQuery** | Displays all the default routes which belong to an endpoint in the database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsDBShow** | DIsplays the state of the Primary and Alternate NRS database, and the local NRS database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |

## nrsomm commands — NRS operational measurements

Table 25 lists the OAM NRS operational measurements commands in the nrsomm command group.

**Table 25**
**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 Configuration* (553-3001-213). | 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 Configuration* (553-3001-213). | N/A |

## pbxlink commands — PBX link

Table 26 lists the OAM PBX link commands in the pbxlink command group.

**Table 26**
**OAM pbxlink commands**

| Command | Description | Element Manager |
|---|---|---|
| **pbxLinkShow** | Displays PBX link status. See *IP Line: Description, Installation, and Operation* (553-3001-365). | pbxLink |

## securityShell commands — Security shell

Table 27 lists the OAM Security shell commands in the securityShell command group.

**Table 27**
**OAM securityShell commands**

| Command | Description | Element Manager |
|---|---|---|
| **disInsecureShells** | Disables all insecure shells in the system, including TELNET and RLOGIN sessions. See *System Security Management* (553-3001-302). | See Note. |
| **enlInsecureShells** | Enables all insecure shells in the system, including TELNET and RLOGIN sessions. See *System Security Management* (553-3001-302). | See Note. |
| **statInsecureShells** | Displays whether insecure shell access is enabled or disabled. See *System Security Management* (553-3001-302). | See Note. |

***Note:*** These commands are not accessible from Element Manager as described in "Element Manager" on page 185. They are available in Element Manager at **Services > Security > Shell Login Options**. Refer to *System Security Management* (553-3001-302) for more information.

## sipnpm commands — SIP Network Protocol Module

Table 28 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 Configuration* (553-3001-213). | Sip |
| **SIPCallTrace** | Traces messages sent through SIP channels. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **SIPTraceShow** | Displays the SIP trace settings and all active traces for the SIP call trace tool. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **SIPOutput** | Specifies where the output for the trace tool is to be directed. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **SIPTraceLevel** | Sets the SIPCallTrace output to Summary or Detailed format. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |

## system commands — system administration commands

Table 29 lists the OAM system administration commands in the system command group.

**Table 29**
**OAM system commands (Part 1 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **routeShow** | Displays host and network routing tables. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | System |
| **routeAdd** | Adds a route to the routing tables. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **routeDelete** | Deletes a route from the routing tables. See *IP Trunk: Description, Installation, and Operation* (553-3001-363). | N/A |
| **ping** | Tests that a remote site is reachable. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | 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 |
| **swVersionShow** | Displays software version. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

**Table 29**
**OAM system commands (Part 2 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **date** | Displays the system date and time, and prompts to set new system data and time. | N/A |
| **uptime** | Displays the amount of time lapsed since the last system reboot. | N/A |
| **stty [speed]** | Sets console speed.<br>Available speeds are 9600, 19 200, 38 400, and 115 200. | N/A |
| **consoleShow** | Displays console speed. | N/A |
| **ppp [-l localAdd -r remoteAdd -o optionsFile -f]** | Initiates a PPP connection with options.<br>Where:<br>• localAdd is the local IP address. Default is 137.135.x.1.<br>• remoteAdd is the remote IP address. Default is 137.135.x.2.<br>• optionsFile is the full path to the options file.<br>• -f signifies no hardware flow control signals during PPP connection. | N/A |

## tps commands — TPS module

Table 30 lists the OAM TPS module commands in the tps command group.

**Table 30**
**OAM tps commands (Part 1 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **disiTPS** | Disables TPS service when idle. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **enaTPS** | Enables TPS service. See *IP Line: Description, Installation, and Operation* (553-3001-365). | 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 Configuration* (553-3001-213). | Tps |
| **forcedisTPS** | Forces all registered Line TPS to unregister from the local server. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | Tps |
| **enlTPS** | Causes Line TPS application to be enabled and to accept set registrations. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | 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 Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | Tps |
| **UKLossPlanSet** | Sets IP Phone's loss plan to UK-specific values. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

**Table 30**
**OAM tps commands (Part 2 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **lossPlanSet** | Adjusts the levels of a given transducer by the entered RLR and SLR offsets. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **UKLossPlanClr** | Sets IP Phone's loss plan to default values. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **lossPlanClr** | Sets IP Phone's loss plan to default values. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **echoServerShow** | Displays information about the Echo Servers used by this system. See *IP Line: Description, Installation, and Operation* (553-3001-365). | Tps |

## trace commands — General trace tools

Table 31 lists the OAM General trace tools in the trace command group.

**Table 31**
**OAM trace commands (Part 1 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **traceAllOff** | Disables the trace facilities from writing to the TTY, SYSLOG, and specified files. See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

**Table 31**
**OAM trace commands (Part 2 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **traceAllOn** | Enables the trace facilities to resume writing to the TTY, SYSLOG, and/or specified files. See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **tracePrintOff** | Disables the trace facilities from writing to the TTY. See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **tracePrintOn** | Enables the trace facilities to resume writing to the TTY. See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **traceFileOff** | Disables the trace facilities from writing to the SYSLOG and specified files. See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **traceFileOn** | Enables the trace facilities to resume writing to the SYSLOG and/or specified files. See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **traceShow** | Displays the names of active traces in the system. See *IP Peer Networking: Installation and Configuration* (553-3001-213) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

## uipc commands — Universal ISDN Protocol module

Table 32 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 Configuration* (553-3001-213) or *IP Trunk: Description, Installation, and Operation* (553-3001-363). | N/A |

## ums commands — UMS module

Table 33 lists the OAM UMS module commands in the ums command group.

**Table 33**
**OAM ums commands (Part 1 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **firmwareFileGet** | Initiates a firmware download from a specified FTP server. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **firmwareFileGetI2004** | Initiates a firmware download for an IP Phone 2004 from a specified FTP server. Replaced by **firmwareFileGet**. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **firmwareFileGetI2002** | Initiates a firmware download for an IP Phone 2002 from a specified FTP server. Replaced by **firmwareFileGet**. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

**Table 33**
**OAM ums commands (Part 2 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **umsPolicyShow** | Displays the current upgrade policy. See *IP Line: Description, Installation, and Operation* (553-3001-365). | Ums |
| **umsSetPolicy** | Assigns the policy for the particular firmware. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **umsSetPolicyRetries** | Sets the number of retries for the policy. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **umsSetPolicyProtocol** | Sets the protocol for the policy. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **umsCreatePolicy** | Creates a firmware policy. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **umsDeletePolicy** | Deletes a firmware policy. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **umsUpgradeAll** | Upgrades all registered sets according to policy and firmware file. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **umsUpgradeTimerShow** | Displays the upgrade schedule. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **umsUpgradeTimerCancel** | Cancels the scheduled upgrade. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

## usi commands — RUDP timeout and retry commands

Table 34 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: Description, Installation, and Operation* (553-3001-365). | N/A |
| **usiGetPhoneRudpRetries** | Displays the RUDP Max Retries count for IP Phones. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **usiSetPhoneRudpTimeout** | Sets the RUDP Timeout value (in ms) for IP Phones. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **usiGetPhoneRudpTimeout** | Displays the RUDP Timeout value (in ms) for IP Phones. See *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

## vte commands — Virtual Terminal Emulator

Table 35 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 “Unpacking Help files for Virtual Terminal Emulator” on page 92 or page 107. | N/A |

## vtrk commands — Virtual Trunk module

Table 36 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 Configuration* (553-3001-213). | Vtrk |
| **disVTRK** | Gracefully switches the registered Virtual Trunks to another Signaling Server in the same node. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | Vtrk |
| **forcedisVTRK** | Forces all registered Virtual Trunks to unregister from the local server. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | Vtrk |
| **enlVTRK** | Enables the Virtual Trunk application to accept Virtual Trunk registrations. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | Vtrk |

# 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>`**'.

## Command groups

Table 37 lists the CLI command groups which 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*** | Stand-alone NRS commands | Table 38 on page 220 |
| ***PDT*** | PDT built-in commands | Table 39 on page 221 |
| ***Patcher*** | Patch commands | Table 40 on page 221 |
| **RID** | Remote iset diagnostic commands | Table 41 on page 223 |
| ***cds*** | Converged Desktop Services module commands | Table 42 on page 224 |
| ***disk*** | File system maintenance and diagnostics. | Table 43 on page 225 |
| **nrsDB** | Network Routing Service commands | Table 44 on page 225 |
| ***rdtools*** | rd tools commands | Table 45 on page 227 |
| **sipnpm** | SIP Network Control Module commands | Table 46 on page 228 |
| **system** | System administration commands | Table 47 on page 230 |

## Accounts commands — stand-alone NRS user commands

Table 38 lists the commands for an NRS running on a stand-alone 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 stand-alone Signaling Server. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **adminUserCreate** | Creates an administrator-level user of an NRS running on a stand-alone Signaling Server. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **adminUserDelete** | Deletes an administrator-level user of an NRS running on a stand-alone Signaling Server. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **adminAccountShow** | Displays User ID and access privileges for all users of an NRS running on a stand-alone Signaling Server. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |

## PDT commands — PDT built-in

Table 39 lists the PDT built-in commands in the PDT command group.

**Table 39**
**PDT built-in commands**

| Command | Description | Element Manager |
|---|---|---|
| **vxshell** | Switches to VxWorks shell. Requires PDT2 password. | N/A |
| **vxWorksShell** | Switches to VxWorks shell. Requires PDT2 password. | N/A |

## Patcher commands — patching

Table 40 lists the patching commands in the Patcher command group.

**Table 40**
**PDT Patcher commands (Part 1 of 2)**

| Command | Description | Element Manager (see Note) |
|---|---|---|
| **pload** | Loads a patch into memory. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **pins** | Puts a patch in service. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **poos** | Takes a patch out of service. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

**Table 40**
**PDT Patcher commands (Part 2 of 2)**

| Command | Description | Element Manager (see Note) |
|---|---|---|
| **pout** | Removes a patch from memory. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **plis** | Displays details of a specific patch. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |
| **pstat** | Displays status of all active patches. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | PSTAT |
| **pnew** | Creates memory patches. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | N/A |

***Note:*** The Patcher commands are not available in Element Manager from the **Node Maintenance** web page. They are available from **IP Telephony > Software > Patching**

## RID commands — remote iset diagnostics

Table 41 lists the PDT remote iset diagnostic commands in the RID command group. These commands are in addition to the OAM commands listed in Table 15 on page 193.

**Table 41**
**PDT RID commands**

| Command | Description | Element Manager |
|---|---|---|
| **RTPStatShow** | Displays most recent Realtime Conferencing Protocol (RTCP) statistics, including r-value statistics. See *Converging the Data Network with VoIP* (553-3001-160). | QoS |
| **RTPTraceShow** | Periodically displays RTCP statistics for a given polling period, including r-value statistics. See *Converging the Data Network with VoIP* (553-3001-160). | N/A |
| **RTPTraceStop** | Cancels a previously issued RTPTraceShow command for an IP Phone. See *Converging the Data Network with VoIP* (553-3001-160). | N/A |

## cds commands — Converged Desktop Service module

Table 42 lists the PDT Converged Desktop Service (CDS) commands in the cds command group. These commands are in addition to the OAM commands listed in Table 17 on page 195.

**Table 42**
**PDT cds commands**

| Command | Description | Element Manager |
|---|---|---|
| **cdsAmlTrace** | Sets the Application Module Link (AML) trace level for the CDS application. See *CS 1000 to MCS 5100 Converged Desktop Type 2: Configuration Guide* (553-3001-521). | N/A |
| **cdsCallTraceSetAll** | Enables CDS call trace for all calls. See *CS 1000 to MCS 5100 Converged Desktop Type 2: Configuration Guide* (553-3001-521). | N/A |
| **cdsCallTraceOff** | Turns off CDS call trace for all calls. See *CS 1000 to MCS 5100 Converged Desktop Type 2: Configuration Guide* (553-3001-521). | N/A |
| **cdsCallTraceSetDn** | Sets CDS call trace for a particular calling-party or called-party DN. See *CS 1000 to MCS 5100 Converged Desktop Type 2: Configuration Guide* (553-3001-521). | N/A |

## disk commands — file system maintenance and diagnostics

Table 43 lists the PDT file system maintenance and diagnostic command in the disk command group.

**Table 43**
**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.<br>Where:<br>• m is the mount flag.<br>• devname is the device to check. | N/A |

## nrsDB commands — Network Routing Service

Table 44 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 24 on page 205.

**Table 44**
**PDT nrsDB commands (Part 1 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **nrsDbCutover** | Swaps the Active and Standby database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | See Note. |
| **nrsDbRevert** | Swaps the Active and Standby database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | See Note. |

**Table 44**
**PDT nrsDB commands (Part 2 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **nrsDbCommit** | Copies the table from the Active to the Standby database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | See Note. |
| **nrsDbRollback** | Copies the table from the Active to the Standby database. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | See Note. |
| **nrsDbCommitNow** | Performs the cutover and commits immediately. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | See Note. |
| **disNRS** | Gracefully disables the NRS server service. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **forcedisNRS** | Forces the NRS server out of service. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **enlNRS** | Enables the SIP Redirect Server service. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsSIPTestQuery** | Queries a SIP Routing Entry with DN and cost information. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **nrsGKTestQuery** | Queries an H.323 Routing Entry with DN and cost information. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |

***Note:*** The database cutover, revert, commit, and rollback commands are not available in Element Manager as described on “Element Manager” on page 185. The same functionality is available in NRS Manager at

**Tools > Database Actions**. See *IP Peer Networking: Installation and Configuration* (553-3001-213) for details.

## rdtools commands — rd tools

Table 45 lists the PDT rd tools commands in the rdtools command group.

**Table 45**
**PDT rdtools commands (Part 1 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **rdopen [filename]** | Opens a report log file.<br>Where [filename] is the name of the report file to be opened. | N/A |
| **rdgo [N]** | Goes to a specific record.<br>Where [N] is the absolute record number. | N/A |
| **rd [S] [R]** | Displays a specified number of records starting at a specified point.<br>Where:<br>• [S] is the number of steps to traverse to the starting point.<br>• [R] is the number of records to display.<br>Both [S] and [R] can be negative. | N/A |
| **rds [S] [R]** | Displays a specified number of records, with a symbolic dump, starting at a specified point.<br>Where:<br>• [S] is the number of steps to traverse to the starting point.<br>• [R] is the number of records to display.<br>Both [S] and [R] can be negative. | N/A |

**Table 45**
**PDT rdtools commands (Part 2 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **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.<br>Where [N] is the number of records to display. | N/A |
| **rdhead [N]** | Displays the specified number of oldest records.<br>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.<br>Where [filename] is the name of the log file to be converted. | N/A |

## sipnpm commands — SIP Network Protocol Module

Table 46 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 on page 209.

**Table 46**
**PDT sipnpm commands (Part 1 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **sip2IsdnSet** | Changes the SIP status code to the ISDN cause code mapping. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |

**Table 46**
**PDT sipnpm commands (Part 2 of 2)**

| Command | Description | Element Manager |
|---|---|---|
| **sip2IsdnReset** | Resets a single SIP status code to the default ISDN cause code mapping. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **sip2IsdnResetAll** | Resets all SIP status codes to the default ISDN cause code mappings. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **sip2IsdnShow** | Shows one specific SIP status code to ISDN cause code mapping. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **sip2IsdnShowAll** | Shows all mappings from SIP status code to ISDN cause code. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **isdn2SipSet** | Changes the ISDN cause code to the SIP status code mapping. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **isdn2SipReset** | Resets a single ISDN cause code to the default SIP status code mapping. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **isdn2SipResetAll** | Resets all the ISDN cause codes to the default SIP status code mappings. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **isdn2SipShow** | Shows one specific ISDN cause code to SIP status code mapping. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |
| **isdn2SipShowAll** | Shows all mappings from ISDN cause codes to SIP status codes. See *IP Peer Networking: Installation and Configuration* (553-3001-213). | N/A |

## system commands — System administration

Table 47 lists the PDT system administration commands in the system command group. These commands are in addition to the OAM commands listed in Table 29 on page 210.

**Table 47**
**PDT system commands (Part 1 of 3)**

| Command | Description | Element Manager |
|---|---|---|
| **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 I taskID]** | Displays task information for task specified by name or task ID.<br>Where:<br>• name is the task name.<br>• taskID is the task ID. | N/A |
| **i** | Displays task information. See *IP Line: Description, Installation, and Operation* (553-3001-365). | System |
| **version** | Displays vxWorks version, date of build, and other information. | N/A |
| **x [name]** | Executes a function.<br>Where name is the name of the function. | N/A |
| **ifShow** | Displays the attached network interfaces. See *IP Trunk: Description, Installation, and Operation* (553-3001-363) or *IP Line: Description, Installation, and Operation* (553-3001-365). | System |

**Table 47**
**PDT system commands (Part 2 of 3)**

| **Command** | **Description** | **Element Manager** |
|---|---|---|
| **reboot [-1]** | Warm restarts the system.<br>If -1 specified, cold restarts the system. | N/A |
| **ls [path]** | Displays the contents of a directory.<br>Where path is the path name of the directory.<br>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.<br>Where path is the path name of the directory.<br>If path is not specified, the contents of the current directory are specified. | N/A |
| **cd [path]** | Changes the default directory.<br>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.<br>Where:<br>• input is the name of the file to be copied from. If NULL, stdin is used.<br>• output is the name of the new or destination file to be copied to. If NULL, stdout is used. | N/A |

**Table 47**
**PDT system commands (Part 3 of 3)**

| Command | Description | Element Manager |
|---|---|---|
| **rename [file1 file2]** | Renames one file or moves one file to another.<br>Where:<br>• file1 is the file to be renamed or moved.<br>• file2 is the new or destination filename. | N/A |
| **remove [file]** | Removes a file.<br>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 I name level]** | | N/A |
| | Sets the log level for a task, given by task ID or task name.<br>Where:<br>• tid is the task ID.<br>• name is the task name.<br>• level is the log level in the range 0-7. | |
| **hwdShow** | Displays the status of the system hardware watchdog timer. | N/A |

# Maintenance

## Contents

This section contains information on the following topics:

## Introduction

This section explains how to use and maintain the Signaling Server and its software after installation. Some of the tasks included in this section are:

- using the Signaling Server tools menu
- setting the Signaling Server port speed
- replacing a faulty Signaling Server

## Connecting a maintenance terminal

A maintenance terminal is required for installation, configuration and maintenance of the Signaling Server.

To connect and configure a maintenance terminal for the Signaling Server, see Procedure 3 on page 51.

## Logging in to the Signaling Server

To access the Signaling Server from a maintenance terminal, you must log in to the vxWorks$^{TM}$ shell using Procedure 8 on page 93. From this shell, you can change the Signaling Server port speed (see Procedure 39 on page 239) and run the commands described in "Command Line Interface (CLI) commands" on page 183.

## Signaling Server tools menu

From the Tools Menu in the Signaling Server Install Tool, you can perform the following tasks:

- set the system time and date
- repartition and initialize the hard desk
- reset the Administrator login and password
- test the hard disk
- change the web server security flag
- initialize the unprotected partition (/u)
- clear the boot sector to allow reinstallation of the previous release (see "Reinstalling the previous release of software" on page 120)
- copy the IP configuration from a floppy to the hard disk (see "Copying an IP configuration from a floppy disk" on page 237)
- back up the IP configuration from the hard disk to a floppy (see "Backing up the IP configuration" on page 236)

**WARNING**

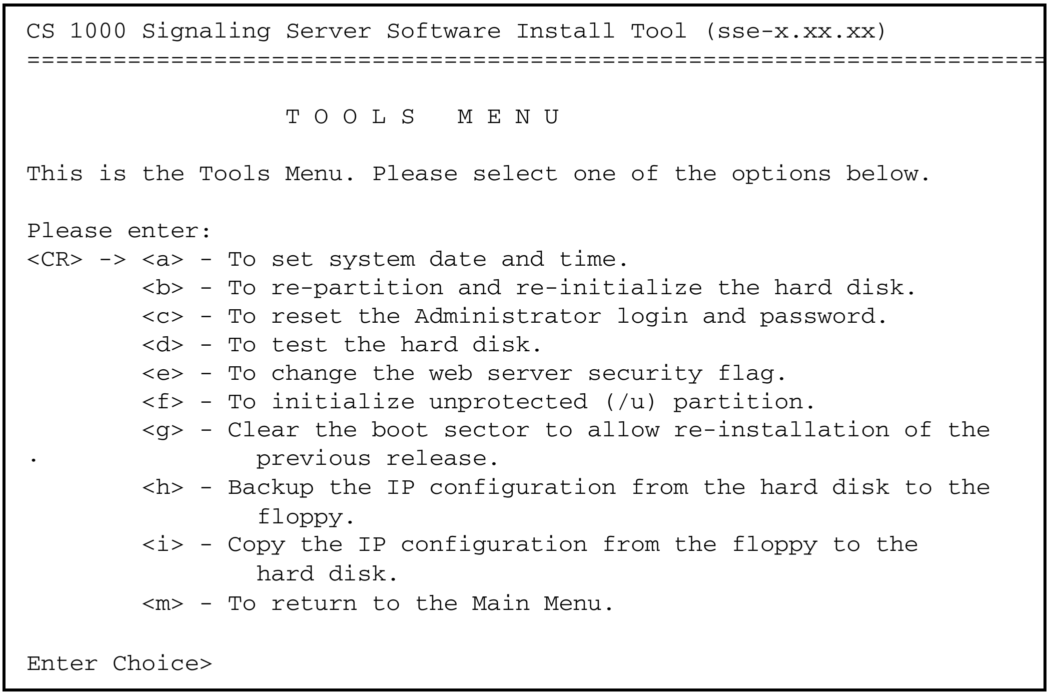
Option **f** ("To initialize unprotected (/u) partition") deletes the database, reports, and all other files and directories on partition **u**. Back up the database before selecting this option.

Use Procedure 36 to access the Signaling Server Tools Menu in the Signaling Server Install Tool.

**Procedure 36**
**Accessing the Signaling Server Tools Menu**

1 Enter **t** at the Install Tool **Main Menu** (Figure 26 on page 74) to access the **Tools Menu**, shown in Figure 106 on page 235.

**Figure 106**
**Tools menu**



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

                  T O O L S   M E N U

This is the Tools Menu. Please select one of the options below.

Please enter:
<CR> -> <a> - To set system date and time.
        <b> - To re-partition and re-initialize the hard disk.
        <c> - To reset the Administrator login and password.
        <d> - To test the hard disk.
        <e> - To change the web server security flag.
        <f> - To initialize unprotected (/u) partition.
        <g> - Clear the boot sector to allow re-installation of the
.               previous release.
        <h> - Backup the IP configuration from the hard disk to the
                floppy.
        <i> - Copy the IP configuration from the floppy to the
                hard disk.
        <m> - To return to the Main Menu.

Enter Choice>
```

2 Under the **Tools Menu**, you can enter:

- **a** to set the date and time (default).
- **b** to repartition and reinitialize the hard disk. This option results in a reboot. Leave the Signaling Server Software CD-ROM in the drive so

that the Install Tool can restart. Then, reinstall the Signaling Server software as described in Procedure 6 on page 66.

- **c** to reset the Administrator login and password.
- **d** to test the hard disk.
- **e** to change the web server security flag. See “Restricting web access to the ELAN subnet” on page 173.
- **f** to initialize the unprotected partition (/u).
- **g** to clear the boot sector before reinstalling the previous software release.
- **h** to back up the IP configuration from the hard drive to a floppy disk.
- **i** to copy the IP configuration from a floppy disk to the hard drive.
- **m** to return to the Main Menu.

**WARNING**

Option **f** deletes the database, reports, and all other files and directories on partition **u/**. Back up the database before selecting this option.

**End of Procedure**

# Backing up and restoring the IP configuration

The IP configuration on a Signaling Server can be backed up to a floppy disk, and subsequently restored.

## Backing up the IP configuration

The existing IP configuration can be backed up during the upgrade.

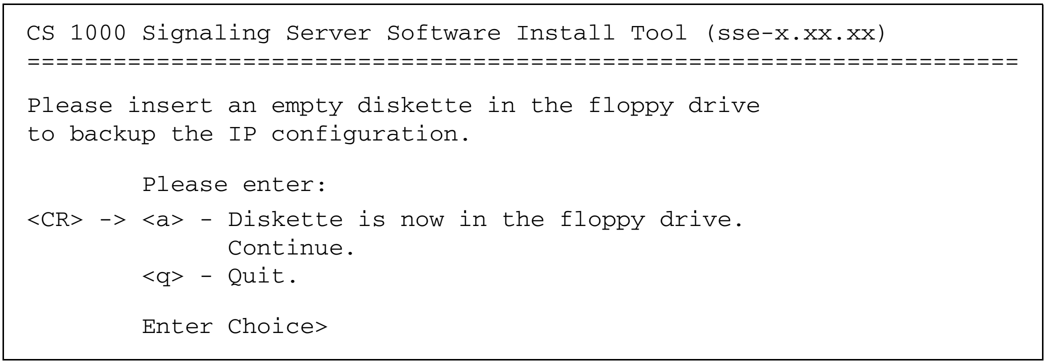
> ***Note:*** If you are upgrading from CS 1000 Release 4.0, you can back up your existing IP configuration during the upgrade, and then restore it after the upgrade is complete. This saves you the time and effort of having to manually reconfigure your IP configuration on the upgraded system. You can perform the backup during the upgrade procedure (see Procedure 11 on page 98).

Follow the steps in Procedure 37 to back up your IP configuration.

**Procedure 37**
**Backing up your existing IP configuration**

1. Enter **t** at the Install Tool **Main Menu** (Figure 26 on page 74) to access the **Tools Menu**, shown in Figure 106 on page 235.
2. Enter **h** to back up the IP configuration from the hard disk to a floppy disk.
3. Insert a floppy disk in the drive, and enter **a** at the menu shown in Figure 107.

**Figure 107**
**Copy IP configuration**



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

Please insert an empty diskette in the floppy drive
to backup the IP configuration.

        Please enter:
<CR> -> <a> - Diskette is now in the floppy drive.
              Continue.
        <q> - Quit.

        Enter Choice>
```

When the backup is complete, the system displays the following message:

```
Done copying IP configuration to floppy
```

**End of Procedure**

## Copying an IP configuration from a floppy disk

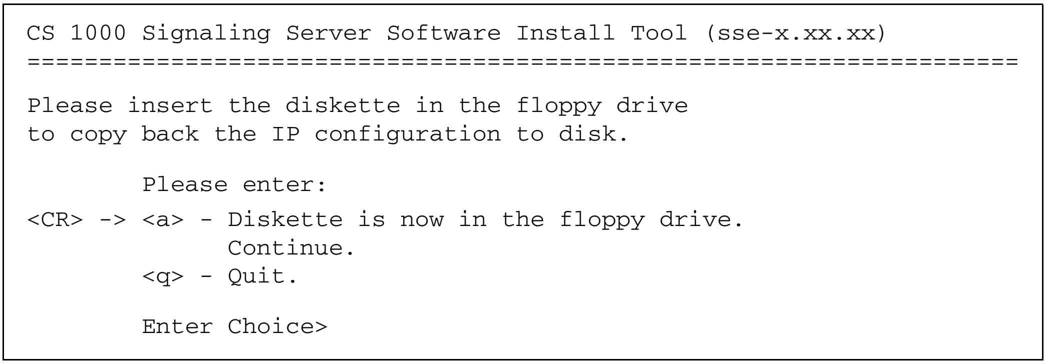
To copy (restore) an IP configuration from a floppy disk created during an upgrade, follow the steps in Procedure 38 on page 238.

**Procedure 38**
**Copying an IP configuration from a floppy disk**

You cannot restore the IP configuration from the Tools Menu before the upgrade is complete, and all files have been copied from the Install Tool CD to the hard disk.

1. Enter **t** at the Install Tool **Main Menu** (Figure 26 on page 74) to access the **Tools Menu**, shown in Figure 106 on page 235.
2. Enter **i** to copy the IP configuration from a floppy disk to the hard disk.
3. Insert the floppy disk in the drive, and enter **a** at the menu shown in Figure 108.

**Figure 108**
**Restore IP configuration**



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

Please insert the diskette in the floppy drive
to copy back the IP configuration to disk.

        Please enter:
<CR> -> <a> - Diskette is now in the floppy drive.
              Continue.
        <q> - Quit.

        Enter Choice>
```

When the backup is complete, the system displays the following message:

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

**End of Procedure**

# Setting the Signaling Server port speed

Administrators can change the port speed of the Signaling Server for a maintenance terminal connection.

**Procedure 39**
**Changing the Signaling Server port speed**

1 Log in to the Signaling Server. See Procedure 8 on page 93.

2 Enter **`stty 9600`** to change the port speed to 9600 baud.

*Note:* Acceptable values for the maintenance port speed are 9600, 38 400 and 115 200.

3 Change the port speed on the terminal, terminal emulator, or PC (which 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 out of the CLI.

**End of Procedure**

## Replacing a defective Signaling Server

*Note:* The Signaling Server is not a user-serviceable device. Any defective units should be returned to the supplier.

**WARNING**

Before replacing a defective Signaling Server, back up the IP Telephony node database files. Use the EDD command in LD 43 or use Element Manager (refer to "Backing up IP Telephony node configuration files" on page 181).

**Procedure 40**
**Replacing a defective Signaling Server:**

1 Remove the defective Signaling Server.

a. Turn off the power to the defective unit.

b. Disconnect all cables from the unit, including the power cord.

c. Loosen the screws through the faceplate of the Signaling Server to the rack-mount bracket, and slide the unit out of the rack.

2 Install the new Signaling Server hardware. Refer to the procedures in "Hardware installation" on page 41.

3 Transfer the IP Telephony node information to the new Signaling Server.

- If the defective Signaling Server was a Leader Signaling Server:

  **i.** Install the Signaling Server software on the new Signaling Server and configure it as a Leader Signaling Server. Refer to the procedures in "Software installation and configuration" on page 65.

  Configure a temporary IP Telephony node, using the same IP addresses as those for the old Signaling Server.

  **ii.** Boot the new Signaling Server and access Element Manager.

  **iii.** Choose **Configuration > IP Telephony**.

  **iv.** Choose **Node Summary**.

  **v.** Click **Edit**.

  ***Note:*** The information that is being edited is the node configuration that resides on the Call Server, not the Signaling Server.

  **vi.** Choose **Signaling Servers**, and choose the Signaling Server being replaced.

  **vii.** Enter the MAC address of the new Signaling Server in the **Management LAN (ELAN) MAC address** field.

  **viii.** Click **Save and Transfer** to transfer the node information to the new Signaling Server.

  **ix.** Reboot the new Leader Signaling Server.

- If the defective Signaling Server was a Follower Signaling Server:

  **i.** Log in to Element Manager from the Leader Signaling Server.

  **ii.** Choose **Configuration > IP Telephony**.

  **iii.** Choose **Node Summary**.

  **iv.** Click **Edit**.

  **v.** Enter the MAC address of the new Signaling Server in the **Management LAN (ELAN) MAC address** field.

**vi.** Click **Save and Transfer** to save the MAC address of the new Follower Signaling Server in Element Manager on the associated Leader Signaling Server.

**vii.** Install the Signaling Server software on the new Signaling Server, and configure it as a Follower Signaling Server. Refer to the procedures in "Software installation and configuration" on page 65.

**viii.** Reboot the new Signaling Server and access Element Manager again.

**ix.** Choose **Configuration** > **IP Telephony**.

**x.** Choose **Node Summary**.

**xi.** Click **Edit**.

**xii.** Click **Save and Transfer** to transfer the node information to the new Signaling Server.

**xiii.** Reboot the new Follower Signaling Server.

- If you are replacing a stand-alone Signaling Server:

  **i.** Install the Signaling Server software on the new Signaling Server, and configure it as a stand-alone Signaling Server. Refer to the procedures in "Software installation and configuration" on page 65.

  **ii.** Restore the NRS database using NRS Manager. Refer to *IP Peer Networking: Installation and Configuration* (553-3001-213) for instructions.

**End of Procedure**

# Appendix A: Upgrading memory

## Contents

This section contains information on the following topics:

## Introduction

For capacity reasons, the memory on the Signaling Server has been increased from 256 Mbytes to 512 Mbytes. 256 Mbytes is more than sufficient for Succession 1000 Release 1.0 and 2.0 systems in smaller environments (less than 1000 IP Phones).

However, for CS 1000 Release 4.0 and higher, all Signaling Servers must be equipped with at least 512 MBytes of memory. In some cases, 1 GByte may be required (see “Upgrading the Signaling Server memory” on page 59).

To enable customers to redeploy their current NTDU27AA 01, 02, or 03 Signaling Servers into a CS 1000 Release 4.0 or higher environment, a Signaling Server Memory Upgrade Kit (NTDU80) is available. This section explains how to upgrade the memory using this kit. The procedure is the same whether installing one NTDU80 Upgrade Kit to provision 512 MBytes or two NTDU80 Upgrade Kits to provision 1 GByte. The procedure can also be used to extend an NTDU27AA Signaling Server later than Succession 3.0 to 1 GByte of memory (which requires two NTDU80 Upgrade Kits).

***Note:*** These instructions are intended for qualified technical personnel with experience installing and configuring servers.

## Preparation

Read the following warnings carefully before beginning the upgrade process.

**DANGER OF ELECTRIC SHOCK**

SYSTEM POWER ON/OFF: The Power button on the front panel of the Signaling Server DOES NOT remove AC power to the Signaling Server system. Some circuitry in the Signaling Server may 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 OF ELECTRIC SHOCK**

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 should be done by technically qualified personnel.

### DANGER OF ELECTRIC SHOCK

HAZARDOUS CONDITIONS, DEVICES, AND CABLES: Hazardous electrical conditions may 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 WITH ESDS DEVICES

ELECTROSTATIC DISCHARGE (ESD) AND ESD PROTECTION: Since the 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 Signaling Server.
- Touch the metal on the Signaling Server before touching the other components.
- Keep part of your body in contact with the metal Signaling Server to dissipate the static charge while handling the components.
- Avoid moving around unnecessarily.
- Hold the Signaling Server components (especially boards) only by the edges.
- Place the 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 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.

## Upgrading the memory

To upgrade the memory of the Signaling Server, perform the following:

1. Remove the cover of the Signaling Server.
2. Remove the existing DIMM boards.
3. Insert the new DIMM boards.
4. Replace the cover on the Signaling Server.

These steps are described in Procedure 41.

**Procedure 41**
**Upgrading the Signaling Server memory**

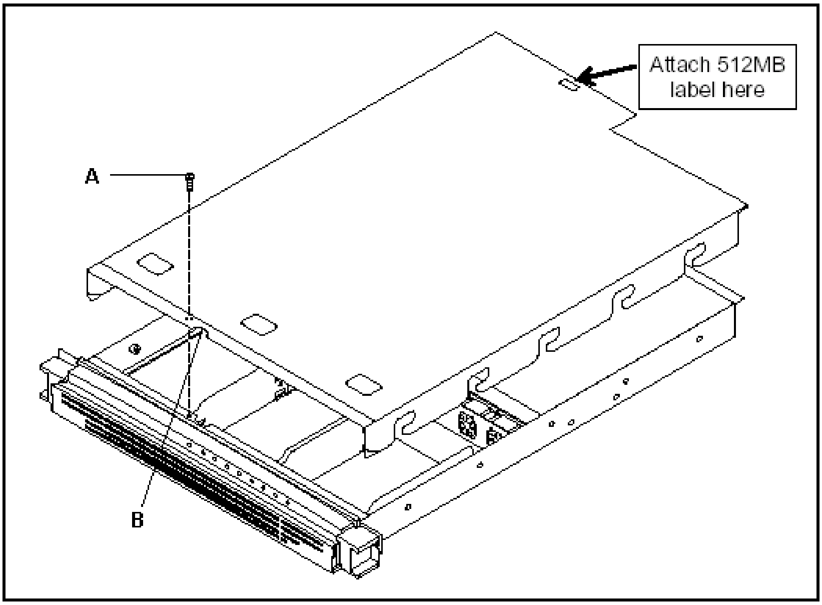
1. Remove the cover from the Signaling Server. Refer to Figure 109 on page 247.

   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 Signaling Server front panel.

   c. Grasp the notch (B) in the front center of the cover and lift up to remove the cover.

**Figure 109**
**Removing/replacing the cover on the Signaling Server**



2 Remove the 128 Mbyte DIMM boards from the Signaling Server. Refer to Figure 110 on page 248.

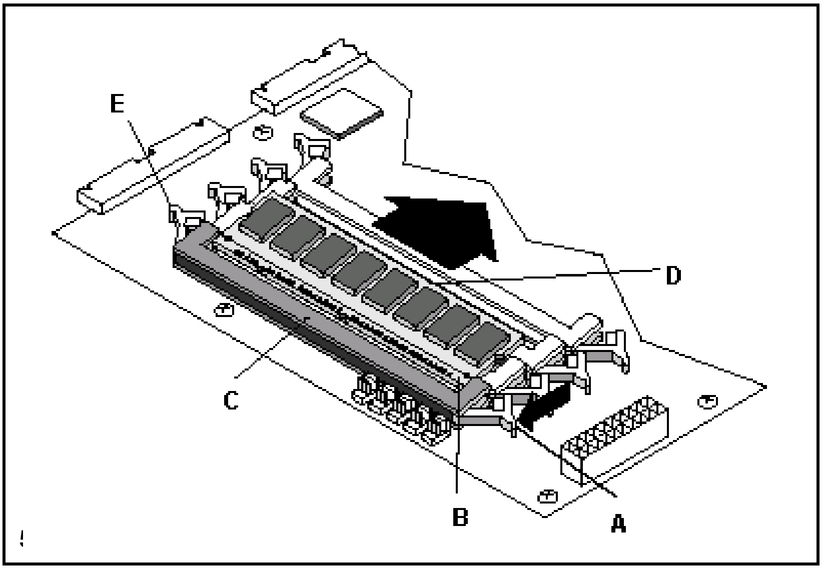
> **CAUTION**
> Hold the tips of your fingers lightly on the back edge (D) of the DIMM board to prevent the board from suddenly ejecting from the socket (C). The DIMM board or other components on the Signaling Server board could be damaged if the DIMM board is allowed to suddenly eject from the socket.

***Note:*** Remove all of the original 128 Mbyte DIMM boards.

**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).

**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.

**Figure 110**
**Removing a 128 Mbyte DIMM board**



**3** Install the new 512 Mbyte DIMM boards in the Signaling Server. Refer to Figure 111 on page 250.

> **CAUTION**
> Use extreme care when installing a DIMM board. Applying too much pressure or misaligning 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 Signaling Server board and move toward the front of the Signaling Server board.

***Note 1:*** Use only DIMM boards contained in the NTDU80 Signaling Server Memory Upgrade Kit. Nortel does not recommend the use of other memory modules.

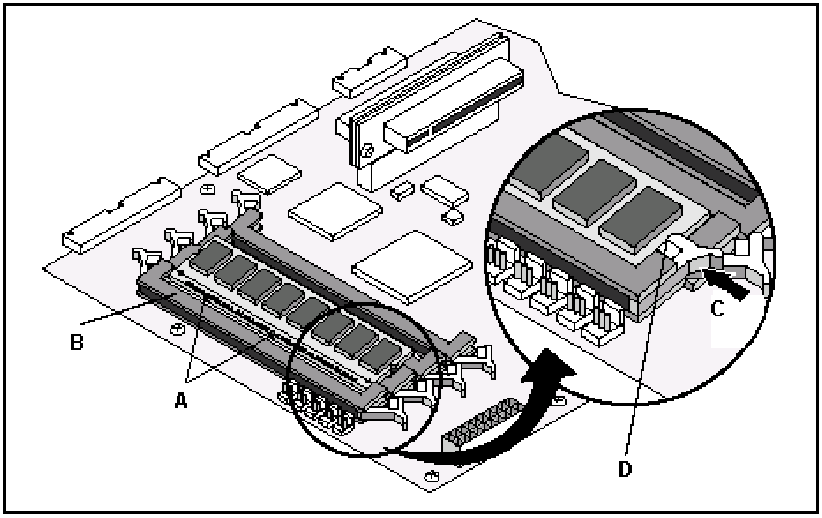
***Note 2:*** Do not mix the new 512 Mbyte DIMM boards with the original 128 Mbyte DIMM boards. Make sure that all the original boards have been removed during step 2 on page 247.

**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.)

**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.

**Figure 111**
**Installing a 512 Mbyte DIMM board**



4 Replace the cover on the Signaling Server. Refer to Figure 109 on page 247.

a. Position the cover on the 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 Signaling Server front panel.

c. Use a Phillips screwdriver and the screw (A) removed in step 1 on page 246 to securely attach the cover to the Signaling Server.

d. Attach the memory label (reading “512MB”) to the back edge of the cover.

**End of Procedure**

# Verifying a successful memory upgrade

Use Procedure 42 to ensure that the memory upgrade was successful.

**Procedure 42**
**Verifying a successful memory upgrade**

> ***Note:*** When upgrading to 1 GByte, the system responses indicate "1 GB" or "1024 MB" 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 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 Signaling Server.

**4** Press the power switch, the left-most button on the front of the Signaling Server.

The following should 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
512MB OK

Hit <F2> if you want to run SETUP
```

**5** <Optional> To do a more detailed memory 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 Signaling Server reboots and performs a more detailed memory test at boot time.

If "512MB OK" appears on the screen, the memory upgrade has been successful. If not, the memory upgrade has failed.

6 Power off the Signaling Server by depressing the Power button for seven seconds.

7 Disconnect the power cable.

**End of Procedure**

# List of terms

### ELAN subnet

Embedded Local Area Network subnet. This isolated subnet 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 videoconferencing applications. Although most videoconferencing vendors have announced that their products conform to H.323, it is too early to say whether such adherence actually results in interoperability.

### 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 which 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 Configuration

Publication number: 553-3001-212
Document release: Standard 10.00
Date: March 2007
Produced in Canada

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