Nortel Communication Server 1000

Communication Server 1000E SIP Line Service for Release 5.5

Release: 5.5
Document Revision: 01.01

www.nortel.com

NN43041-320

Nortel Communication Server 1000
Release: 5.5
Publication: NN43041-320
Document release date: 3 December 2008

Printed in Canada
LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Contents

New in this release

The following sections detail what's new in *Communication Server 1000E SIP Line Service for Release 5.5* (NN43041-320).

This document is new for Nortel Communication Server 1000 (CS 1000) Release 5.5, and describes the SIP Line service, which provides SIP Phone support in CS 1000 Release 5.5

Features

See the following sections for information about feature changes:

- No new features are introduced as part of SIP Line Service for CS 1000 Release 5.5.

Other changes

This section describes the detailed history of past releases of this document.

Revision History

December 2008	Standard 01.01 This document is issued to support Communication Server 1000 (CS 1000) Release 5.5.

Introduction

This document introduces the Session Initiation Protocol (SIP) Line Service on Nortel Communication Server 1000E Release 5.5. By installing the servers, applying patches, and making the configuration changes described in this document, you can enable SIP Lines on your CS 1000 Release 5.5 system.

This document describes steps you must follow to install the dedicated servers required to support SIP Lines, and various configuration changes you must make on the call server and on the phones. Once you have configured SIP Lines support, CS 1000 Release 5.5 can support a variety of Nortel SIP phones and third-party SIP phones.

If you have an existing Communication Server 1000E system, see the instructions in *Communication Server 1000E Software Upgrades* (NN43041-458), and *Communication Server 1000 Fault Management - SNMP* (NN43001-719).

Fundamentals

This chapter explains the concepts that you must understand to implement Session Initiation Protocol (SIP) Line on Communication Server 1000E Release 5.5.

ATTENTION
Before you configure or use SIP Line:

- You must have a Communication Server 1000E Release 5.5 system with CPPM call processor.
- If you have an existing Communication Server 1000E system, you must upgrade it to CS 1000 Release 5.5. For more information, see the instructions in *Communication Server 1000E Software Upgrades* (NN43041-458) before you carry out the configuration steps described in this NTP.
- You must have the following core software licensing for SIP Universal Extension (UEXT):
  - SIPN UEXT license
    - Order code NTE906NB (Enhanced)
    - Order code NTE907LB (Premium)
  - SIP3 UEXT license
    - Order code NTE906PB (Enhanced)
    - Order code NTE907MB (Premium)
- SIP Line requires dedicated Core 1U COTS servers to support SIP Gateway (VxWorks) and SIP Proxy Server (Linux base). The following servers are supported:
  - IBM X306M 1U COTS server (Order code NTDU99AAE5).
  - HP DL320G4 1U COTS server (Order code NTDU97AAE5).

Deployment model

To support SIP clients on CS 1000 Release 5.5, you must create two dedicated servers: one must be a dedicated SIP Gateway server, and the other a dedicated SIP Proxy Server. To allow controlled patching,

dedicated servers are required, as shown in Figure 1 "CS 1000 Release 5.5 SIP Line solution hardware view" (page 12) and Figure 2 "SIP Line solution network architecture and example dialing plan" (page 13).

Figure 1
CS 1000 Release 5.5 SIP Line solution hardware view

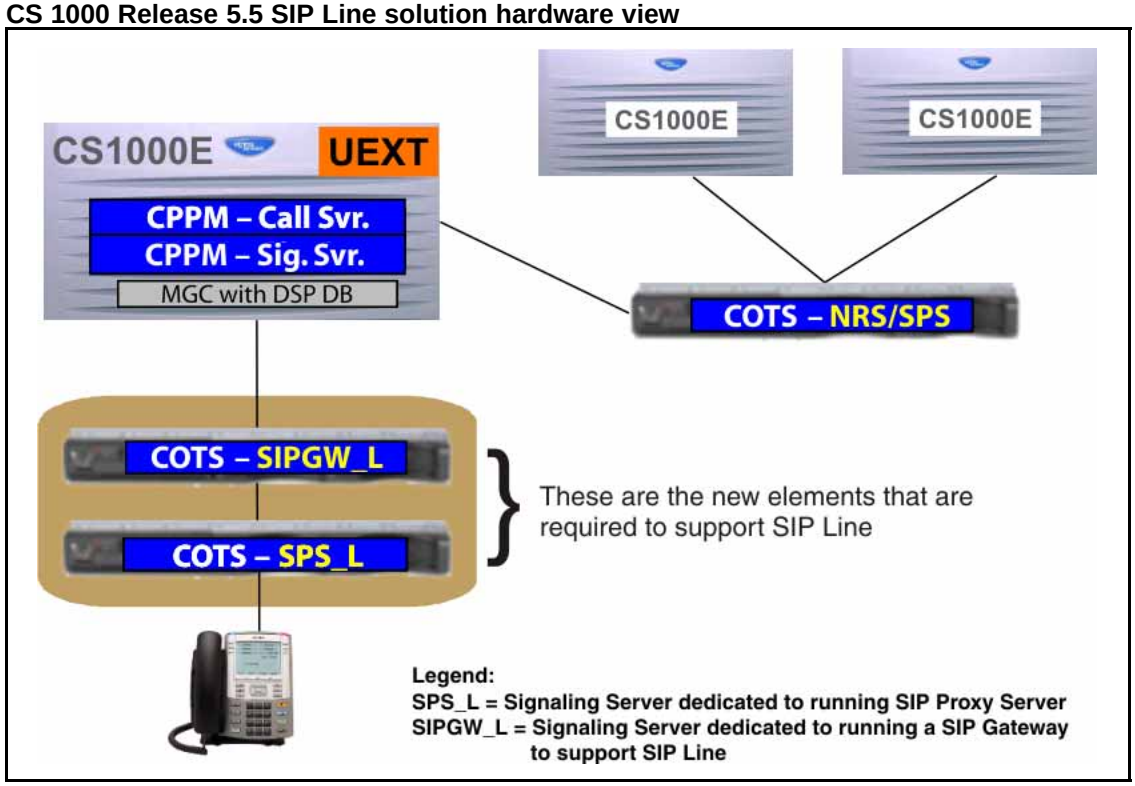
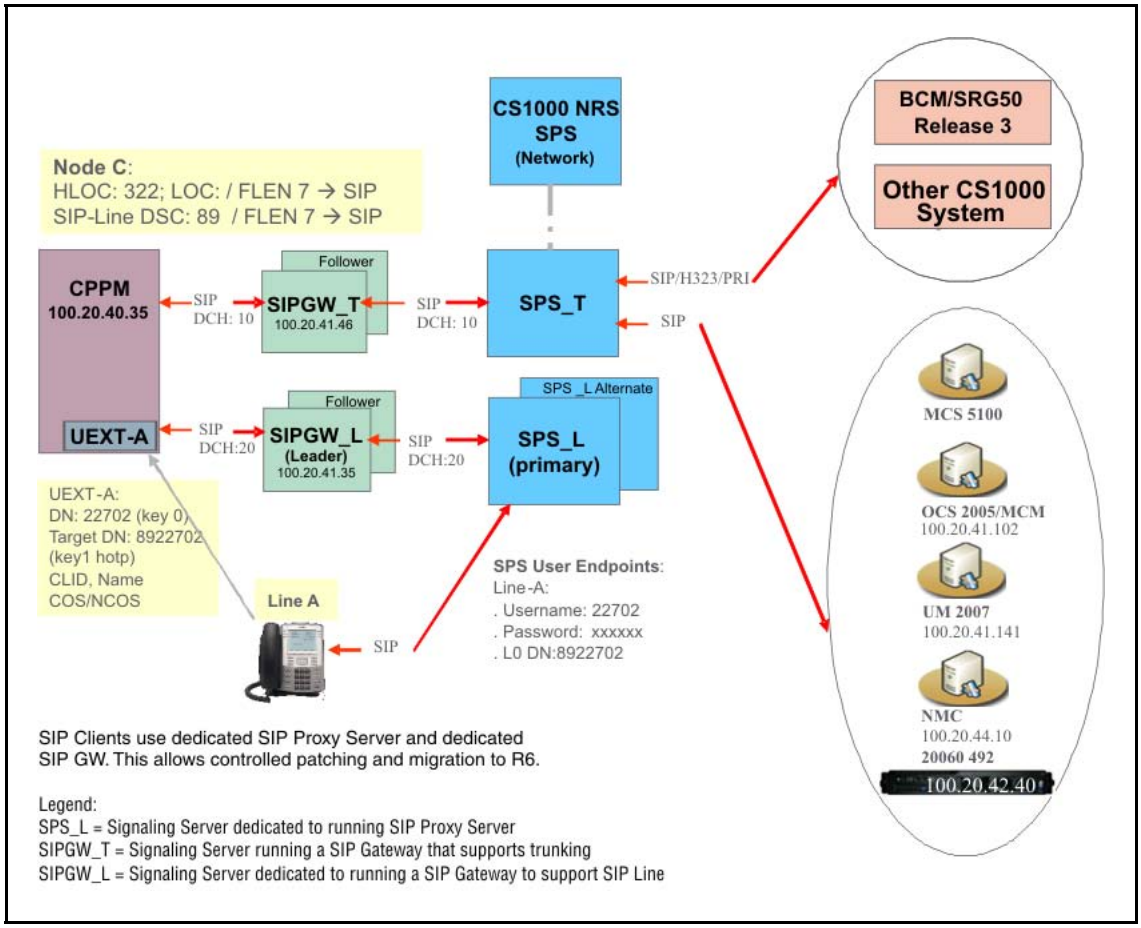


Figure 2
SIP Line solution network architecture and example dialing plan



For a nonredundant configuration, deploy SIP Line servers in groups of two: a dedicated SIP Gateway and a dedicated SIP Proxy Server deployed in a 1:1 ratio. To expand the system, you can add up to 5 multiples of 2-server groups to the Communication Server 1000E system, for a total of 10 servers in a nonredundant configuration. For a redundant configuration, you can add a follower for each dedicated SIP Gateway, and an alternate for each dedicated SIP Proxy Server. Each dedicated 2-server group becomes a 4-server group in a redundant configuration.

ATTENTION
CS 1000 SIP Line redundancy is available only for SIP clients that support Server1/Server2 (S1/S2) Communication Server configuration. Other clients will become inactive after fail-over from Primary to Alternate SIP Proxy Server.

Each dedicated SIP Gateway can support up to 1800 users, and each dedicated SIP Proxy Server can support up to 1800 SIP Line users. A 2-server group (1 SIP Gateway and 1 SIP Proxy Server) can support up

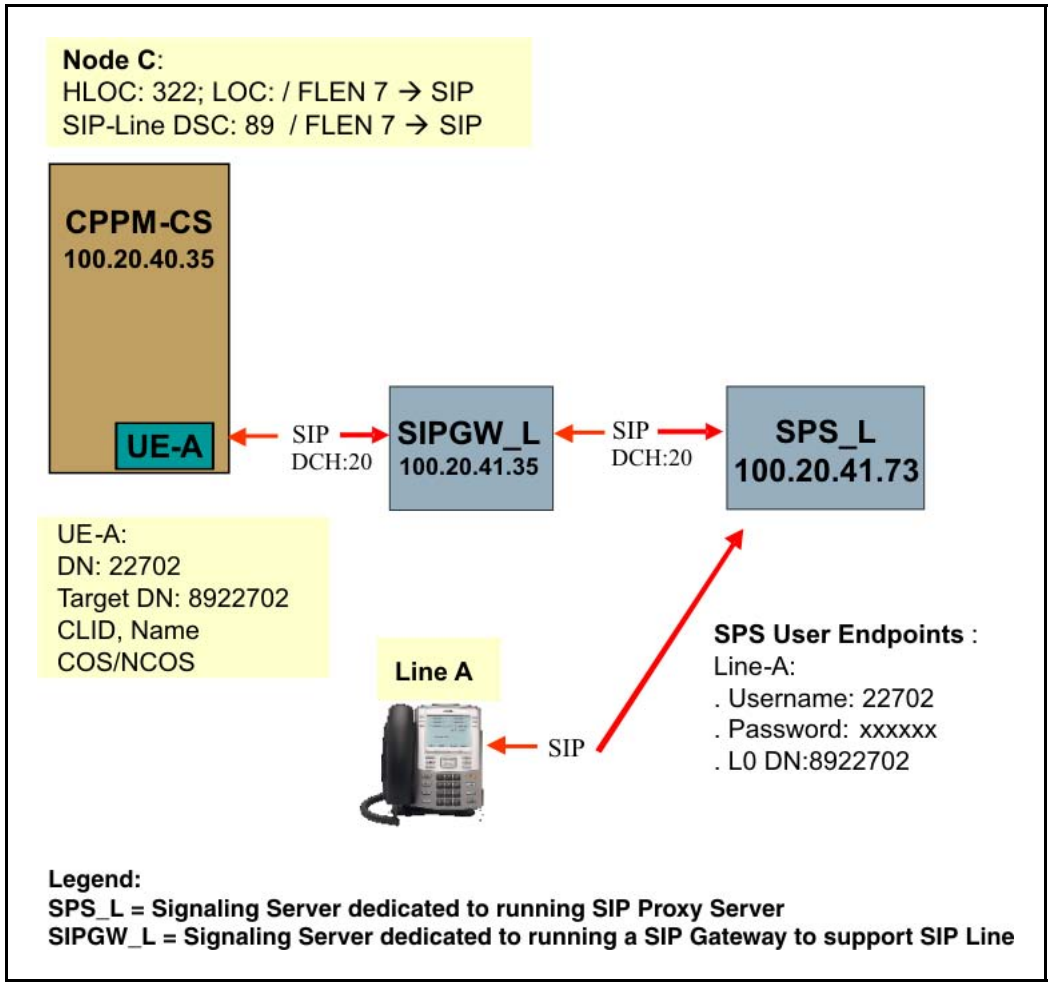
to 1800 SIP users. A single Communication Server 1000E Release 5.5 system can support up to five of these 2-server groups for a maximum capacity of 9000 SIP users. For more information about supported capacity configurations on a single Communication Server 1000E system, see Table 1 "SIP Line capacity" (page 14).

Table 1
SIP Line capacity

Number of servers	Maximum supported users
2 servers (or 4 with redundancy)	1800 users
4 servers (or 8 with redundancy)	3600 users
6 servers (or 12 with redundancy)	5400 users
8 servers (or 16 with redundancy)	7200 users
10 servers (or 20 with redundancy)	9000 users

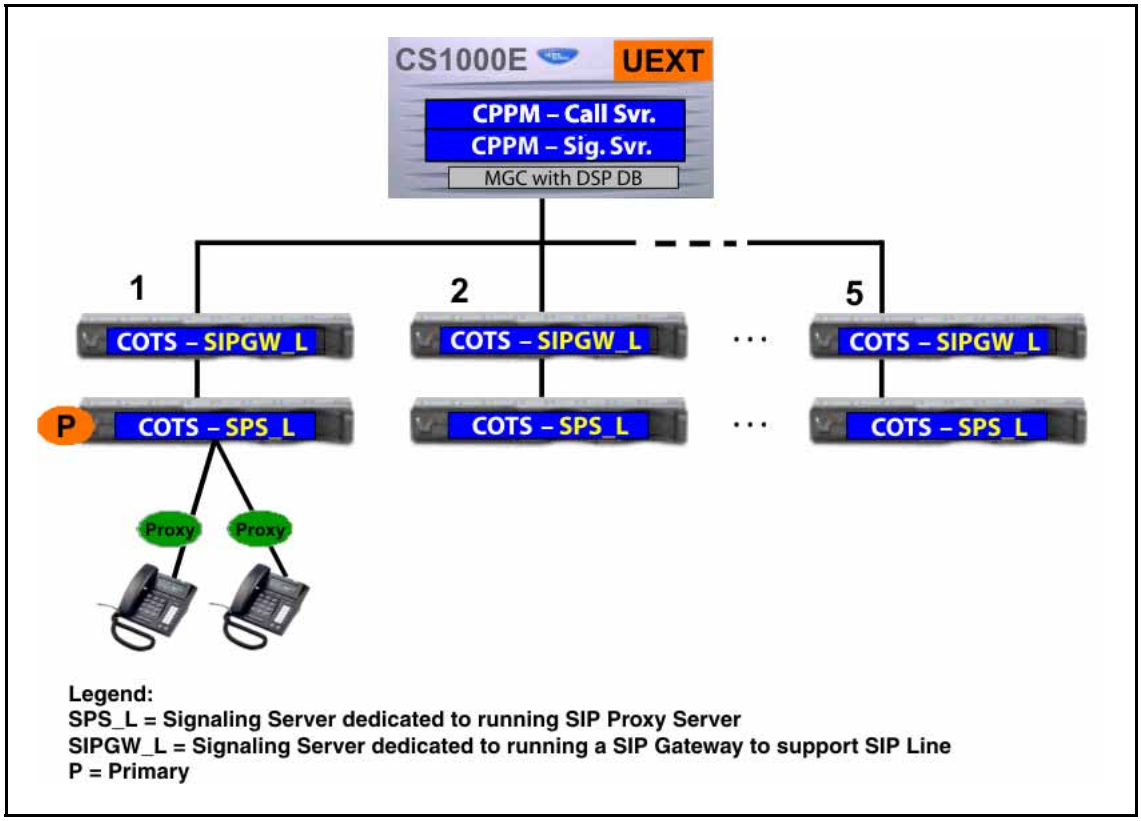
For more information about SIP Line deployment without redundancy, see Figure 3 "SIP Line deployment example -- without redundancy" (page 15).

Figure 3
SIP Line deployment example -- without redundancy



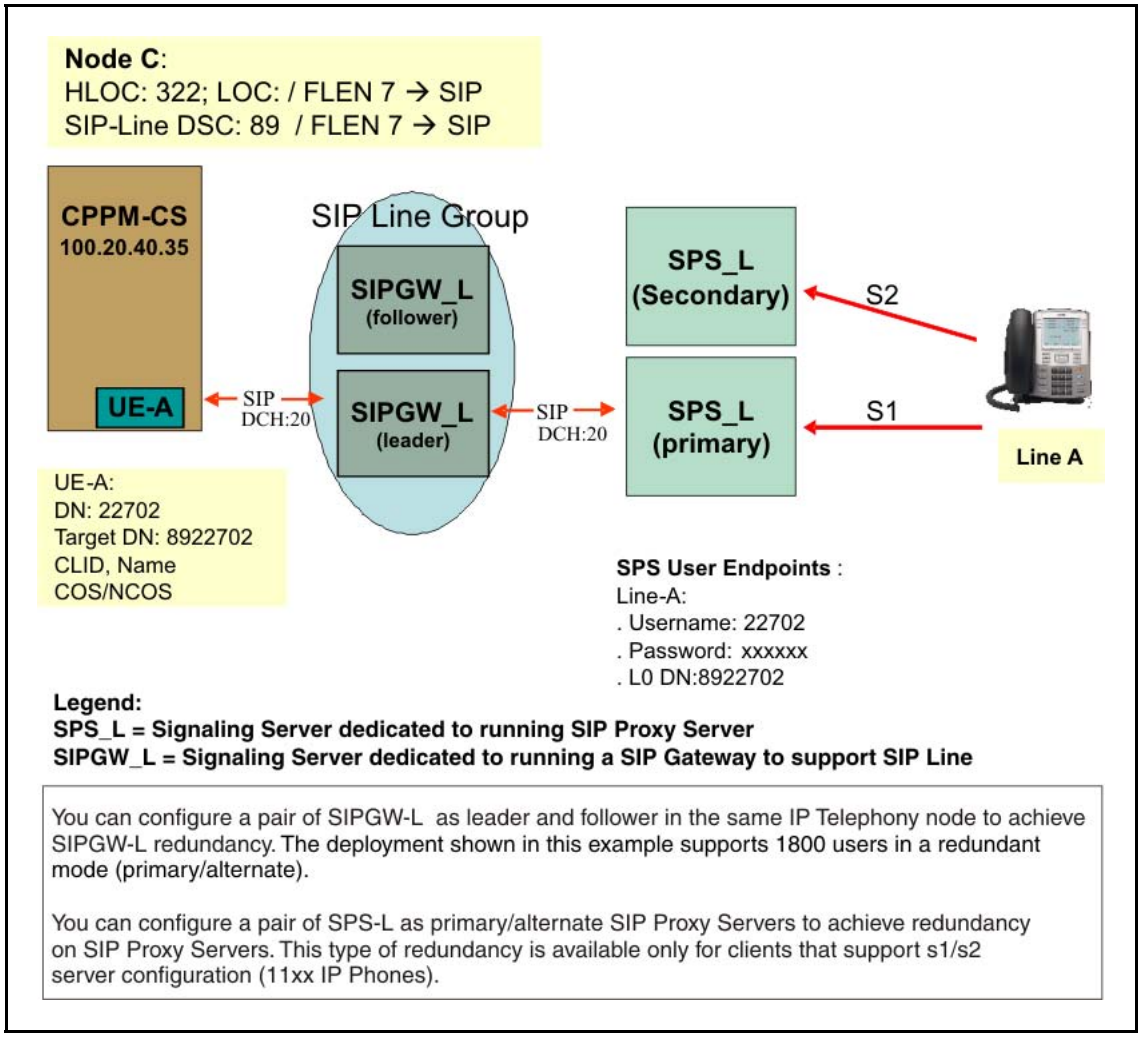
For an overview of the hardware deployment for SIP Line, without redundancy, see Figure 4 "SIP Line Hardware deployment -- without redundancy" (page 16).

Figure 4
SIP Line Hardware deployment -- without redundancy



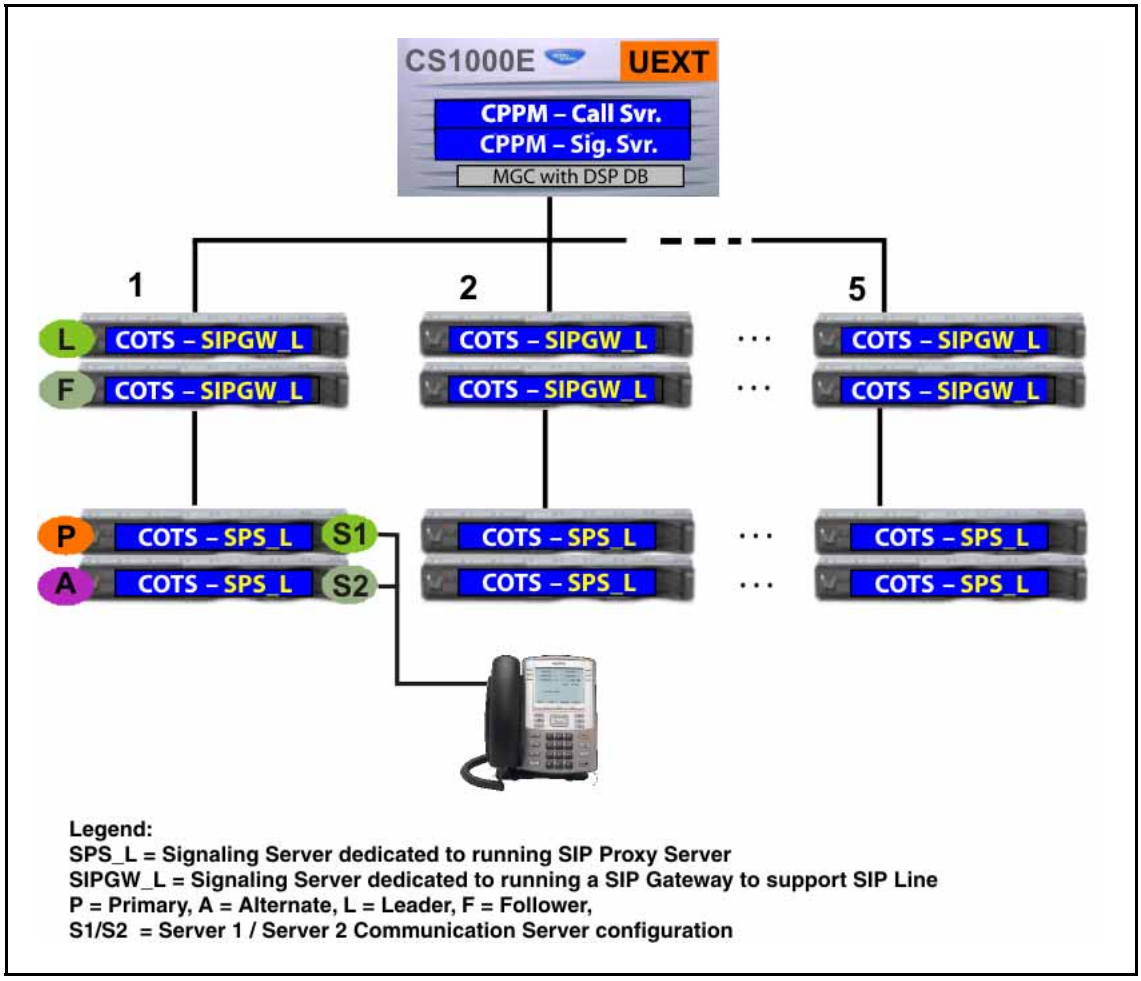
For more information about SIP Line deployment with redundancy, see Figure 5 "SIP Line deployment example -- with redundancy" (page 17).

Figure 5
SIP Line deployment example -- with redundancy



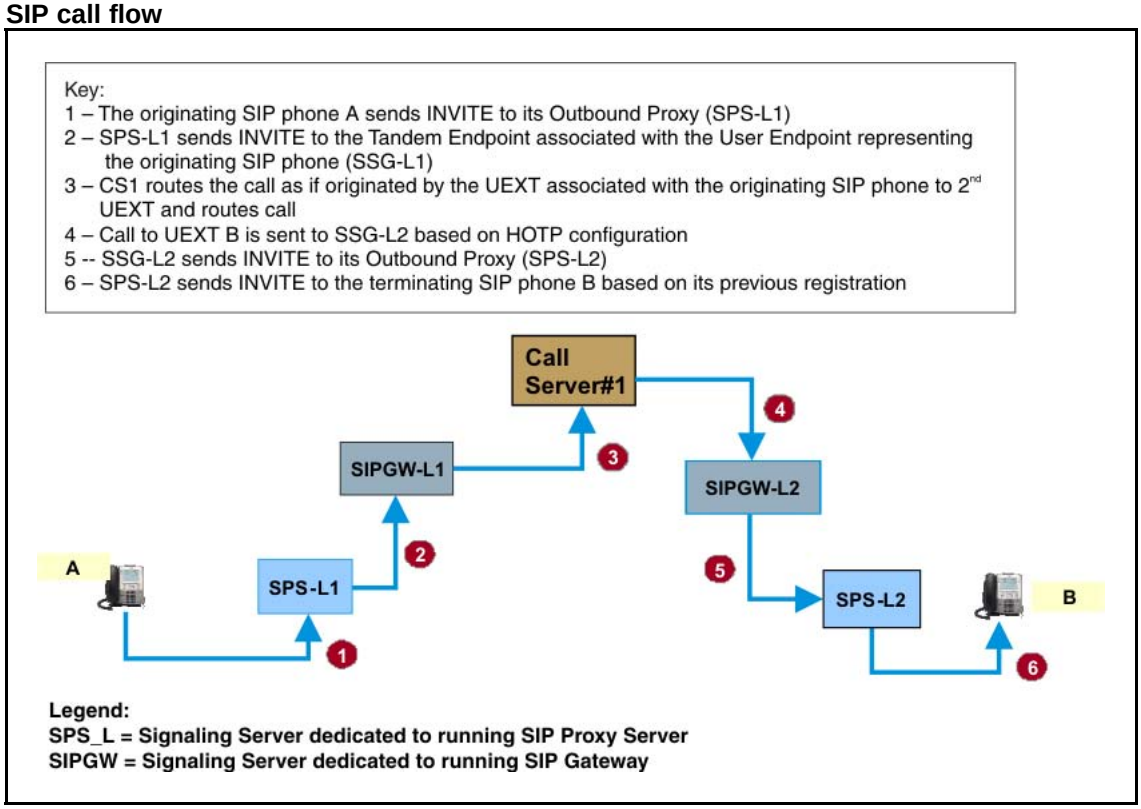
For an overview of the hardware deployment for SIP Line, without redundancy, see Figure 6 "SIP Line Hardware deployment -- with redundancy" (page 18).

Figure 6
SIP Line Hardware deployment -- with redundancy



For more information about SIP call flow, see Figure 7 "SIP call flow" (page 19).

Figure 7
SIP call flow



Platform description

CS 1000 Release 5.5 software supports SIP Line through existing software on the Call Server, SIP Signaling Gateway, and the SIP Proxy Server software elements. SIP Line operates on the same hardware platforms supported for CS 1000 Release 5.5, with the following exceptions:

- Works with all Communication Server 1000E configurations approved for Release 5.5. SIP Line is not supported on Communication Server 1000M in Release 5.5.
- SIP Line is not supported on CPPII and CPPIV; the CPPM is the Call Server hardware platform that supports SIP Line.
- The SIP Gateway that is dedicated to SIP Line and the SIP Proxy Server that is dedicated to SIP Line are supported on the COTS1 platforms approved for CS 1000 Release 5.5. The ISP1100 and CPPM are not supported for the SIP Gateway that is dedicated to SIP Line.

SIP Line leverages the deployment and maintenance methodologies used in CS 1000 Release 5.5, including system management tools and software.

Patches required

You must load the latest Dependency (DEP) list on the call server and on each signaling server in your Communication Server 1000E system. In addition, you must install patches to support SIP Line; for more information about the patches that are required, see Table 2 "Patches required for SIP Line" (page 81).

Supported features

Telephony feature functionality for CS 1000 Release 5.5 SIP Line is delivered as a combination of SIP client built-in features and Call Server-delivered features. SIP Line offers limited support for Call Server-delivered features in CS 1000 Release 5.5. For a list of supported features, see Figure 8 "SIP Telephony Features" (page 20).

Figure 8
SIP Telephony Features

	Nortel 11xx	Nortel 1535	LG-Nortel 68xx	IPDialog SipTone V
Client-based Telephony Features				
Call Hold	Yes	Yes	Yes	Yes
Call Forward	Yes	Yes	Yes	Yes
Call Transfer - Blind	Yes	Yes	Yes	Yes
Call Transfer - Consultative	Yes	Yes	Yes	Yes
Conference - 3WC	Yes	**No**	Yes	Yes
Last Number Redial	Yes	Yes	Yes	Yes
Do Not Disturb	Yes	**No**	Yes	Yes
Video	**No**	Yes	**No**	**No**
S1/S2 support	Yes	**No**	**No**	**No**
Note: SIP clients support features differently depending on the Client type and manufacturer. Consult individual client documentation for details				
Call Server-driven Telephony Features				
Calling Party Name/Number Display	Yes	Yes	Yes	Yes
Call Server Call Forward	Yes	Yes	Yes	Yes
Call Forward Busy	Yes	Yes	Yes	Yes
Call Forward No Answer, Second Level	Yes	Yes	Yes	Yes
Call Forward No Answer-Flexible Call Forward No Answer	Yes	Yes	Yes	Yes
Hunting	Yes	Yes	Yes	Yes
Privacy	Yes	Yes	Yes	Yes
New Flexible Code Restriction	Yes	Yes	Yes	Yes
Single Appearance Directory Number	Yes	Yes	Yes	Yes
Restricted Direct Inward Dialing Class of Service	Yes	Yes	Yes	Yes
Call Detail Recording	Yes	Yes	Yes	Yes
Call Detail Recording - Expansion (7 digit)	Yes	Yes	Yes	Yes
Call Detail Recording - Internal	Yes	Yes	Yes	Yes
Attendant Barge-In	Yes	Yes	Yes	Yes

ATTENTION
Other than the features in the preceding list, CS 1000 system-provided desktop features (normally available to digital or UNIStim sets) are not supported, including Flexible Feature Codes (FFC) and Special Prefix (SPRE) codes. For example, the following CS 1000 Release 5.5 features are not supported:

- Music on Hold
- Call Park and Retrieve
- Call Waiting

Other features can be available for your use, if provided by connected SIP Phone clients.

Supported clients

The following minimum firmware versions are required:

- Nortel clients
  - Nortel IP Phone 11xx series with Firmware Version 02.00.10 or later
  - Nortel 1535 Video Telephone Phase2, Firmware Version 00.2.76
- Third-party clients (SIP Line)
  - LG6804, 6812, 6830, Firmware Version 1.2.45sc
  - IpDialog phones (SIP Tone V), Revision 1.5.0 Beta build 84

The Nortel Developer Partner Program (DPP) provides third-party phone support. If you have a third-party SIP phone other than the ones in the preceding list, contact Nortel to find out if it can be tested through the DPP.

ATTENTION
Once a SIP client has gone through DPP testing and been certified, it is added to patch 25722. Otherwise it can not operate in the system.

Planning and Engineering

This chapter provides information about system planning and engineering. To use Session Initiation Protocol (SIP) Line, you must deploy a separate SIP Signaling Gateway server and SIP Proxy server, each of which you must dedicate specifically to SIP Line. You must also configure each SIP client in both Call Server (in Universal Extensions [UEXT]) and SIP Proxy Server (to define user endpoint).

Feature dependencies and restrictions

SIP Line depends on both UEXT and SIP Virtual Trunk (VTRK) operation.

Server considerations and provisioning requirements

The following provisioning requirements apply to SIP Line configurations in CS 1000 Release 5.5:

- You must configure the User endpoint on the SIP Proxy Server designated for SIP Line in Directory Number (DN) format. You cannot use an alphanumeric name.
- SIP Line supports UDP SIP transport only; TCP, TLS, and sRTP are not supported.
- You must disable Trunk Optimization Before Answer (TRO) and Trunk Anti-Tromboning (TAT) on trunks connected to the SIP Gateway designated for SIP Line.
- SIP client-based call features such as call forward, call consultation, transfer, and conferencing, are not controlled by CS 1000 Call Server Access Restrictions. You can limit access to these features by lowering the Network Class of Service (NCOS); for example, to prevent Call Forwarding from pointing to an off-net destination.

In addition, the following considerations apply to SIP Line configurations in CS 1000 Release 5.5:

- Multiple client registrations for a single SIP user against a UEXT are not supported, and each SIP client must have a unique IP address.
- Geographic Redundancy or Branch Office survivability are not supported for SIP clients.
- Name Dialing is not supported.
- Client-based Multimedia services (such as Instant Message [IM], Presence, or Collaboration) are not supported.
- Enhanced 911 services, including location autodiscovery, are not supported.

  ATTENTION
  Basic 911 service is supported.

- SIP Computer Telephony Interface (CTI) is not supported for CS 1000 SIP lines.
- In some situations, ringback fails when a call is blind transferred to Nortel Business Communications Manager (BCM) 50 using an H323 trunk.
- The Nortel 1535 SIP Video telephone cannot initiate a 3-way voice call.
- The Nortel 1535 SIP Video telephone's implementation of PRACK can exhibit clipping when calling voice mail systems, clipping part of the voice mail greeting.
- When you install the SIP Gateway dedicated to SIP Line, you must provision SIP Gateway only. Disable Failsafe NRS, TPS, H323 Gatekeeper, Personal Directory, and other services.
- Basic (1+1) redundancy of the dedicated SIP Proxy Server can be supported only by phones that support Server1/Server2 (S1/S2) mechanism, such as the Nortel 11xx series SIP clients. If you create a redundant configuration, SIP clients that do not support S1/S2 mechanism cannot operate.
- When a call is transferred, it is routed back to the Call Server for call setup, which uses a new trunk.
- Calling Party identity is not always under the control of the call server.
- SIP Line does not support media security.
- SIP client initiated Ad-hoc conference on Call Server is not supported. Only client-internal conferencing is supported.
- CS 1000 Release 5.5 SIP Line Universal Extensions are not supported within the CS 1000 Bandwidth Management calculations.
- Caller ID (CLID) is not updated when a call is redirected, forwarded, or transferred.

- IP Call Recording is not supported on SIP clients.
- SIP Line does not support Multiple Appearance Directory Number (MADN), therefore you must configure SCR to ensure proper UEXT busy status indication.
- Feature interactions for Session Initiation Protocol (SIP) Line are the same as those for SIP VTRK. In addition, IP Phone 11xx telephones remain busy after Nortel Business Communications Manager (BCM) 50 releases call.
- The supported CS1000 release 5.5 SIP Line redundancy configurations improve availability and resiliency with fully automated failure recovery mechanisms for each software element of the solution (the Call Server and Signaling Servers that are dedicated to SIP Line). Individual SIP Line functionality for each line is restored by an automatic mechanism. However, when a catastrophic hardware failure occurs on the CPPM running the Call Server software, the automatic synchronization of the redundant Call Server and the SIP Gateway dedicated to SIP Line can take up to several minutes. For example, if a CPPM hardware failure of the active core occurs in a redundant SIP Line configuration (with the Call Server core running on the supported CPPM hardware), it can take up to 10 minutes for every 3000 SIP phones, for all SIP lines to fully recover.

System engineering

This section provides recommendations for system engineering.

Call Server

The following considerations apply to Call Server configuration:

- A maximum of 9000 SIP lines can be supported in CS 1000 Release 5.5 on CPPM-based systems. The maximum number of SIP lines supported can be further reduced by other factors, such as available TN space and Central Processing Unit (CPU) usage.
- SIP Line clients cannot be supported as ACD agents.
- Each SIP client is configured as SIPN or SIP3 UEXT, and each client requires one SIP VTRK during the call, thus extra Virtual Terminal Numbers (VTN) are required to support SIP client. Client TN and VTRK TN are in a 1-to-1 ratio.

SIP Proxy Server

The call rate supported by the system is limited by the capacity of the primary SIP Proxy Server, because it is involved in processing all SIP Line calls within this system.

Limitations on the SIP Proxy Server are the same as those for Release 5.5; 1800 clients for each dedicated SIP Proxy Server.

For ease of management, if you desire redundancy, Nortel recommends that you configure an alternate SIP Proxy Server as the backup. A backup proxy server can support only those clients that support S1/S2 configuration (for example, IP Phone 11xx series telephones).

SIP Gateway

The performance of a SIP Gateway when used for SIP Line is the same as the performance of traditional SIP trunks with a SIP Gateway.

Limitations on the SIP Gateway are the same as those for Release 5.5; 1800 trunks for each SIP Gateway designated for SIP Line.

Signaling protocol

Only UDP SIP clients are supported; therefore TLS and TCP are not supported for SIP clients.

Planning

Nortel recommends that you plan UEXT DN and HOT P DN so that SIP clients are grouped together, and are routed to the desired SIP Gateway and SIP Proxy Server you have designated for SIP Line. For example, assign the first five hundred DNs to the first gateway, the next five hundred DNs to the second gateway, and so on.

Work flow: installing and configuring SIP Line

Install components and configure and Communication Server 1000 (CS 1000) Release 5.5 to support Session Initiation Protocol (SIP) Line service.

This chapter contains information that guides you through the steps you must complete to configure SIP Line on CS 1000 Release 5.5:

- Follow “Installing and configuring SIP Line tasks” (page 27) to learn what tasks you must perform, and in what order.
- Follow the Task flows, identified in the Work flow, to complete each of the tasks described in the Work flow.

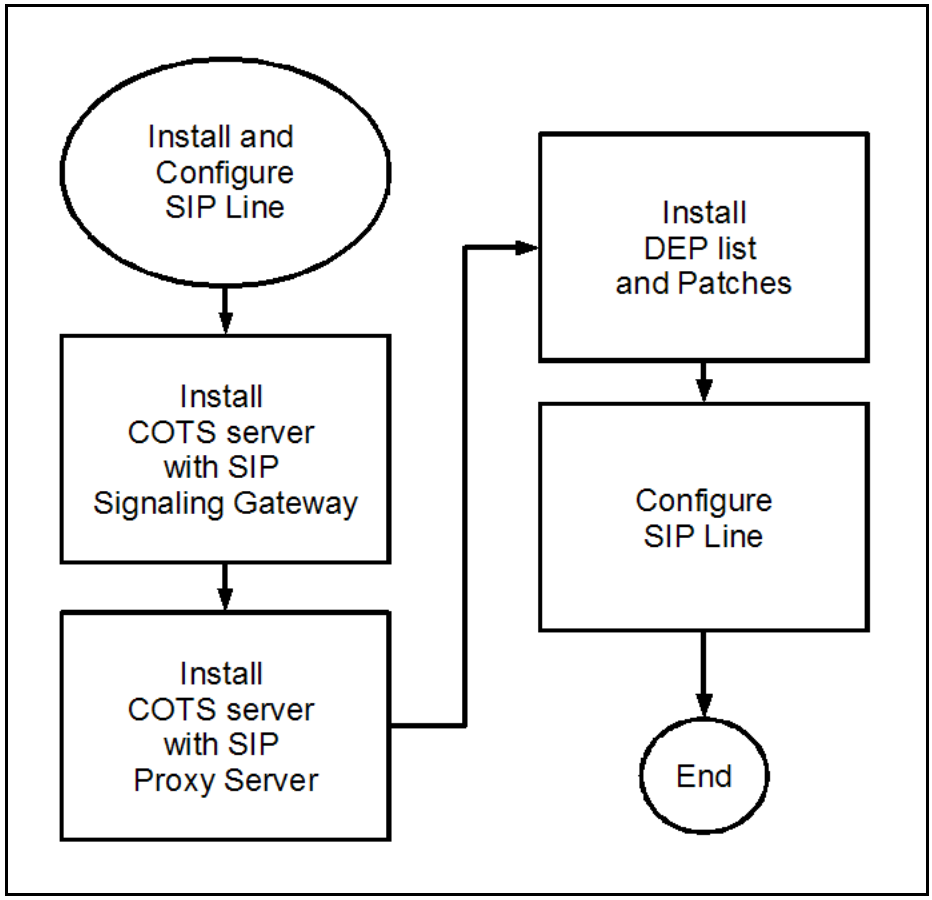
Prerequisites for installing and configuring SIP Line

- You must have a Communication Server 1000E system, with CPPM, installed and configured with CS 1000 Release 5.5 software before you begin to install and configure SIP Line. If you have an existing Communication Server 1000E system that is not installed with CS 1000 Release 5.5, see *Communication Server 1000E Software Upgrades* (NN43041-458) for more information about upgrading.
- You must install the latest DEP list for the Call Server and Signaling Servers (including Signaling Servers that run SIP Gateways that support trunking, and Signaling Servers that run SIP Gateways that are dedicated to supporting SIP Line).

Installing and configuring SIP Line tasks

This work flow shows you the sequence of tasks you perform to install and configure the SIP Line service on CS 1000 Release 5.5. To link to any tasks, click on “Installing and configuring SIP Line navigation” (page 28).

Figure 9
Installing and configuring SIP Line tasks



Installing and configuring SIP Line navigation

- “Install COTS server with SIP Signaling Gateway” (page 30)
- “Install COTS server with SIP Proxy Server” (page 31)
- “Install patches” (page 80)
- “Configure SIP Line” (page 94)

Installation

Use the information and procedures in this chapter to install and configure the hardware and software that is required to support Session Initiation Protocol (SIP) Line.

To support SIP Line you must install a commercial off-the-shelf (COTS) server running VxWorks to support a SIP Gateway. The IBM X306m server is a rack-mountable, Pentium 4, PC-based, COTS 1U server. For more information, see the following documents:

- *Nortel Communication Server 1000 Signaling Server Installation and Commissioning* (NN43001-312).
- User and installation guides that are included in the box with the server, or otherwise available from the manufacturer.

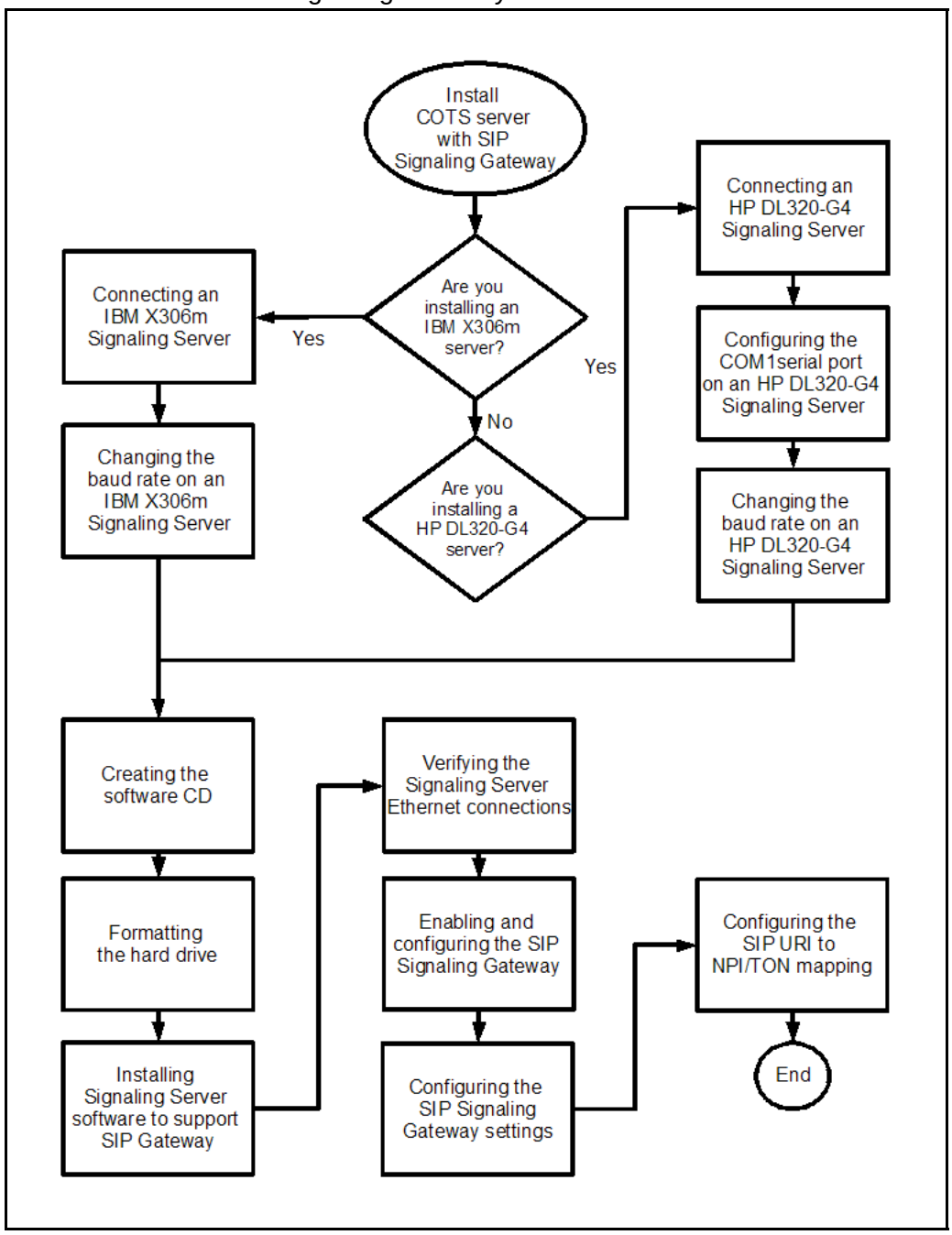
ATTENTION
You must have a Communication Server 1000E system, with CPPM, installed and configured before you begin to install and configure SIP Line.

Use the task flow on the following page to guide you in the order to perform the procedures in this chapter.

Task Flows

Install COTS server with SIP Signaling Gateway

Install and configure a Commercial Off-The-Shelf (COTS) server, including a SIP Signaling Gateway.

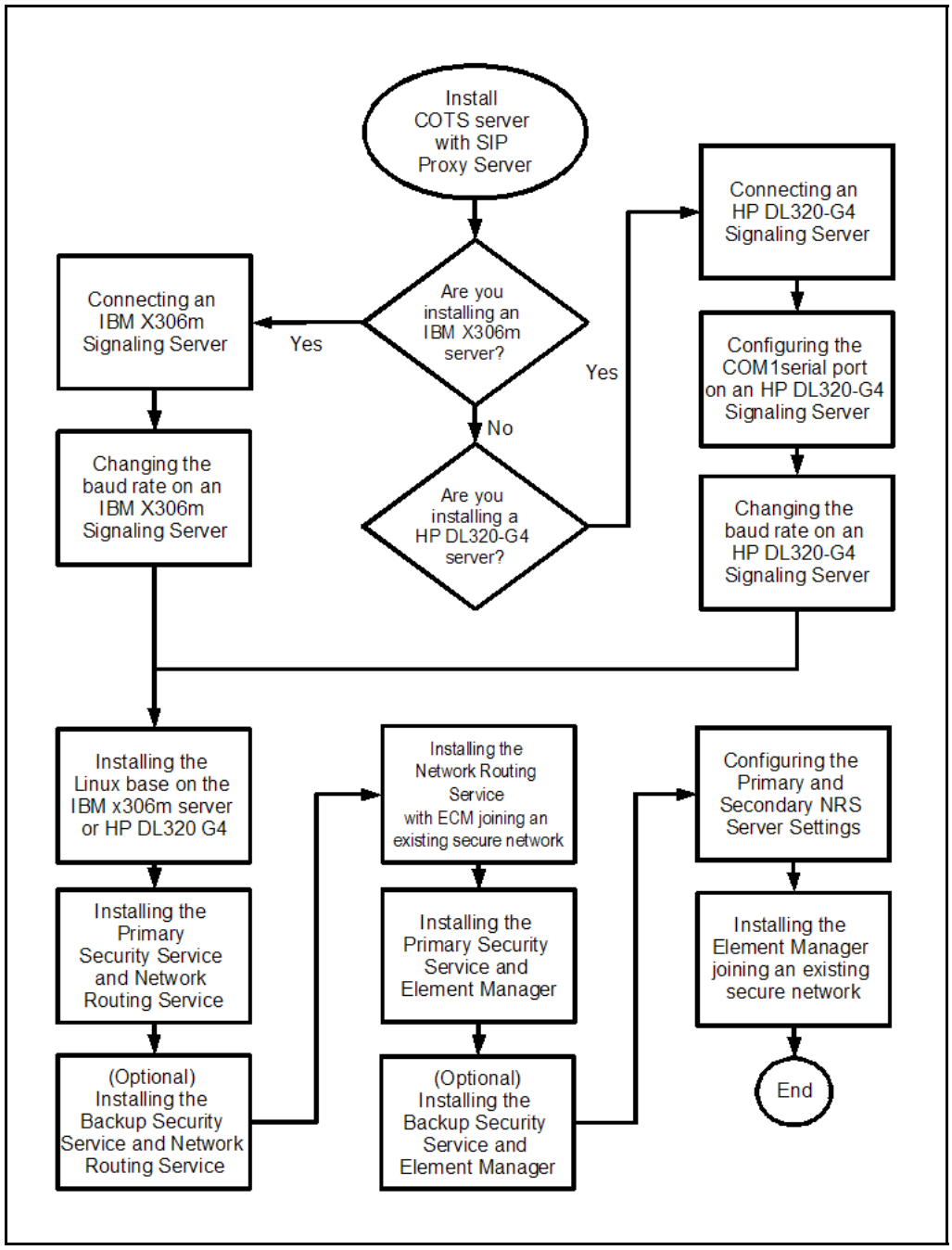


Install COTS server with SIP Signaling Gateway navigation

- “Connecting an HP DL320-G4 Signaling Server” (page 38)
- “Changing the baud rate on an IBM X306m Signaling Server” (page 36)
- “Connecting an IBM X306m COTS server” (page 34)
- “Configuring the COM1 serial port on an HP DL320-G4 Signaling Server” (page 40)
- “Changing the baud rate on an IBM X306m Signaling Server” (page 36)
- “Creating the software CD” (page 43)
- “Formatting the hard drive” (page 45)
- “Installing Signaling Server software to support SIP Gateway” (page 47)
- “Verifying the Signaling Server Ethernet connections” (page 52)
- “Enabling and configuring the SIP Signaling Gateway” (page 53)
- “Configuring the SIP Signaling Gateway settings” (page 55)
- “Configuring the SIP URI to NPI/TON mapping” (page 57)

Install COTS server with SIP Proxy Server

Install and configure a Commercial Off-The-Shelf (COTS) server, including a SIP Proxy Server.



Install COTS server with SIP Proxy Server navigation

- “Connecting an IBM X306m COTS server” (page 34)
- “Changing the baud rate on an IBM X306m Signaling Server” (page 36)
- “Connecting an HP DL320-G4 Signaling Server” (page 38)

Connecting an IBM X306m COTS server

Use the following procedure to install an IBM X306m COTS server.

Prerequisites

- In addition to the server, ensure that you have the following server equipment and peripherals:
  - — Installation accessories for rack-mounting the server.
  - — AC-power cord.

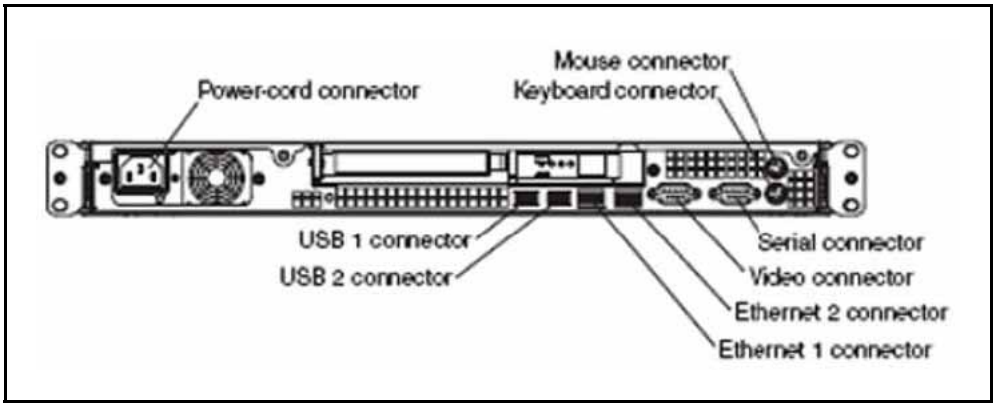
WARNING
Do not modify the power cord, or use a supplied AC-power cord if it is not the exact type required in the region where the Signaling Server is installed and used. If you must replace the cord, ensure that the replacement cord is the correct type.

CAUTION
In geographic regions that are susceptible to electrical storms, Nortel recommends that you plug the IBM X306m server into an AC surge suppressor.

  - — A Data Terminal Equipment (DTE)-DTE null modem serial cable. Use this to connect the Signaling Server to the maintenance terminal (this cable is supplied).
  - — Two CAT5 (or higher) cables. Use these cables to connect the Signaling Server to the ELAN and TLAN subnets.

Procedure steps

Step	Action
1	Connect the server to the TLAN subnet. Insert the RJ-45 CAT5 (or better) cable into the Ethernet 1 connector (TLAN network interface) on the back of the server.



2 Connect the server to the ELAN subnet.
Insert the RJ-45 CAT5 (or better) cable into the Ethernet 2 connector (ELAN network interface) on the back of the server.

3 Connect a DTE–DTE null modem serial cable from the serial port on the back of the Signaling Server to the serial port on a maintenance terminal.

4 Connect the server power cord.
Attach the female end of the power cord to the mating AC power receptacle on the left side of the server back panel. Plug the male end of the AC power cord into the AC power source (wall outlet).

WARNING
Ensure that the power cord is the type required in the region where the server is used. Do not modify or use the supplied AC power cord if it is not the correct type.

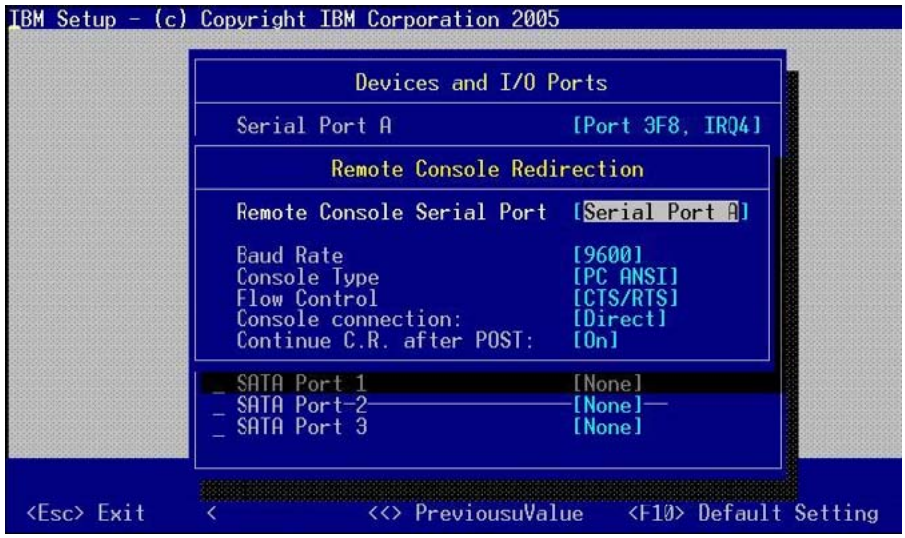
--End--

Changing the baud rate on an IBM X306m Signaling Server

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

Procedure steps

Step	Action
1	Do one of the following: • If the server is running, ensure that a monitor, keyboard and mouse are connected directly to the Signaling Server (through ports on back of Signaling Server), and press the Reset button on the front of the IBM X306m server to restart. • If the server is not running, proceed to step 2.
2	Ensure that a monitor, keyboard and mouse are connected directly to the Signaling Server (through ports on back of Signaling Server), then press the Power switch to start the server. The server starts.
3	Press **F1** . The Configuration/Setup message appears on the maintenance terminal.
4	Press **F1** The Configuration/Setup Utility menu appears.
5	Select the **Devices and I/O Ports** option, and then press **Enter**. The Devices and I/O Ports menu appears.
6	Select the **Remote Console Redirection** option, and then press **Enter**. The Remote Console Redirection menu appears.



7 Select the **Baud Rate** option and enter the value `9600`.

Press **Enter**.

8 Press **Esc** to exit the **Remote Console Redirection** page. The Devices and I/O Ports menu appears.

9 Press **Esc** to exit the **Devices and I/O Ports** page. The Configuration/Setup Utility menu appears.

10 Select the **Save Settings** option, and then press **Enter** to save the changed parameters.

11 Select the **Exit Setup** option, and then press **Enter** to exit the IBM X306m Configuration/Setup Utility.
The server restarts.

--End--

Connecting an HP DL320-G4 Signaling Server

Use the following procedure to install an HP DL320-G4 Signaling Server.

Prerequisites

- Ensure that you have the following server equipment and peripherals:
  - — Installation accessories for rack-mounting the server.
  - — AC-power cord.

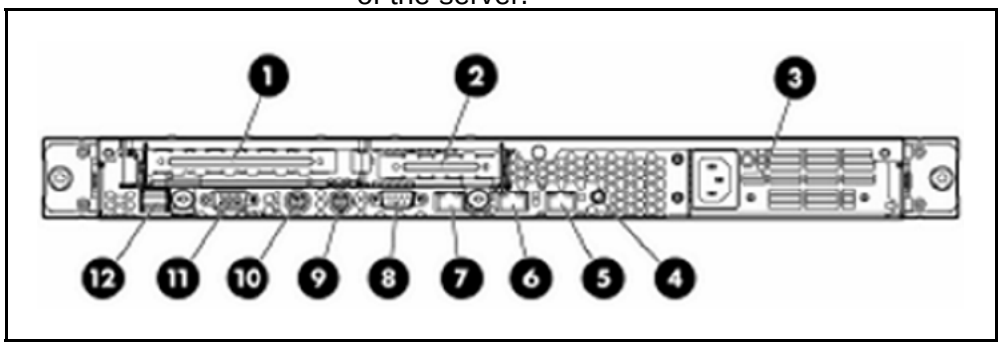
WARNING
Do not modify the power cord, or use a supplied AC-power cord if it is not the exact type required in the region where the Signaling Server is installed and used. If you must replace the cord, ensure that the replacement cord is the correct type.

CAUTION
In geographic regions that are susceptible to electrical storms, Nortel recommends that you plug the IBM X306m server into an AC surge suppressor.

  - — A DTE-DTE null modem serial cable. Use this to connect the Signaling Server to the maintenance terminal (this cable is supplied).
  - — Two CAT5 (or higher) cables. Use these cables to connect the Signaling Server to the ELAN and TLAN subnets.

Procedure steps

Step	Action
1	Connect the server to the TLAN subnet. Insert the RJ-45 CAT5 (or better) cable into the connector labeled with the number 5 (TLAN network interface) on the back of the server.



2 Connect the server to the ELAN subnet. Insert the RJ-45 CAT5 (or better) cable into the connector labeled with the number 6 (ELAN network interface) on the back of the server.

3 Connect a DTE–DTE null modem serial cable from the serial port on the back of the server (COM1) to a maintenance terminal.

4 Connect the server power cord.
Attach the female end of the power cord to the mating AC power receptacle on the right side of the back panel. Plug the male end of the AC power cord into the AC power source (wall outlet).

WARNING
Ensure that the power cord is the type required in the region where the server is used. Do not modify or use the supplied AC power cord if it is not the correct type.

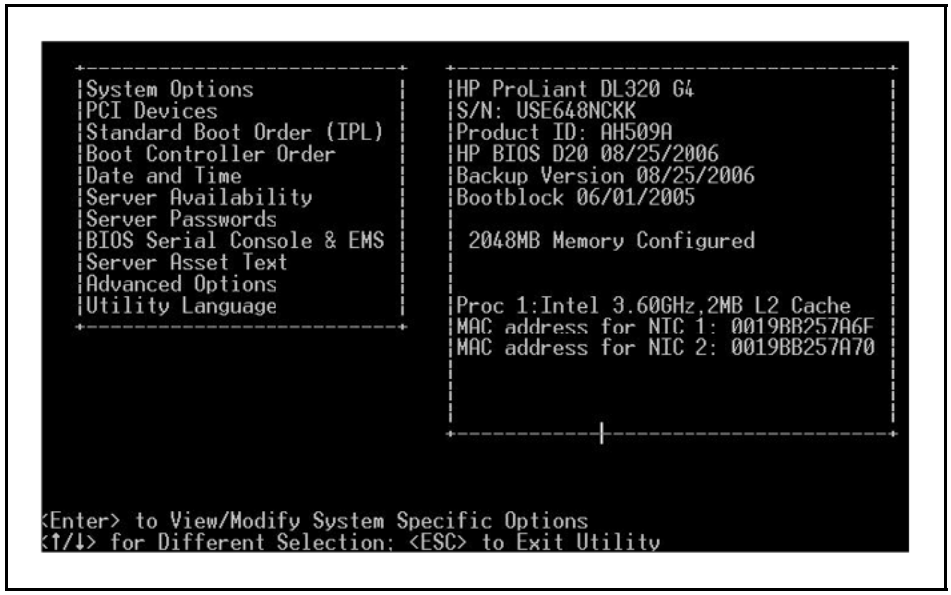
--End--

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

Use the following procedure to configure the COM1 port of an HP DL320-G4 Signaling Server as the communication port for the connected maintenance terminal.

Procedure steps

Step	Action
1	Connect a monitor, keyboard and mouse directly to the Signaling Server (through ports on back of Signaling Server) before you turn on the Signaling Server. If you use your maintenance terminal connection (Null Modem cable connected to the serial port), you cannot access the Graphical User Interface (GUI) for the ROM-Based Setup Utility. You must use the Command line prompt of the ROM-Based Setup Utility.
2	Press the Power switch to start the server. The server starts and the HP DL320-G4 boot menu appears.



3	Press **F9** to invoke the ROM-Based Setup Utility (RBSU) menu. The RBSU menu appears.
4	Select the **BIOS Serial Console & EMS** option, and then press **Enter**. The BIOS Serial Console & EMS configuration menu appears.

5 Select the **BIOS Serial Console Port** option, and then press **Enter**.

The BIOS Serial Console Port configuration menu appears:

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

6 Select the **3 | COM 1** option, and then press **Enter**.

This step configures the COM 1 port as the serial port for communicating with the connected maintenance terminal. The BIOS Serial Console & EMS configuration menu reappears.

7 Press **Esc** to exit the BIOS Serial Console & EMS configuration menu.

The RBSU menu reappears.

8 Press **Esc** to exit the ROM-Based Setup Utility.

9 Press **F10** to Confirm Exit Utility.

The server restarts

--End--

Changing the baud rate on an HP DL320-G4 Signaling Server

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

Procedure steps

Step	Action
1	Press the power switch to start the server. The server starts and the HP DL320-G4 boot menu appears.
2	Press **F9** to invoke the **ROM-based Setup Utility (RBSU)** menu. The RBSU menu appears.
3	Select the **BIOS Serial Console & EMS** option, and then press **Enter**. The BIOS Serial Console & EMS configuration menu appears.
4	Select the **BIOS Serial Console Baud Rate** option, and then press **Enter**. The BIOS Serial Console Baud Rate configuration window appears: • `9600` • `19200` • `57600` • `115200`
5	Select the**9600** setting, and then press **Enter** to configure the serial port speed to 9600 bps. The BIOS Serial Console & EMS configuration menu reappears.
6	Press **ESC** to exit the **BIOS Serial Console & EMS configuration** menu. The RBSU menu reappears.
7	Press **ESC** to exit the ROM-Based Setup Utility.
8	Press **F10** to confirm. The server restarts.

--End--

Creating the software CD

Use the following procedure to download Signaling Server software, operating system, Web files, and a Signaling Server software Installation Tool, and load them onto a bootable compact disk (CD) to install the CS 1000 Release 5.5 Signaling Server software onto the IBM X306m or HP DL320-G4 COTS server.

Prerequisites

- You must download the appropriate Signaling Server software file from the Nortel Technical Support Web site:
  - To download the file, go to http://support.nortel.com/.

    Use the following information as a guide to help you identify the file:
    - Page: Home, Technical Support, HOW DO I DOWNLOAD CONTENT?
    - Product Category: VOIP & Multimedia Communications/Communications Servers
    - Product Name: Signaling Server and IP Peer Networking
    - Content Type: Software
- You must have CD writer software that can create a CD from an .ISO image, and you must be familiar with the use of that software. For more information about instructions to help you create a CD from an .ISO file, see your CD writer software documentation. The Readme file that accompanies the Signaling Server software download contains additional information.

Procedure steps

Step	Action
1	Use your CD writer software to create a CD from the ISO image. Select the disk-at-once write option. **ATTENTION** Do not drag and drop the ISO image to the CD, as this can trigger a file copy, which can result in a CD that does not work as required.
2	Close the session.

3 Label the CD appropriately.
For example, Signaling Server, *sse-x.xx.xx* where x.xx.xx represents the Signaling Server software version.

--End--

Formatting the hard drive

Use the following procedure to format the hard drive on a newly installed IBM X306m or HP DL320-G4 COTS server.

Prerequisites

- Install and connect the Signaling Server.
- Obtain the appropriate Signaling Server software CD.

Procedure steps

Step	Action
1	Start the Signaling Server from the CD. Insert the Signaling Server software CD into the CD drive, and then press the **RST** button on the front panel of the Signaling Server. The VxWorks™ banner appears, followed by system messages indicating that the Signaling Server Software Installation Tool is being loaded from the Signaling Server software CD. After the Signaling Sever Software Installation Tool is loaded, the Installation Tool banner appears.
2	Press **Enter** to perform system checks. If the hard drive of the Signaling Server is not partitioned, the file system verification process fails and the file system verification failure message appears.

```
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
```

3	Type **a** to partition and initialize the disk. The following system messages appear: **Partitioning hard disk ...Hard disk partitioning succeeded. Creating filesystems ...Filesystems**

```
creation succeeded.  Rebooting system ...
```

--End--

Installing Signaling Server software to support SIP Gateway

Use the following procedure to install the Signaling Server software and system components on an IBM X306m or HP DL320-G4 Signaling Server, and to enter basic configuration parameters.

Prerequisites

- Install and connect the Signaling Server.
- Obtain the appropriate Signaling Server software CD.
- Partition the server hard drive.
- Obtain the network and IP Telephony data for the Signaling Server from your Planning and Engineering group:
  - node ID of the new IP Telephony node for the SIP Gateway that is dedicate to SIP Line.
  - node IP address for the IP Telephony node.
  - host name for the Signaling Server.
  - ELAN network interface IP address, Subnet mask, and Gateway.
  - TLAN network interface IP address, Subnet mask, and Gateway.
  - ELAN network interface IP address of the Call Server
  - Primary and Alternate NRS IP addresses for this networked system. For more information, see *IP Peer Networking Installation and Commissioning* (NN43001-313).
  - NRS role, if applicable. For more information, see *IP Peer Networking Installation and Commissioning* (NN43001-313).

Procedure steps

Step	Action
1	Start the Signaling Server from the CD. Insert the Signaling Server software CD into the CD drive, and then press the **RST** button on the front panel of the Signaling Server. The VxWorks™ banner appears followed by system messages indicating that the Signaling Server Software Installation Tool is being loaded from the Signaling Server software CD. After the Signaling Sever Software Installation Tool is loaded, the **Installation Tool** banner appears.

2 Press **Enter** to perform system checks.
The following system messages appear:
`Verifying filesystems ... Filesystems verification succeeded.`
The **Date and Time** page appears.

3 Confirm or enter the date and time.
The **System Information** page appears.
For a new installation, data fields in the system information page are normally blank.

4 Press **Enter** a to continue the installation.
The **Installation Tool Main Menu** appears.

5 Enter **a** to perform a complete installation.
During installation, a series of system messages appear.
Once the installation is complete, the **Dependency (DEP) lists installation** page appears.

6 Enter **y** to install the DEP lists.
The **Installation Status Summary** appears.

7 Enter **y** to confirm your selected installation options and start the installation.
The following windows and messages appear in succession:

- The first window provides information about the installation of the Signaling Server software.
- The second window indicates the successful installation of the Signaling Server software.
- The third window provides information about the installation of the IP phone firmware.
- The fourth window provides information about the installation of the Voice Gateway Media Card loadware.
- After the Signaling Server software and system components are installed, the **Restore IP configuration** page appears.

8 Enter **b** to bypass the restoration of IP configuration data.
You must enter the IP configuration data in the subsequent steps of this procedure.
The **Signaling Server role selection** menu appears.

9 Configure the Signaling Server as a Leader or Follower.

- If a Leader Signaling Server exists in the IP Telephony node, enter **b** at the prompt to configure this Signaling Server as a Follower. The **Follower Signaling Server configuration** page appears. For more information about configuring a follower signaling server, see *Nortel Communication Server*

1000 Signaling Server Installation and Commissioning (NN43001-312).

- If a Leader Signaling Server does not exist in the IP Telephony node, press **a** at the prompt to configure this Signaling Server as Leader. The **Application configuration** page appears.

10 Enter **a** at the prompt to configure this Signaling Server as co resident LTPS, VTRK, and NRS.

The **Network Routing Service (NRS): Coresident Signaling Server** page appears.

For more information about the NRS, see *IP Peer Networking Installation and Commissioning* (NN43001-313).

11 Enter the data networking and IP telephony parameters for the Signaling Server, as prompted, including TLAN subnet parameters as required. The Call Server IP address is automatically configured to 0.0.0.0.

The **Primary NRS IP address** page appears.

12 Enter the address of the Primary NRS (optional).

If you entered the address of the Primary NRS, enter the address of the Alternate NRS (optional).

The **IP Telephony parameter confirmation** page appears.

13 Enter **y** to confirm all parameters, or enter the letter preceding a parameter to dynamically change its value.

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

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

ATTENTION

Record the MAC address that appears on the screen. You must use this value later in the procedure to configure the ELAN network interface MAC address for the newly installed Signaling Server in the Element Manager node configuration Web page.

The Installation Status Summary page appears.

14 Press **Enter** to exit to the main menu.
The Installation Tool Main Menu page appears.

15 Enter **q** to close the **Installation Tool**.
The Installation Tool quit confirmation page appears.

16 Remove the Signaling Server software CD from the Removable Media Disk (RMD) of the Signaling Server and restart the system.
The following system messages appear:
```
Removing temporary file "/u/disk.sys".  Rebooting system ...
```

17 Log on to Element Manager on the Signaling Server.
The **Home - System Overview** page appears.

If you have installed and configured a Leader Signaling Server, use steps 18 - 21 to import the temporary IP Telephony node files configured during the software installation into Element Manager for further configuration. Otherwise, go to step 22.

18 On the navigation pane, click **IP Telephony -> Nodes: Servers, Media Cards -> Configuration**.
The **Node configuration** page appears.

19 Click **Import node files**...
The Import node files page appears.

20 Enter the IP address of the Leader Signaling Server.

21 Click **Save and Transfer**.

22 On the navigation pane, click **IP Telephony -> Nodes: Servers, Media Cards -> Configuration**.
The **Node configuration** page appears.

23 Click the **Edit** button that corresponds to the node that is hosting your Signaling Server.
The **Node Edit** page appears.

24 Click **Signaling Servers**.
A list of all the Signaling Servers on the node appears.

25 Click on the **Signaling Server xxx.xxx.xxx.xxx Properties** option that corresponds to your Signaling Server (by IP address).
A list of the properties of the Signaling Server appears.

26 Clear the**Enable Line TPS** check box.

27 Configure **Enable IP Peer Gateway (Virtual Trunk TPS)** as **None**.

28 Clear the**Enable SIP Proxy / Redirect Server** check box.

29 Enter a value fpr the **Embedded LAN (ELAN) MAC address**.

30 Click **Save and Transfer**.
A message appears, indicating that the transfer was successful. This disables processes that are not required by SIP Line.

31 Click **System > IP Network > Personal Directories > Server Configuration**.
The **Server Configuration** page appears.

32 Ensure that no value is entered in the Server IP Address field.

33 Click **Submit**.
This disables processes that are not required by SIP Line.

34 Click **System -> IP Network -> Nodes: Servers, MediaCards**.
The **IP Nodes page** appears.

35 Click **EDIT**.
The **Edit Nodes** page appears.

36 Scroll down, and then click **Signaling Servers**.

37 Click **Signaling Server Properties**.

38 Clear the **Enable Line TPS** check box.

39 Clear the **Enable SIP Proxy / Redirect Server** check box.

40 Click **Save and Transfer**.
A message appears instructing you that a restart is required, and asking you to confirm the changes.

41 Click **OK**.
A message appears, indicating that the transfer was successful.

42 Restart the media card and the Signaling Server.

--End--

If you have installed and configured a Follower Signaling Server, when it restarts, it sends out BOOTP requests to the Call Server using File Transfer Protocol (FTP) to acquire the associated IP Telephony node configuration files, and waits for a response. Because the Follower Signaling Server is not yet configured in an IP Telephony node, no BOOTP response is received. Do not wait for a response; use Element Manager to add the Follower Signaling Server to an IP Telephony node, and to acquire the associated node configuration files.

For more information on IP Telephony nodes from the perspective of Voice Gateway Media Cards, see *IP Line Fundamentals* (NN43001-500).

Verifying the Signaling Server Ethernet connections

Use the following procedure to verify that you have successfully configured the Signaling Server Ethernet connections (for the ELAN and TLAN subnets) by performing a ping test to one or more of the other devices connected to the network, particularly the Call Server.

Procedure steps

Step	Action
1	Log on to the Signaling Server.
2	Ping the IP address of the Signaling Server. Enter the command **`ping x.x.x.x`** where x.x.x.x is the IP address of the ELAN network interface on the Signaling Server.
3	Ping the IP address of the Call Server. Enter the command **`ping x.x.x.x`** where x.x.x.x is the IP address of the ELAN network interface on the Call Server. If the ping test fails, ensure that the network cables are correctly connected, and ensure that the IP Address of the SIP Gateway that supports IP Line has been configured in Element Manager.
4	Optionally, repeat step 3 for other devices connected to the network.

--End--

Enabling and configuring the SIP Signaling Gateway

Use the following procedure to enable and configure the SIP Signaling Gateway. The SIP Gateway runs on the Signaling Server. You must configure the SIP Gateway on both the Call Server and the Signaling Server. Use Element Manager to configure the SIP Gateway on the Signaling Server.

Procedure steps

Step	Action
1	Log on to Element Manager.
2	In the Element Manager navigation tree, choose **System**, **IP Network**, **Nodes: Servers, Media Cards**. The Node Configuration Web page appears.
3	Click **Edit**. The Edit Web page dialog box appears.
4	Click **Signaling Servers** to expand the section. A list of Signaling Servers appears.
5	Choose the appropriate Signaling Server xxx.xxx.xxx.xxx Properties. The properties for that Signaling Server appear.
6	Choose a SIP option from the **Enable IP Peer Gateway (Virtual Trunk TPS)** menu. This step enables SIP Gateway and Services.
7	On the **SIP Transport Protocol** menu, choose **UDP**. UDP is the transport protocol used for SIP message exchange between the Gateway and Redirect/Proxy Server.
8	Verify the Local SIP Port. The Local SIP Port is the port to which the gateway listens. The default is 5060.
9	Enter the SIP Domain Name. The SIP Domain Name is the SIP Service Domain. The SIP Domain Name configured in the Signaling Server properties must match the Service Domain name configured in the NRS. The SIP Domain Name is used in building all SIP messages and appears in the phone context, and must be less than 128 characters in length. The valid characters are a-z, 0-9, period (.), hyphen (-), comma (,), and underscore (_). If the SIP Gateway application is enabled, you must enter a SIP Domain Name.
10	If authentication is turned on in the NRS (SIP Redirect Server) or on the MCS 5100 Proxy Server, you must enter a SIP Gateway Endpoint Name and SIP Gateway Authentication Password.

The values you enter must match the Gateway Endpoint name and Gateway Endpoint authentication password used by the SIP Redirect Server. The name and authentication password are used in authenticating the Gateway Endpoint with the SIP Redirect Server.

a. SIP Gateway Endpoint Name: Enter the endpoint name. The SIP Gateway Endpoint Name is the user name that is used when authenticating this gateway with the NRS (SIP Redirect Server) or the MCS 5100 Proxy Server. If authentication is enabled for the Gateway Endpoint in the NRS or Proxy Server, you must enter a SIP Gateway Endpoint Name.

b. SIP Gateway Authentication Password: Enter the password. The SIP Gateway Authentication Password is the password that is used when authenticating this gateway with the NRS (SIP Redirect Server) or the MCS 5100 Proxy Server. If authentication is enabled for the Gateway Endpoint in the NRS or Proxy Server, you must enter a SIP Gateway Authentication Password.

11 Click **Save and Transfer**.

--End--

Configuring the SIP Signaling Gateway settings

Use the following procedure to configure the SIP Signaling Gateway settings.

Procedure steps

Step	Action
1	Log on to Element Manager.
2	In the Element Manager **System, IP Network**menu, choose **Nodes: Servers, Media Cards**. The Node Configuration Web page appears.
3	Click **Edit**. The Edit Web page dialog box appears.
4	Click **SIP Gateway Settings** to expand the section.
5	Complete the following for the Primary server: • **Security Policy**: Choose **TLS Disabled**. • **Primary Proxy/Re-direct IP address**: Enter the TLAN network interface IP address of the Primary SIP Redirect Server or the MCS 5100 Proxy Server. • **Primary Proxy/Re-direct IP Port**: Leave the default port value as 5060 for the Primary SIP Redirect Server or the MCS 5100 Proxy Server. • **Primary Proxy Supports Registration**: The Primary Proxy Supports Registration check box tells the SIP Gateway whether the primary NRS (SIP Redirect Server) supports registration. If the Primary Proxy Supports Registration check box is selected, the SIP Gateway registers with the primary NRS. If the check box is cleared, the SIP Gateway does not register with the primary NRS. • **The Primary CDS Proxy or Re-direct** server flag is not used in this release. • **Secondary Proxy/Re-direct IP address**: Enter the TLAN network interface IP address of the Secondary SIP Redirect Server or the MCS 5100 Proxy Server (if configured). • **Secondary Proxy/Re-direct IP Port**: Leave the default port value as 5060 for the Secondary SIP Redirect Server or the MCS 5100 Proxy Server (if configured). • **Secondary Proxy Supports Registration**: The Secondary Proxy Supports Registration check box tells the SIP Gateway whether the secondary NRS (SIP Redirect Server) supports registration. If the Secondary Proxy Supports Registration

check box is selected, the SIP Gateway must register with the secondary NRS. If the check box is cleared, the SIP Gateway does not register with the secondary NRS.

- **The Secondary CDS Proxy or Re-direct** server flag is not used in this release.

6 Click **Save and Transfer**.

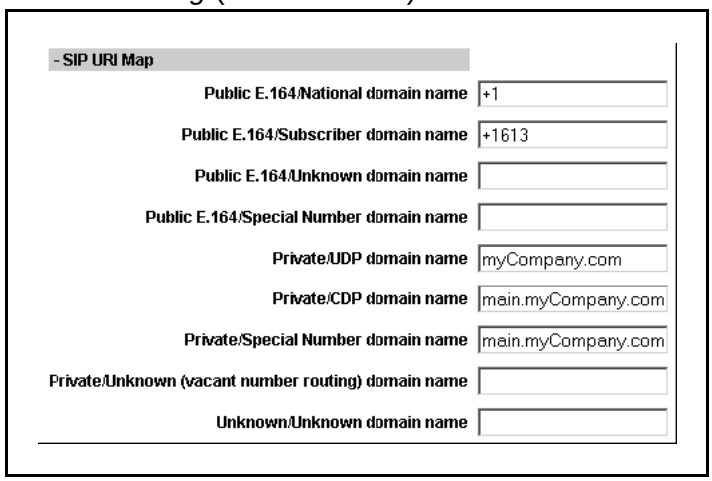
--End--

Configuring the SIP URI to NPI/TON mapping

Use the following procedure to configure the SIP Uniform Resource Identifier (URI) to Numbering Plan Indicator (NPI)/Type of Number (TON) mapping.

Procedure steps

Step	Action
1	Log on to Element Manager.
2	Choose **System IP Network**, **Nodes: Servers, Media Cards** from the Element Manager navigation tree. The Node Configuration Web page appears.
3	Click **Edit**. The Edit Web page dialog box appears.
4	Select **SIP URI Map** to expand the section. The SIP URI Map fields require a character string that is less than 128 characters in length. The valid characters include: a-z, 0-9, ., -, _, and +. If the SIP Gateway application is enabled, you must enter values for SIP URI Map. For more information about the values in this SIP URI Map section, see *Network Routing Service Installation and Commissioning* (NN43001-564).



5	Fill in the following fields for the NRS example: • Type `+1` in the **Public E.164/National domain name**box. • Type `+1613` in the **Public E.164/Subscriber domain name** box. • Leave the **Public E.164/Unknown domain name** box blank.

- Leave the **Public E.164/Special Number domain name** box blank
- Type **myCompany.com** in the **Private/UDP domain name** box.
- Type **myCdpDomain.myCompany.com** in the **Private/CDP domain name** box.
- Type **special.myCdpDomain.myCompany.com** in the **Private/Special Number domain name** box.
- Leave the **Private/Unknown (vacant number routing) domain name** box blank.
- Leave the **Unknown/Unknown domain name** box blank.

6 Click **Save and Transfer**.

--End--

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

Use the following procedure to install the Linux base software. The installation time for Nortel Linux base is approximately twenty minutes.

ATTENTION
This procedure documents the installation of Nortel Linux base on a commercial off-the-shelf (COTS) server with no previous Nortel Linux base installation.

Procedure steps

Step	Action
1	Connect to the COTS server using a serial console or keyboard, video monitor, and mouse (KVM). **ATTENTION** Before installing the Linux base, read all of the documentation provided by the manufacturer of the COTS server.
2	Insert the Linux base bootable CD-ROM in the CD-ROM tray.
3	Restart the server.
4	To install using a serial console on COM1, type **com1** at the boot prompt, and then press **Enter**. **OR** To install using an attached keyboard, video monitor, and mouse, type **kvm** at the boot prompt, and then press **Enter**. The Do you wish to proceed with installation prompt appears.
5	Type **Y**, and then press **Enter**. The Format all partitions page appears.
6	Press **Enter** to continue.
7	At the prompt, type **1** for Normal installation, and then press **Enter**.
8	Press **Enter** to continue. The System Configuration page appears.
9	Press **Enter** to continue.
10	When prompted, on the Network configuration page, enter the customer information for ELAN IP address, ELAN gateway, ELAN netmask, host name, domain name, Machine TLAN IP address, TLAN gateway, Default gateway, and TLAN netmask.

After the installation is complete, you can change the default gateway Network Interface Card (NIC) by using the CLI commands **baseparamsconfig** or **networkconfig**. You can add or delete routing entries by using the CLI command **routeconfig**.

11 Press **Enter** to continue.
The Timezone Selection page appears.

12 On the **Timezone Selection** page, type the appropriate region number at the prompt and then press **Enter** to continue.
The Configuration Validation 1 page appears.

13 On the **Configuration Validation 1** page, enter **Y** for yes or **N** for no. Press **Enter**.

If you have attached a keyboard, monitor, and mouse, the System Console Redirection page appears.

14 Select the redirection option, and then press **Enter** to continue.
The Timezone Selection for Region page appears.

15 On the **Timezone Selection for Region** page, type the appropriate time zone number at the prompt, and then press **Enter** to continue.
The Network Time Protocol (NTP) Configuration page appears.

16 On the **Network Time Protocol (NTP) Configuration** page, type **Y** or **N** to choose the Network Time Protocol transfer mode for the system. Type **1**, **2**, or **3**, and then press **Enter**.
Network Time Protocol uses Message Digest Algorithm 5 (MD5) signatures to authenticate the exchange of timestamps when operating in secure mode.

17 On the **NTP Clock Source Configuration** page, type **E** for an external clock source, or **I** for an internal clock source.
Press **Enter** to continue.

18 At the prompt, type the machine TLAN IP address of the clock source server.

19 At the prompt, configure the primary Domain Name Server (DNS) server IP address.
Type **Y** to configure or **N** if you do not wish to configure and then press **Enter**. If you selected Yes, enter the IP address for the Primary DNS server at the prompt. The default for the Primary DNS server is No.

20 On the **Configuration Validation 2** page, type **Y** if the information is correct, and then press **Enter**. If the information is incorrect, type **N**, make the required changes, and then press **Enter**.
You can use the CLI command **hostconfig** to modify the static lookup table for host names.

The Configuration Validation 2 page appears with the correct information.

21 Press **Enter** to continue.

22 On the **Date and Time Configuration** page, configure the date and time.
Type **Y** to keep the date and time, or **N** to change the date and time. Press **Enter**.
The Date and Time Configuration page appears with the new date and time.

23 Press **Enter** to continue.

24 On the **Password Configuration** page, at the prompt, enter the root password.

25 Enter the sysadmin password.

26 Enter the nortel password.
Press **Enter** to continue. The Configuration File Backup page appears

27 On the **Configuration File Backup** page, select an option to back up the configuration data.

The naming convention for the Linux base backup archive is hostname-install-yyyy.mm.dd.hh.MM.ss.tar.gz. The name for the backup archive is automatically generated and includes the key word *install* to indicate that the archive is generated as part of the upgrade procedure. For example, hp3-e-install-2008.09.04.18.54.47.tar.gz is a backup archive name where hp3-e is the host name. The archive name begins with the short host name (not the Fully Qualified Domain Name [FQDN]) and the key word *install*, and contains the following fields:

- yyyy -- year
- mm -- month
- dd -- day
- hh -- hour
- MM -- minutes
- ss -- seconds

Nortel Linux base uses the CLI command **sysbackup** to back up system data to external storage. You can choose to back up the data to a Universal Serial Bus (USB) device or to a Secure File Transfer Protocol (SFTP) server.
After you back up the configuration data, the Package Installation page appears.

28 The Post System Configuration page appears.

The system automatically restarts as a Linux server.

--End--

Installing the Primary Security Service and Network Routing Service

Use the following procedure to install the Primary Security Service and Network Routing Service (NRS).

Procedure steps

Step	Action
1	Log on to the server command line using the nortel account.
2	Insert the NRS CD-ROM in the CD-ROM tray.
3	Enter the **appinstall**.
4	At the prompt, enter the root account password. The system then prompts you to check the media.
5	Enter **Y** to check the media, or **N** to proceed without checking the media, and then press **Enter**. The Application installation window appears.
6	From the **Application installation** window select 1 to install the Primary Security Service with NRS. The appropriate packages are installed to the hard drive. The Solid server configuration confirmation page appears.
7	Confirm the server selection by selecting **Yes**, or return to the **Solid server configuration** window by selecting **No**.
8	Press **Enter** to continue. The Solid server configuration confirmation page appears.
9	Enter the option number for the Solid server to install. The Private Certificate Authority (CA) certificate window appears.
10	Press **Enter** to display the prompts for Country, State or Province, Location, Organization Name and Organization Unit.
11	Type the response for each of these categories, and then press **Enter** to continue. The Private CA Certificate confirmation window appears.
12	Verify that the common name information is correct. Type **yes** if correct or **no** if incorrect, and then press **Enter**. If you entered **yes**, the installation finishes and the system creates the CA certificate. If you selected **no**, edit the information as required and repeat the step. The installation takes approximately thirty minutes to complete. After the installation is complete the disk automatically ejects from the drive and a summary of the installation appears.

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

--End--

Installing the Backup Security Service and Network Routing Service

Optionally, use the following procedure to install the Backup Security Service and Network Routing Service (NRS).

Procedure steps

Step	Action
1	Log on to the server using the nortel account.
2	Insert the NRS CD-ROM in the CD-ROM tray.
3	Enter the appinstall CLI command
4	At the prompt, enter the root account password. The system then prompts you to check the media.
5	Enter **Y** to check the media, or **N** to proceed without checking the media, and then press **Enter**. The Application installation window appears.
6	From the **Application installation** window select **2** to install the Backup Security Service with NRS. The appropriate packages are installed to the hard drive. The Solid server window appears.
7	On the **Solid server configuration** page, type the option number of the Solid server to install, and then press **Enter**.
8	Press **Enter** to continue. The Solid server configuration confirmation page appears.
9	Confirm the server selection by selecting **Yes**, or return to the Solid server configuration window by selecting **No**.
10	Press **Enter** to continue. The Primary Security Service server TLAN IP address page appears.
11	Enter the IP address of the TLAN network interface Primary Security Service server.
12	Type **yes** to confirm the TLAN IP address is correct. The Primary Security Service server Fully Qualified Domain Name (FQDN) appears.
13	Enter the FQDN of the Primary Security Service server.
14	Type **Yes** to confirm the FQDN is correct.

ATTENTION
Ensure that the Primary Security Service is running at this point.

The Primary Security Service fingerprint page appears.

15 Type **Yes** to verify the Primary Security Service fingerprint. The nortel password page appears.
You must know the password for the nortel account on the Primary Security Service server to proceed. The installation stops if you do not know this password.

16 The nortel password page appears. Type the password of the nortel account, and then press Enter. The connection to the Primary Security Service server is complete.
The installation takes approximately thirty minutes to complete. After the installation is complete the disk automatically ejects from the drive and a summary of the installation appears.
For more information about NRS, see *Network Routing Service Installation and Commissioning* (NN43001-564).

--End--

Installing the Network Routing Service with ECM joining an existing secure network

Use the following procedure to install the Network Routing Service with ECM joining an existing secure network.

Procedure steps

Step	Action
1	Log on to the server using the nortel account.
2	Insert the NRS CD-ROM in the CD-ROM tray.
3	Enter the appinstall CLI command.
4	At the prompt, enter the root account password. The system then prompts you to check the media.
5	Enter **Y** to check the media, or **N** to proceed without checking the media. The Application installation page appears.
6	From the Application installation window, select **3** to install the Network Routing Service with ECM joining an existing secure network. The appropriate packages are installed to the hard drive. The Solid server configuration window appears.
7	On the **Solid server configuration** page, type the number of the Solid server to install.
8	Press **Enter** to continue. The Solid server configuration confirmation page appears
9	Confirm the server selection by selecting **Yes**, or return to the Solid server configuration window by selecting **No**.
10	Press **Enter** to continue. The Primary Security Service server TLAN IP address page appears.
11	Enter the IP address of the TLAN network interface Primary Security Service server. Type **Yes** to confirm the TLAN IP address is correct. The Primary Security Service server Fully Qualified Domain Name (FQDN) appears.
12	Enter the FQDN of the Primary Security Service server.
13	Type **Yes** to confirm the FQDN is correct.

ATTENTION
Ensure that the Primary Security Service is running at this point.

The Primary Security Service fingerprint page appears.

14 Type **Yes** to verify the Primary Security Service fingerprint.
The nortel password page appears.

15 Enter the password of the nortel account.
You must know the password for the nortel account on the Primary Security Service server. The Installation stops if you do not know this password.
The connection to the Primary Security Service server is complete. The installation takes approximately thirty minutes to complete. After the installation is complete the disk automatically ejects from the drive and a summary of the installation appears.
For more information about NRS, see *Network Routing Service Installation and Commissioning* (NN43001-564).

--End--

Installing the Primary Security Service and Element Manager

Use the following procedure to install the Primary Security Service and Element Manager.

Procedure steps

Step	Action
1	Log on to the server command line using the nortel account.
2	Insert the MGMT DVD in the DVD tray.
3	Enter **appinstall**.
4	At the prompt, enter the root account password. The system then prompts you to check the media.
5	Enter **Y** to check the media, or **N** to proceed without checking the media, and then press Enter. The Application Installation page appears.
6	From the **Application installation** page, select **1** to install the Primary Security Service with Element Manager. The appropriate packages are installed to the hard drive. The Solid server configuration window appears.
7	On the **Solid server configuration** page, enter the number of the Solid server to install. The Solid server configuration confirmation page appears.
8	Enter **Yes** to confirm the Solid server selection, or enter **No** to return to the Solid server configuration window. The Private CA certificate window appears.
9	Press **Enter** to display a series of location prompts. Type a response for each of these categories: • Country • State or Province • Location • Organization Name • Organization Unit
10	Press **Enter** to continue. The Private CA Certificate confirmation window appears.
11	Verify that the common name information is correct. Enter **Yes** if the correct common name information appears, or **No** if the information is not correct.

If you entered yes, the installation finishes and the system creates the CA certificate. If you entered no, edit the information as required and repeat the step.
The installation takes approximately thirty minutes to complete. After the installation is complete the disk automatically ejects from the drive and a summary of the installation appears.
For more information about Element Manager, see *Element Manager System Reference—Administration* (NN43001-632).

--End--

Installing the Backup Security Service and Element Manager

Use the following procedure to install the Secondary Security Service and Element Manager. This procedure is optional.

Procedure steps

Step	Action
1	Log on to the server using the nortel account.
2	Insert the MGMT DVD in the DVD tray.
3	Enter the appinstall CLI command.
4	At the prompt, enter the root account password. The system then prompts you to check the media.
5	Enter **Y** to check the media, or **N** to proceed without checking the media, and then press Enter. The Application Installation page appears.
6	From the Application installation window select **2** to install the Backup Security Service with Element Manager. The appropriate packages are installed to the hard drive. The Solid server configuration window appears.
7	On the Solid server configuration page, type the number of the Solid server to install.
8	Press **Enter** to continue. The Solid server configuration confirmation page appears.
9	Type **Yes** to confirm the Solid server selection, or type **No** to return to the Solid server configuration window.
10	Press **Enter** to continue. The Primary Security Service server TLAN IP address page appears. Enter the IP address of the TLAN network interface Primary Security Service server.
11	Type **Yes** to confirm the TLAN IP address is correct or type **No** to return to the Primary Security Service server TLAN IP address page.
12	Press **Enter** to continue. The Primary Security Service server Fully Qualified Domain Name (FQDN) page appears.
13	Enter the FQDN of the Primary Security Service server.

14 Type **Yes** to confirm the FQDN is correct or type **No** to return to the Primary Security Service server Fully Qualified Domain Name page.

15 Press **Enter** to continue.

ATTENTION
Ensure that the Primary Security Service is running at this point.

The Primary Security Service fingerprint page appears.

16 Type **Yes** to verify the Primary Security Service fingerprint.

17 The nortel password page appears. Type the password of the nortel account, and then press **Enter**.
The connection to the Primary Security Service server is complete and the installation finishes. The installation takes approximately thirty minutes to complete. After the installation is complete the disk automatically ejects from the drive and a summary of the installation appears.
You must know the password for the nortel account on the Primary Security Service server. Installation stops if you do not know this password.
For more information about Element Manager, see *Element Manager System Reference—Administration* (NN43001-632).

--End--

Configuring the Primary and Secondary NRS Server Settings

Use the following procedure to configure the Primary and Secondary NRS Server Settings.

ATTENTION
Configure the primary and secondary NRS servers one by one. You must log on to the specific (either primary or secondary) server to configure it. For more information, see *Nortel Communication Server 1000 Network Routing Service Installation and Commissioning* (NN43001-564).

Procedure steps

Step	Action
1	In the NRS Manager select **System**, **NRS Server**. The NRS Server Web page appears.
2	In the **Server Configuration** pane of the **NRS Server** web page, click **Edit**. The Edit Server Configuration web page appears.
3	Configure the NRS Server settings as follows: • **Host name**: Enter the Primary server host name in the box. The host name must be alphanumeric and can be up to 20 characters in length. • **Primary TLAN IP address**: Enter the IP address of the Primary NRS (that is, the TLAN network interface IP address) in the box. The default is 0.0.0.0. • **Secondary TLAN IP address**: Enter the IP address of the Secondary NRS (that is, the TLAN network interface IP address), in the box. The default is 0.0.0.0. • **Secondary server host name**: Enter the Secondary server host name in the box. • **Control priority**: Enter a value for the control priority in the box. The Control Priority value is a priority bit setting inside the protocol that determines the signaling routing priority. The range is 0 to 63. The default value is 40. The control priority must be a numeric value. • **Server mate communication port**: Enter a value for the Server mate communication port in the box. The Server mate communication port is numeric and can be up to five digits in length. The range is 0 to 65535. The default port number is 50005.

- **Realm name**: Enter a value for the Realm name in the box. The Realm name is alphanumeric and can be up to 20 characters in length.
- **Server role**: Choose Primary or Secondary from the list.

4 To configure **SIP Server Settings** scroll down to the SIP Server Settings section of the **Edit Server Configuration** Web page, and configure the following:

- Select **Proxy** from the **Mode** list. This step specified the mode of the SIP Server. A SIP Proxy acts as both a server and a client. A SIP Proxy receives requests, determines where to send the requests, and acting as a client on behalf of SIP endpoints passes requests on to another server.
- Enter **`Public name`** for nontrusted networks in the box.
- Enter **`Public number`** for nontrusted networks in the box
- Enable UDP
  - Select the **UDP transport enabled** check box.
  - Enter the Primary server UDP IP in the box.
  - Enter the Primary server UDP port in the box. The UDP port must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port number is 5060.
  - Enter the Secondary server UDP IP in the box.
  - Enter the Secondary server UDP port in the box. The UDP port must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port number is 5060.
  - Enter the UDP maximum transmission unit (MTU) in the box. The MTU is the maximum size of an Ethernet Layer 2 packet going out on the IP network. In this context, MTU is the maximum size of a SIP packet that is sent out on the UDP interface. The default value is 1500 bytes. The maximum value for MTU is 64K. When configuring the MTU, remember that there is a trade-off between packet size and the number of packets that have to be transmitted over the network.

ATTENTION
TCP and TLS are not supported.

5 Click **Save**.
The NRS Server web page reopens.

6 Click **Restart** on the Service Status pane of the NRS Server web page.

--End--

Installing the Element Manager joining an existing secure network

Use the following procedure to install Element Manager.

Procedure steps

Step	Action
1	Log on to the server using the nortel account.
2	Insert the MGMT DVD in the DVD tray.
3	Enter the appinstall CLI command.
4	At the prompt, enter the root account password. The system then prompts you to check the media.
5	Enter **Y** to check the media, or **N** to proceed without checking the media, and press **Enter**. The Application Installation page appears
6	From the Application installation window select **3** to install the Element Manager joining an existing secure network. The appropriate packages are installed to the hard drive. The Solid server configuration window appears.
7	On the Solid server configuration page, type the number of the Solid server to install.
8	Press **Enter** to continue. The Solid server configuration confirmation page appears.
9	Type **Yes** to confirm the Solid server selection, or type **No** to return to the Solid server configuration window.
10	Press **Enter** to continue. The Primary Security Service server TLAN IP address page appears
11	Enter the IP address of the TLAN network interface Primary Security Service server.
12	Type **Yes** to confirm the TLAN IP address is correct or type **No** to return to the Primary Security Service server TLAN IP address page.
13	Press **Enter** to continue. The Primary Security Service server Fully Qualified Domain Name (FQDN) page appears.
14	Enter the FQDN of the Primary Security Service server.

15 Type **Yes** to confirm the FQDN is correct or type **No** to return to the Primary Security Service server Fully Qualified Domain Name page.

16 Press **Enter** to continue.
The Primary Security Service fingerprint page appears.

ATTENTION
Ensure that the Primary Security Service is running at this point.

17 Type **Yes** to verify the Primary Security Service fingerprint.

18 The nortel password page appears. Type the password of the nortel account, and then press **Enter**. You must know the password for the nortel account on the Primary Security Service server. Installation stops if you do not know this password.
The connection to the Primary Security Service server is complete and the installation finishes. The installation takes approximately thirty minutes to complete. After the installation is complete the disk automatically ejects from the drive and a summary of the installation appears.
For more information about Element Manager, see *Element Manager System Reference—Administration* (NN43001-632).

--End--

Patches

Use the information and procedures in this chapter to install the DEP list and individual patches required for Session Initiation Protocol (SIP) Line.

ATTENTION
You must have a Communication Server 1000E system, with CPPM, installed and configured before you begin to install and configure SIP Line.

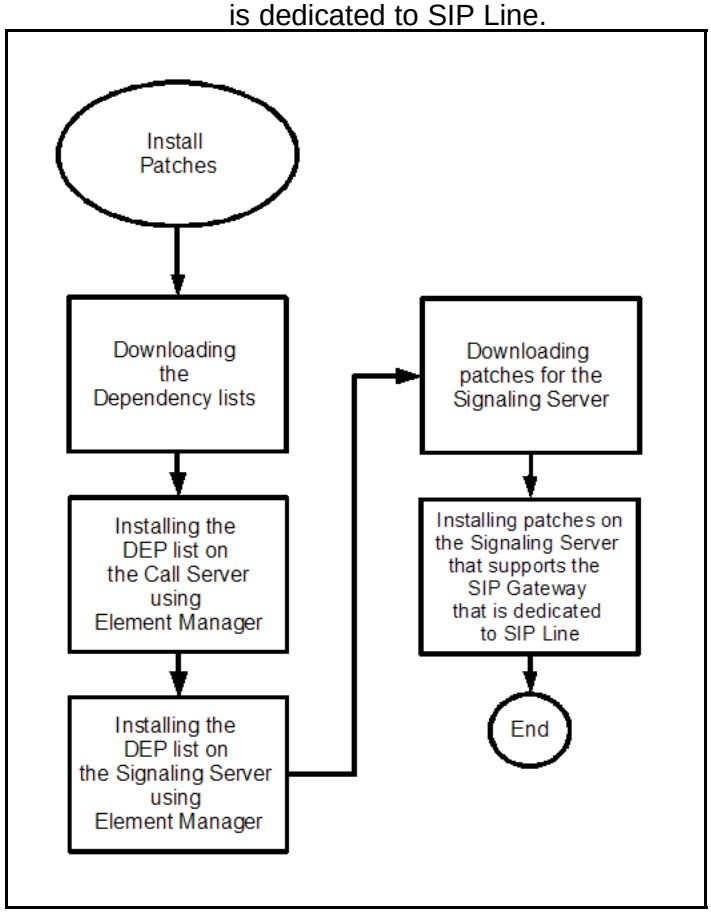
ATTENTION
If you have installed the current CS 1000 DEP list on the Call Server, and on each Signaling Server in your system, you may have installed some of the patches described in this chapter. You need not reinstall a patch you have previously installed.

Use the task flow on the following page to guide you in the order to perform the procedures in this chapter.

Task flow

Install patches

Install patches on the Signaling Server that supports the SIP Gateway that is dedicated to SIP Line.



Install patches navigation

- “Downloading the Dependency lists ” (page 83)
- “Installing the DEP list on the Call Server using Element Manager” (page 85)
- “Installing the DEP list on the Signaling Server using Element Manager” (page 86)
- “Downloading patches for the Signaling Server” (page 87)
- “Installing patches on the Signaling Server” (page 91)

Before you can use SIP Line, you must upgrade your system to the latest version of Communication Server 1000E Release 5.5, and apply the DEP list to the Call Server and to each Signaling Server in your system. Some patches are applied as part of the DEP list, while you must apply others manually. For a list of all the patches required by SIP Line, see Table 2 "Patches required for SIP Line" (page 81). For additional information about using the PEP library and installing patches and DEP lists, see *Matrix Dependency List User Guide*, which you can download from http://www.nortel.com/espl.

Table 2
Patches required for SIP Line

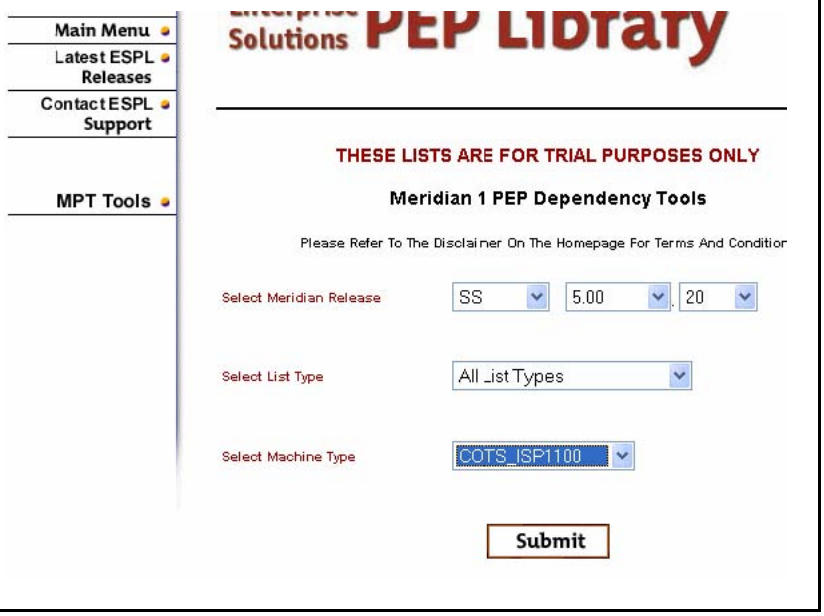
Patch	Install on	Install method	Description
MPLR25583	Call Server	DEP list	Improves Busy treatments.
MPLR25896	Call Server	DEP list	Improves message generation for UEXT SIP3.
MPLR26070	Call Server	DEP list	Improves access restriction checking.
MPLR26142	Call Server	DEP list	Improves access restriction checking.
MPLR26310	Call Server	DEP list	Preserves bandwidth.
MPLR26350	Call Server	DEP list	Enhances error messaging.
MPLR25840	SIP Gateway designated for SIP Line	DEP list	Supports UPDATE to client.
MPLR25886	SIP Gateway designated for SIP Line	DEP list	Improves Message Waiting Indication (MWI) indication for broader client interoperability.
MPLR25894	SIP Gateway designated for SIP Line	DEP list	Enhances MCS-to-SIP Line interworking.
MPLR25993	SIP Gateway designated for SIP Line	DEP list	Supports Address Subscribe requests from the clients.
MPLR26302	SIP Gateway designated for SIP Line	DEP list	Enhances INFO message capabilities.
MPLR26825	Call Server	DEP list	Improves busy status indication.
MPLR26943	SIP Gateway designated for SIP Line	DEP list	Not to display calling name, when calling name presentation is denied for outgoing calls.
MPLR27047	SIP Gateway designated for Trunking	DEP list	Enhances Session Description Protocol (SDP) handling and improves busy status indication.

Patch	Install on	Install method	Description
MPLR27260	SIP Gateway designated for SIP Line	DEP list	Addresses Trunks Pending issue
MPLR25722 Version 5 or higher.	SIP Gateway designated for SIP Line	Load Manually	Binds the SIP client to the Universal Extension.
MPLR25946	SIP Gateway designated for SIP Line	Load Manually	Remove MCDN from outgoing INVITE.
MPLR26327	SIP Gateway designated for SIP Line	Load Manually	Improves client local call forward handling.
MPLR27048	SIP Gateway designated for SIP Line	Load Manually	Supports transfers to other SIP Nodes. Enhances Session Description Protocol (SDP) handling and improves busy status indication.

Downloading the Dependency lists

Use the following procedure to download the Dependency (DEP) list for the Signaling Server and Call Server.

Procedure steps

Step	Action
1	Enter the following address in the Address field of your web browser: **`http://www.nortel.com/espl`**. The **LOG IN** page appears.
2	Enter your user name and password, and click **Log On**. **ATTENTION** To access the Enterprise Solutions PEP Library, you must log on using a Distributor user name and password. The **Enterprise Solutions PEP Library** page appears.
3	Click **Click Here**. The **Main Menu** page appears.
4	Click **Production PEP Dependency Lists**. The **Dependency Tools** page appears. 
5	Use the Job Aid that follows this procedure to select the Release, List Type, and Machine Type. The figure above shows selections relevant to the DEP list for a Signaling Server.
6	Click **Submit**.

7 The **Available PEP Dependency Lists** page appears.

8 Click **Download**.
The **Dependency Lists to Be Added To Zip File** page appears.

9 Scroll down the page until **To Download PEP's In File Format**appears.

10 Next to **To Download PEP's In File Format**, click**Click Here**.

11 A warning appears, which advises you that you must rename the file after downloading it. Click **OK**.
The **File Download** window appears.

12 Click **Save**.
The **Save As** window appears.

13 Select a location in which to store the file, and enter a file name that is eight or fewer characters, does not include any special characters, and has the extension **`.zip`**. For example, **`pp4_450w.zip`**

14 Click **Save**.
The **Download Complete** window appears.

15 Click **Close**.

16 Click **ESPL Home**, and then repeat steps 3 through 14 for each type of device you have in your system.

--End--

Table 3
Job Aid: DEP list selection

Platform	Application	Release	List Type	Machine Type
CPPM (4021)	Call Server	latest available	All list types	CPPM
CPPM-SS	Signaling Server	latest available	All list types	CPPM_SS
HP DL320 G4 and IBM x306m	Signaling Server (vxworks)	latest available	All list types	COTS_ISP1100

Installing the DEP list on the Call Server using Element Manager

Use the following procedure to install the DEP list on the Call Server.

Procedure steps

Step	Action
1	Log on to Element Manager on the Signaling Server.
2	In the navigation pane, click **System > Software > Call Server**.
3	In the **Call Server** pane, click **Dependency Lists**.
4	In the **Dependency List Settings** pane, click Browse. The Load File window appears.
5	Browse to the folder where you saved the DEP list, and select the DEP list zip file.
6	Click **Open**.
7	Click **Load and Activate**. The DEP list is transferred to the Call Server.

--End--

Installing the DEP list on the Signaling Server using Element Manager

Use the following procedure to install the DEP list on the Signaling Servers.

Procedure steps

Step	Action
1	Log on to Element Manager on the Signaling Server.
2	Click **IP Telephony > Software > Servers and Media Cards**. The **Servers and Media Cards** page appears.
3	Select the **Dependency List** radio button. The DEP list contents appear.
4	Click **Signaling server > ITG-Pentium > Media Card**. The **Signaling Server** option is selected by default.
5	Click Browse. The Load File window appears.
6	Browse to the folder where you saved the DEP list, and select the DEP list zip file.
7	Click **Load**.
8	Select the check boxes for the elements you want to patch.
9	Click **Transfer**. The DEP list is transferred to each of the elements you selected in step 8.

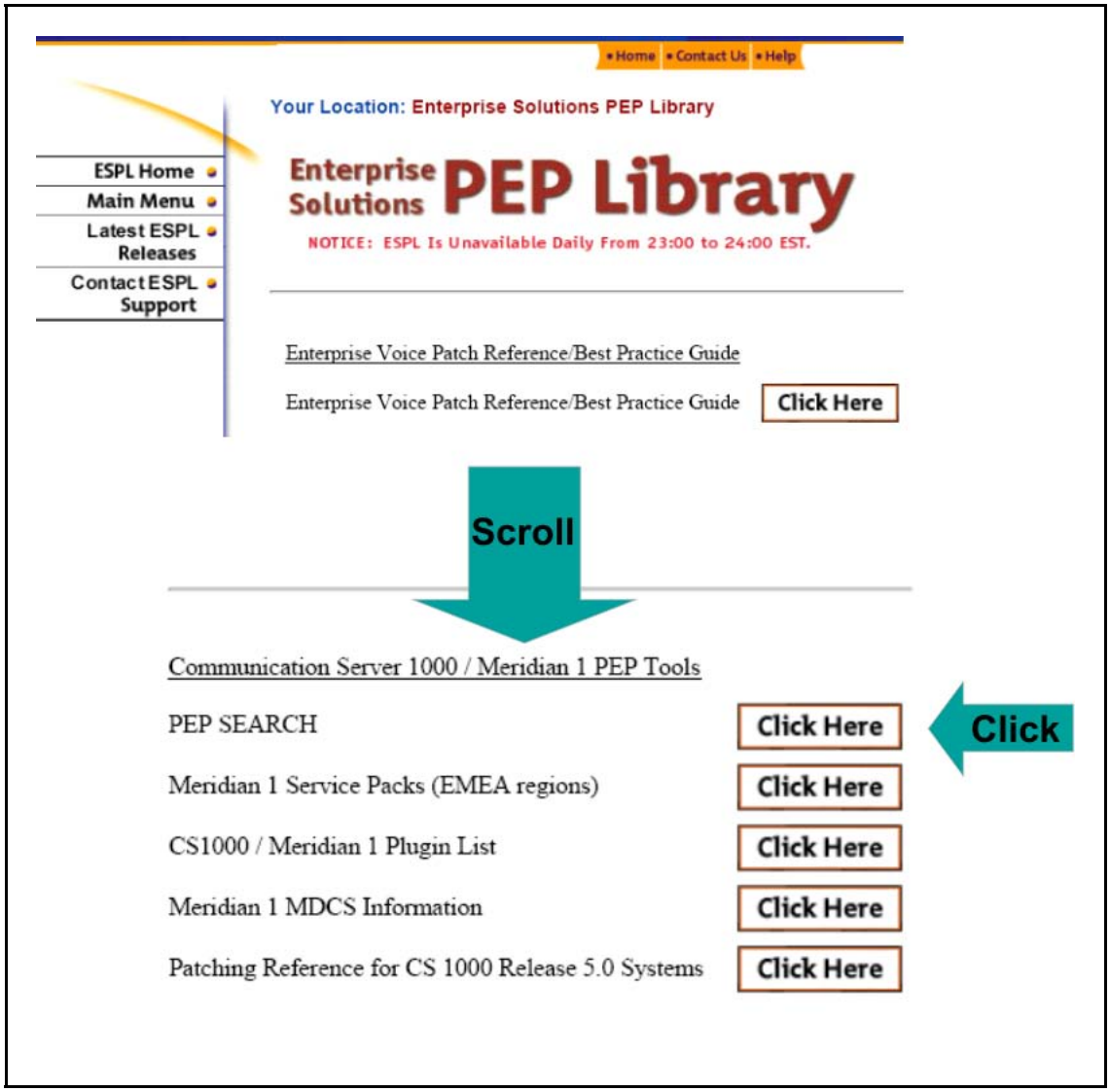
--End--

Downloading patches for the Signaling Server

Use the following procedure to download the patches for the Signaling Server that supports the SIP Gateway that is dedicated to SIP Line. For a list of the patches required to provide SIP Phone support on the Signaling Server, see the Job aid that follows the procedure.

Procedure steps

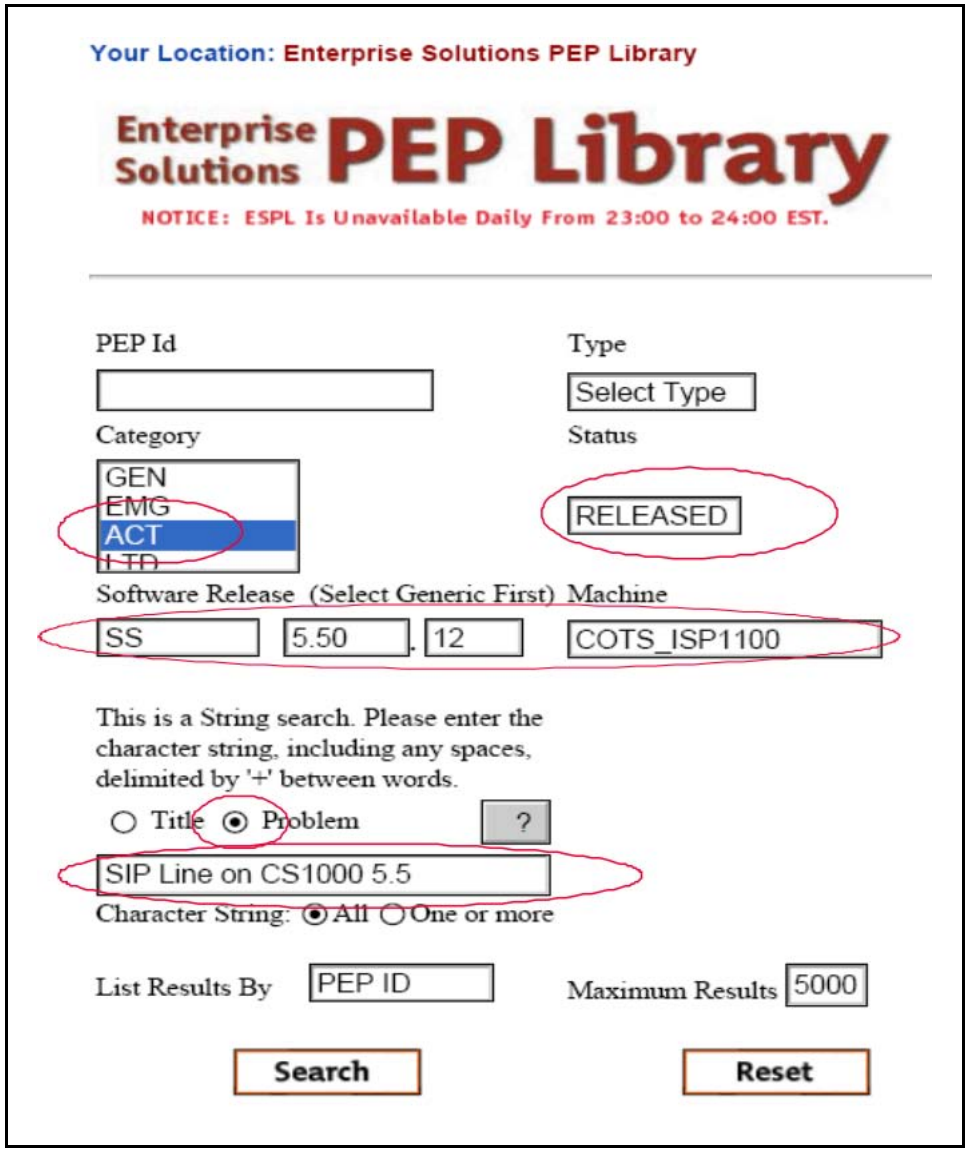
Step	Action
1	Enter the following address in the Address field of your web browser: **`http://www.nortel.com/espl`**. The **LOG IN** page appears.
2	Enter your user name and password, and click **Log On**. **ATTENTION** To access the Enterprise Solutions PEP Library, you must log on using a Distributor user name and password. The **Enterprise Solutions PEP Library** page appears.
3	Click **Click Here**. The **Main Menu** page appears.
4	Scroll down, until the following option appears: **`Communication Server 1000 / Meridian 1 PEP Tools PEP SEARCH`**
5	Next to **PEP SEARCH**, click **Click Here**.



The **PEP Search** page appears.

6 Select the following:

- On the **Category** menu, choose **ACT**.
- In the **Status** field, enter **RELEASED**.
- In the **Software Release (select Generic First) Machine** fields, enter **SS**, **5.50**, **12**, and **COTS_ISP1100**.
- Select the **Problem** radio button.
- In the **Character String** field, enter **SIP Line on CS1000 5.5** .



7 Click **Search**.
A list of the applicable patches appears:

- MPLR27048
- MPLR25722
- MPLR26327
- MPLR25946

These patch numbers are correct at the time of writing. They can become obsolete, and the PEP Library can report updated patch numbers.

8 Select all four of the patches.

9 Click **Submit**.

--End--

Table 4
Job aid: patch descriptions

Patch	Description
MPLR25722	Binds the SIP client to the Universal Extension.
MPLR25946	Remove MCDN from outgoing INVITE.
MPLR26327	Improves client local call forward handling.
MPLR27048	Supports transfers to other SIP Nodes. Enhances Session Description Protocol (SDP) handling and improves busy status indication.
Note: These patch numbers are correct at the time of writing. They can become obsolete, and the PEP Library can report updated patch numbers.	

If you cannot access the Performance Enhancement Packages (PEP) Library, or cannot identify the PEPs for SIP Line, contact your next level of support.

Installing patches on the Signaling Server

Use the following procedure to install patches on the Signaling Server that supports the SIP Gateway that is dedicated to SIP Line.

Prerequisites

- Ensure that you have a Communication Server 1000E Release 5.5 system with CPPM call processor.
- If you have an existing Communication Server 1000E system, ensure that is has been upgraded to 5.5.0.12 (or later). For more information, see the instructions in *Communication Server 1000E Software Upgrades* (NN43041-458) before you install the patches described in this section.
- Load the latest DEP list on the call server and on each signaling server in your Communication Server 1000E system.

Procedure steps

Step	Action
1	Log on to Element Manager using a System password level 2 account that has PDT access.
2	In the System branch of the Element Manager navigation tree, click **System**, **Software**, **Servers, Media Cards PEPs**. The Servers and Media Cards page appears.
3	Select the patch MPLR27047, and click **Unload**.
4	In the **PEP Settings** pane, click **Browse**.
5	Navigate to and select the first patch file, and then click **Load**.
6	Click the right arrow (**-->>**) to transfer the file into the Pep Bin.
7	Repeat steps 4 to 6 for each patch file, until you have added each of the following patches: • MPLR25722 • MPLR25946 • MPLR26327 • MPLR27048

8 In the Pep Bin pane, click **Load and Activate**.
Progress messages appear in the lower part of the window.

--End--

Configuration

Use the information and procedures in this chapter to configure Session Initiation Protocol (SIP) Line.

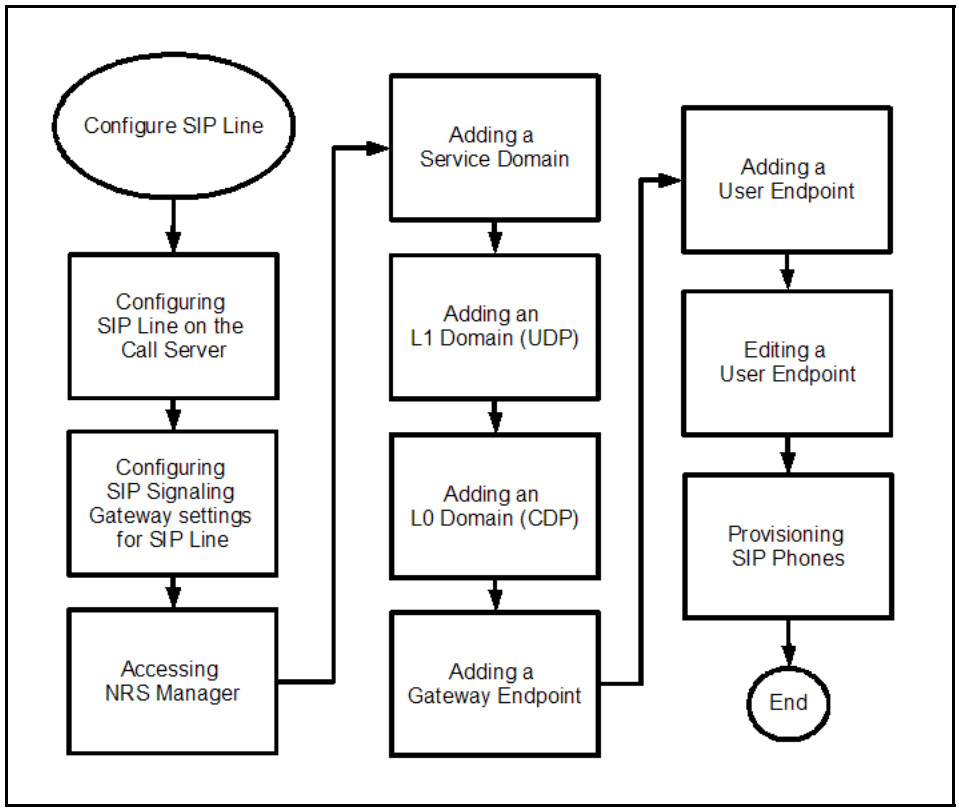
ATTENTION
You must have a Communication Server 1000E system, with CPPM, installed and configured before you begin to install and configure SIP Line.

Use the task flow on the following page to guide you in the order to perform the procedures in this chapter.

Task Flow

Configure SIP Line

Configure SIP Line.



Configure SIP Line navigation

Configuring SIP Line on the Call Server

Use the following procedure to configure SIP Line on the Call Server.

Prerequisites

Ensure that the packages listed in Table 5 "Required packages" (page 95) are enabled. For more information about using LD 22 to verify what packages are enabled on your system, see *Software Input/Output Administration* (NN43001-611).

Table 5
Required packages

Package mnemonic	Package number	Package description	Package type (new or existing or dependency)
SIP_PKG	406	SIP Gateway Package	Existing
SIP_LINE_NT_PKG	415	Nortel SIP Line Package	Existing
SIP_LINE_3P_PKG	416	Third Party SIP Line Package	Existing

Procedure steps

Step	Action
1	Log on to the call server command prompt using a PWD2 account.
2	At the LD 17 prompt, configure IP-D channel: • At the REQ prompt, enter **CHG**. • At the TYPE prompt, enter **ADAN**. • At the ADAN prompt, enter **<NEW/CHG> dch <dch#>**. • At the CTYP prompt, enter **DCIP**. • At the IFC prompt, enter **SL1**. • At the RCAP prompt, enter **MWI ND2**.
3	At the LD 16 prompt, configure the SIP Route: • At the REQ prompt, enter **<NEW/CHG>**. • At the TYPE prompt, enter **RDB**. • At the CUST prompt, enter **<custNum>**.

- At the ROUT prompt, enter **<Route#>**.
- At the TKTP prompt, enter **TIE**.
- At the VTRK prompt, enter **YES**.
- At the ZONE prompt, enter **<Zone#>**
- At the PCID prompt, enter **SIP**.
- At the NODE prompt, enter **<Node#>**.
- At the ISDN prompt, enter **YES**.
- At the MODE prompt, enter **ISLD**.
- At the DCH prompt, enter **<DCH#>**.
- At the IFC prompt, enter **SL1**.
- At the ICOG prompt, enter **IAO**.
- At the ACOD prompt, enter **<Acod#>**.
- At the SIGO prompt, enter **ESN5**.

4 At the LD 14 prompt, configure trunks for the SIP Route:

- At the REQ prompt, enter **<NEW/CHG>**.
- At the TYPE prompt, enter **IPTI**.
- At the TN prompt, enter **TN**.
- At the XTRK prompt, enter **VTRK**.
- At the CUST prompt, enter **<CustNum>**.
- At the RTMB prompt, enter **<routeNummid>**.
- At the CHID prompt, enter **<chid>**.
- At the SUPN prompt, enter **YES**.
- At the CLS prompt, enter **DTN**.
- At the STRO prompt, enter **WNK**.
- At the STRI prompt, enter **WNK**.

5 At the LD 11 prompt, configure SIP Line Universal Extensions (UEXT):

- At the REQ prompt, enter **<NEW/CHG>**.
- At the TYPE prompt, enter **UEXT**.
- At the TN prompt, enter **<tn>**.
- At the CUSTprompt, enter **<custnum>**.
- At the UXTY prompt, enter **<SIPN/SIP3>**.

- At the KEY prompt, enter **<0 SCR DN>**.
- At the KEY prompt, enter **<1 HOT P x y>**.

--End--

Variable definitions table

Variable	Definition
<0 SCR DN>	A primary DN key. MADN is not supported.
<1 HOT P x y>	The HOT P key number to extend the call out to SIP Proxy Server, and then SIP client. The HOT P DN is the target DN and must be the same as the level zero DN on the SIP Proxy Server. x – length of HOT P DN y– HOT P DN. Ensure that this DN is routed to the SIP trunk linked to the designated SIP Gateway.
<Acod#>	Access code for the specified route.
<chid>	Channel ID.
<custNum>	The customer number.
<DCH#>	The IP D-channel (DCH).
<NEW/CHG>	Either NEW or CHG.
<Node#>	The Node number.
<Route#>	The Route number.
<routeNum mid>	Route number and member number.
<SIPN/SIP3>	Either SIP Nortel (SIPN) or SIP third-party (SIP3), depending on the client type.
<tn>	The Terminal Number (TN).
<Zone#>	The Zone number.

Configuring SIP Signaling Gateway settings for SIP Line

Use the following procedure to configure the SIP Gateway designated for SIP Line. Configure the SIP Gateway designated for SIP Line as you normally configure a SIP Gateway, with one exception; you must ensure the SIP proxy is pointing to the SIP Proxy Server you designated for SIP Line.

Procedure steps

Step	Action
1	Log on to Element Manager.
2	In the Element Manager **System, IP Network** menu, choose **Nodes: Servers, Media Cards**. The Node Configuration Web page appears.
3	Click **Edit**. The Edit Web page dialog box appears.
4	Select **SIP Gateway Settings** to expand the section.
5	Complete the following for the Primary server: • **Security Policy**: Choose **TLS Disabled**. • **Primary Proxy/Re-direct IP address**: Enter the TLAN network interface IP address of the SIP Proxy Server you designated for SIP Line. • **Primary Proxy/Re-direct IP Port**: Enter the port number for the SIP Proxy Server you designated for SIP Line. • **Primary Proxy Supports Registration**: The Primary Proxy Supports Registration check box tells the SIP Gateway whether the primary NRS (SIP Redirect Server) supports registration. If the check box is selected, then the SIP Gateway must register with the primary NRS. If the check box is cleared, then the SIP Gateway does not register with the primary NRS. Only the UDP transport protocol is supported. • **Secondary Proxy/Re-direct IP address**: Enter the TLAN network interface IP address of the Secondary SIP Redirect Server or the MCS 5100 Proxy Server (if configured). • **Secondary Proxy/Re-direct IP Port**: Leave the default port value as 5060 for the Secondary SIP Redirect Server or the MCS 5100 Proxy Server (if configured).

- **Secondary Proxy Supports Registration**: The Secondary Proxy Supports Registration check box tells the SIP Gateway whether the secondary NRS (SIP Redirect Server) supports registration. If the check box is selected, then the SIP Gateway must register with the secondary NRS. If the check box is cleared, then the SIP Gateway does not register with the secondary NRS.
  Only the UDP transport protocol is supported.
- **The Secondary CDS Proxy or Re-direct** server flag is not used in this release.

6 Click **Save and Transfer.**

--End--

Accessing NRS Manager

Use the following procedure to access NRS Manager.

Procedure steps

Step	Action
1	On the SIP Gateway that is designated for SIP Line, log on to Element Manager using an Admin account.
2	Click **Dialing and Numbering Plans, Network Routing Service** from the navigation tree. The Network Routing Service (NRS) web page appears.
3	Enter the IP address of the NRS in the **NRS IP Address** box.
4	Click **Next**. The Network Routing Service login window appears.
5	Enter a **User ID** and **Password** that is valid on the NRS Manager.
6	Click **Login** to access the NRS Manager.

--End--

Adding a Service Domain

Use the following procedure to add a Service Domain. The Service Domain is a building block of the routable Session Initiation Protocol (SIP) Uniform Resource Indicator (URI), and represents the service domain name field in the URI.

Procedure steps

Step	Action
1	Click the **Configuration** tab on the NRS Manager tool bar. The first time you open the Configuration page, a dialog box appears indicating the status of the active and standby database. Click **OK**. Ensure that **Standby DB view** is selected. The Service Domains web page appears.
2	Click **Add**.... The Add Service Domain web page appears.
3	Enter a Domain name for the Service Domain in the box. For example, enter **`myServiceProvider.com`**.
4	Enter a Domain description for the Service Domain in the box.
5	Click **Save**.
6	The Service Domains web page appears, showing the newly added Service Domain.

--End--

Adding an L1 Domain (UDP)

Use the following procedure to add a Level 1 (L1) Domain. The L1 Domain is a building block of the phone context for private addresses, and is the phone context root.

Procedure steps

Step	Action
1	Click the **Configuration** tab on the NRS Manager toolbar.
2	Ensure the Standby DB view is selected.
3	In the navigation tree, click **L1 Domains (UDP)**. The L1 Domains (UDP) web page appears.
4	In the menu, choose the **Service Domain** in which to add the new L1 subdomain.
5	Optionally, click **Show** to display a list of configured L1 Domains for the selected Service Domain.
6	Click **Add**.... The Add L1 Domain web page appears.
7	Enter the Domain name of the L1 Domain in the box. The name must be alphanumeric and can be up to 30 characters in length. For example, enter **`myCompany.com`**.
8	Enter the Domain description in the box. The description can include any character except single quotes and can be up to 120 characters in length.
9	From the Endpoint authentication enabled list, select **Authentication on** or **Authentication off** . If you selected Authentication on, then all endpoints require authentication.
10	If you selected Authentication on, enter the Authentication password in the box. The password must be alphanumeric and up to 30 characters in length.
11	Enter the E.164 country code in the box. The code must be numeric and can be up to seven characters in length.
12	Enter the E.164 area code in the box. The code must be numeric and can be up to seven characters in length.

13 Enter the E.164 international dialing access code in the box.
The code must be numeric and can be up to seven characters in length.

14 Enter the E.164 national dialing access code in the box.
The code must be numeric and can be up to seven characters in length.

15 Enter the E.164 local (subscriber) dialing access code in the box.
The code must be numeric and can be up to seven characters in length.

16 Enter the Private L1 domain (UDP location) dialing access code in the box.
The code must be numeric and can be up to seven characters in length.

17 Enter the Special number in the box.
The number must be numeric and can be up to 30 characters in length.

18 Enter the Emergency service access prefix in the box.
The number must be numeric and can be up to 30 characters in length.

19 Click **Save**.
The L1 Domains (UDP) web page appears, showing the newly added L1 domain within the Service Domain.

--End--

Adding an L0 Domain (CDP)

Use the following procedure to add a Level 0 (L0) Domain. The L0 Domain is a building block of the phone context for private addresses.

Procedure steps

Step	Action
1	Click the **Configuration** tab on the NRS Manager toolbar.
2	Ensure the **Standby DB view** is selected.
3	In the navigation tree, click **L0 Domains (CDP)**. The L0 Domains (CDP) web page appears.
4	In the left menu, choose the **Service Domain** in which to add the new L0 subdomain.
5	Click **Add**.... The Add L0 Domain web page appears.
6	Enter the Domain name of the L0 Domain in the box. The name must be alphanumeric and can be up to 30 characters in length. For example, enter **`myCdpDomain.com`**.
7	Enter the Domain description in the box. The description can include any character except single quotes and can be up to 120 characters in length.
8	In the **Endpoint authentication enabled** menu, choose **Not Configured, Authentication on** or **Authentication off** . If you selected Authentication on, then all endpoints require authentication.
9	If you selected Authentication on, enter the Authentication password in the box. The password must be alphanumeric and up to 30 characters in length.
10	Enter the E.164 country code in the box. The code must be numeric and can be up to seven characters in length.
11	Enter the E.164 area code in the box. The code must be numeric and can be up to seven characters in length.
12	Enter the Private unqualified number label in the box. The label must be alphanumeric and can be up to 30 characters in length. The first character in the label must be alphabetic.

13 Enter the E.164 international dialing access code in the box.
The code must be numeric and can be up to seven characters in length.

14 Enter the E.164 national dialing access code in the box.
The code must be numeric and can be up to seven characters in length.

15 Enter the E.164 local (subscriber) dialing access code in the box.
The code must be numeric and can be up to seven characters in length.

16 Enter the Private L1 domain (UDP location) dialing access code in the box.
The code must be numeric and can be up to seven characters in length.

17 Enter the Special number in the box.
The number must be numeric and can be up to 30 characters in length.

18 Enter the Emergency service access prefix in the box.
The number must be numeric and can be up to 30 characters in length.

19 Enter the Special number label in the box.
The label must be alphanumeric and can be up to 30 characters in length. The first character in the label must be alphabetic.

20 Click **Save**.
The L0 Domains (CDP) web page appears, showing the newly added L0 domain.

--End--

Adding a Gateway Endpoint

Use the following procedure to add a Gateway Endpoint.

Procedure steps

Step	Action
1	Click the **Configuration** tab on the NRS Manager toolbar.
2	Ensure that **Standby DB view** is selected.
3	Click **Gateway Endpoints** in the navigation tree. The Gateway Endpoints web page appears. The Gateway Endpoints web page has three menus: configured Service Domains, L1 Domains, and L0 Domains.
4	Choose the **Service Domain**, the **L1 Domain**, and **L0 Domain** from the respective menus.
5	Click **Add**.... The Add Gateway Endpoint web page opens,
6	In the **Endpoint name** field, enter the same name configured for **SIP GW Endpoint Name** in **Element Manager**, **System**, **IP Network**, **Nodes: Servers, Media Cards**, **Select Signaling Server**. The name must be alphanumeric and can be up to 30 characters in length.
7	Select the **Trust Node** check box.
8	Enter a description of the endpoint in the **Endpoint description** box. The description must be alphanumeric and can be up to 120 characters in length.
9	From the **Endpoint authentication** menu, choose one of the following three options: • **Not configured:** If this option is selected, then the gateway endpoint uses the L1 or L0 Authentication (if L1 or L0 authentication is enabled). • **Authentication off:** If this option is selected, then authentication is off for this gateway endpoint even if L1 or L0 authentication is enabled. • **Authentication on:** If this option is selected, then authentication is on for this gateway endpoint and the authentication overrides the L1 or L0 authentication (if it is enabled).

10 If you selected **Authentication on** in step 9, enter the Authentication password in the box.
The password must be alphanumeric and can be up to 30 characters in length.

11 Enter the E.164 country code in the box.
The code must be numeric and can be up to seven characters in length.

12 Enter the E.164 area code in the box.
The code must be numeric and can be up to seven characters in length.

13 Enter the E.164 international dialing access code in the box.
The code must be numeric and can be up to seven characters in length.

14 Enter the E.164 national dialing access code in the box.
The code must be numeric and can be up to seven characters in length.

15 Enter the E.164 local (subscriber) dialing access code in the box.
The code must be numeric and can be up to seven characters in length.

16 Enter the Private L1 domain (UDP location) dialing access code in the box.
The code must be numeric and can be up to seven characters in length.

17 Enter the Private special number 1 in the box.
The number must be numeric and can be up to 30 characters in length.

18 Enter the Private special number 2 in the box.
The number must be numeric and can be up to 30 characters in length.

19 Select IP Version 4 from the Static endpoint address type list. 21
Enter the Static endpoint address in the box.

20 Enter the Static endpoint address in the box.
The Static endpoint address is the Node IP address of the Signaling Server. If a third-party gateway is being used, then it is the IP address of the gateway.

21 Configure SIP support as follows:

- Select one of the following three options from the SIP Support type menu.

— **SIP not supported**

— **Static SIP endpoint**

— **Dynamic SIP endpoint**

- From the **SIP transport** menu, choose **UDP**.
- Enter a port number in the SIP port box. The value must be numeric and can be up to five digits in length. The range is 0 to 65535. The default port number is 5060.

If a SIP Gateway Endpoint is configured with a SIP Support type of Dynamic SIP endpoint, then NRS Manager displays Endpoint Dynamic Registration Information for SIP after the SIP Gateway registers with the NRS.
Endpoint Dynamic Registration Information includes the following: SIP IP, Registration expiry time, User agent, and Preference.
The SIP Endpoint Dynamic Registration Information web page appears only when NRS Manager is in Active DB view. The detailed dynamic registration information also appears only inside the Gateway Endpoint web page.

22 Select the **Network Connection Server is enabled** check box if this Gateway Endpoint supports the Network Connection Server for branch office or Survivable Remote Gateway user redirection to the main office, Virtual Office, or Geographic Redundancy.

23 Click **Save**.
The Gateway Endpoints web page appears, showing the newly added sipGWSite1 endpoint.

24 Optionally, click **Add**... and repeat steps 6 to step 23 to add additional gateway endpoints.

--End--

Adding a User Endpoint

Use the following procedure to add a user endpoint.

Procedure steps

Step	Action
1	In the NRS Manager navigation tree, choose **Numbering Plans**, **Endpoints**. The Endpoints web page opens.
2	Ensure **Standby database** is selected.
3	On the menu, choose a **Service Domain**, an **L1 Domain** and an **L0 Domain** from the respective lists.
4	Click the **User Endpoints** tab. A list of configured User Endpoints appears in the Endpoints pane.
5	Click **Add**.... The Add User Endpoint web page appears.
6	In the **User name** field, enter the DN of the endpoint, which must be the same as the key 0 DN value that you enter when you configure UEXT in the Call Server. The endpoint user name must be alphanumeric and can be up to 30 characters in length. The user name, together with the Service Domain names, becomes a string that is used to build the user's SIP URI, for example: [username]@[service_domain_name]. The SIP URI is used during SIP Phone registration. The user name is used by the SIP authentication procedures.
7	Enter the **User endpoint description**. The endpoint description must be alphanumeric, can include any character except single quotes, and can be up to 120 characters in length.
8	Select the **Trust Node:** check box.
9	In the Tandem gateway endpoint name field, enter the name of the SIP Gateway Signaling Server that you deployed to support SIP Line. The name must be alphanumeric and can be up to 30 characters in length. All calls originating from this User Endpoint are forwarded to the tandem gateway endpoint, which then routes the calls to the appropriate destinations. Tandem routing is useful for generating Call Records for originating User Endpoint calls.
10	In the L0 directory number (DN) field, enter the **HOT P DN** that you configured for the UEXT on the Call Server. The DN must be numeric and can be up to 30 digits in length.

For example, `5000`. The DN is the user's DN. That is, the CDP number.

11 Enter the **L1 directory number (DN)** prefix.
The DN prefix must be numeric and can be up to eight digits in length.
An example is 343. The L1 DN prefix together with the L0 DN creates the user's DN, which is unique within the parent L1 Regional Domain. That is, the UDP number. For example, `3435000`.
L1 domain prefix + L0 DN = User's DN 343 + 5000 = 3435000.

12 Enter the **E.164 local directory number (DN)** prefix.
The DN prefix must be numeric and can be up to eight digits in length.
An example is 967. The E.164 local DN prefix is the location code. The E.164 local prefix, together with the L0 DN, creates the user's E.164 Local (subscriber) DN. For example, `9675000`.
E.164 local prefix + L0 DN = User's E.164 Local (subscriber) DN 967 + 5000 = 9675000.

13 Enter the **E.164 area code**.
The code must be numeric and can be up to eight digits in length.
For example, `613`. The E.164 area code together with both the E.164 local prefix and L0 DN creates the user's national E.164 National DN. For example, `6139675000`.
E.164 area code + E.164 local prefix + L0 DN = User's E.164 National DN 613 + 967 + 5000 = 6139675000.

14 Enter the **E.164 country code**.
The code must be numeric and can be up to eight digits in length.
An example is 1 (for North America). The E.164 country code, together with the E.164 area code, E.164 local prefix, and L0 DN, creates the user's E.164 International DN. For example, `16139675000`.
E.164 country code + E.164 area code + E.164 local prefix + L0 DN = User's E.164 International DN 1 + 613 + 967 + 5000 = 16139675000.

15 Optionally, choose **Authentication on** from the Authentication enabled list, if you want to enable authentication for this endpoint.

ATTENTION
If you choose to enable Authentication, then you must also enable it on the phone, using the same password. Otherwise the phone cannot function.

16 If you enable authentication, then enter the Authentication password.
The password must be alphanumeric and can be up to 24 characters in length.

17 Click **Save**.
The standby database is updated. The Endpoints web page opens, showing the newly added User Endpoint in the User Endpoints pane.

18 Optionally, click **Add**... to add additional User Endpoints.
You can display a maximum of 100 user endpoints on the User Endpoints web page.
If a User Endpoint is configured, then the supported protocol type is dynamic SIP. NRS Manager displays User Endpoint Dynamic Registration Information after the User Endpoint registers with the NRS.
User Endpoint Dynamic Registration information includes the following: SIP IP, Registration expiry time, User agent, and Preference.
The User Endpoint Dynamic Registration Information appears only when NRS Manager is in Active database mode. Detailed dynamic registration information appears inside the User Endpoints Property web page.

19 In the NRS Manager navigation tree, click **System**, **Database**.
The Database web page appears.

20 Click **Cut over**.
The Cut over command is issued, and the database is placed into a Switched over state.

21 Test the configuration changes.

22 In the NRS Manager navigation tree, click **System**, **Database**.
The Database web page appears.
The Database status is Switched over.

23 Click **Commit**.
The Commit command is issued, and the database is placed into a Committed state.

--End--

Editing a User Endpoint

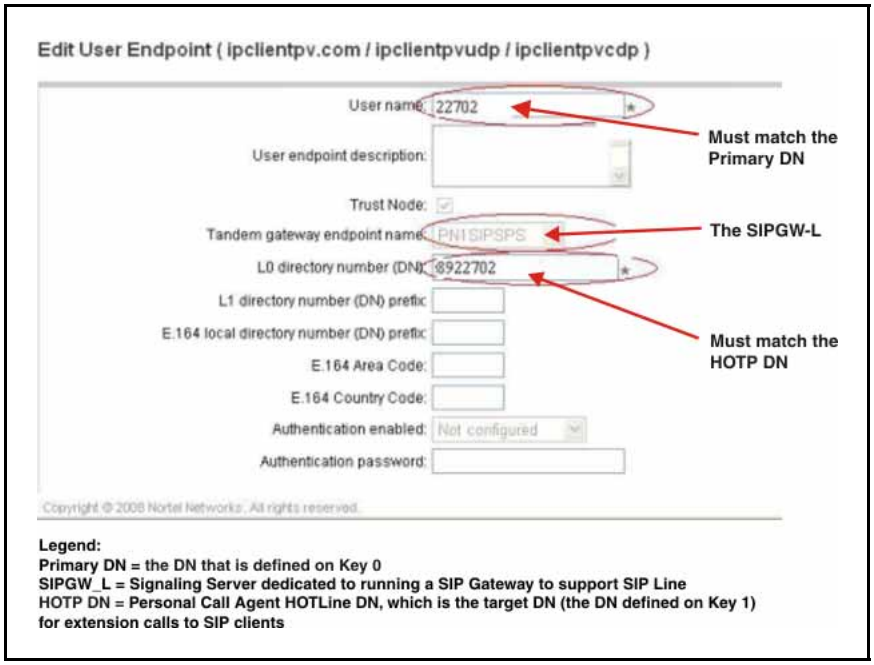
Use the following procedure to edit a User Endpoint.

Procedure steps

Step	Action
1	In the NRS Manager navigation tree, click **Numbering Plans**, **Endpoints**. The Endpoints web page appears.
2	Ensure **Standby database** is selected.
3	On the menus, choose a **Service Domain**, an **L1 Domain** and an **L0 Domain**.
4	Click the **User Endpoints** tab. A list of configured User Endpoints appears in the Endpoints pane. You can sort the User Endpoints in ascending or descending alphabetical order.
5	Click a link in the **ID** column of the Endpoints pane. The Edit User Endpoint web page appears.
6	Modify the fields of the **Edit User Endpoint** web page as appropriate.
7	Click **Save**. The standby database is updated and the Endpoints web page appears.
8	In the NRS Manager navigation tree, click **System**, **Database**. The Database web page appears.
9	Click **Cut over**. The Cut over command is issued, and the database is placed into a Switched over state.
10	Test the configuration changes.
11	In the NRS Manager navigation tree, click **System**, **Database**. The Database web page appears. The Database status is Switched over.
12	Click **Commit**. The Commit command is issued, and the database is placed into a Committed state.

--End--

Figure 10
Job aid: Edit User Endpoint



Provision SIP Phones

For more information about how to configure SIP Line clients, see *Nortel Communication Server 1000 IP Phones Fundamentals* (NN43001-368). SIP Line supports only the clients listed in “Supported clients” (page 21).

This chapter provides some suggested choices for configuring your Nortel SIP Phones. Use the following information to edit the DeviceConfig.dat file for each phone type.

Nortel IP Phone 11xx series

To support SIP Line on the Nortel IP Phone 11xx series of clients, configure them as SIPN UEXT type, then equip the phones with Firmware Version 2.0.10. In the DeviceConfig.dat file, configure the following:

- ENABLE_3WAY_CALL = YES
- ENABLE_UPDATE = YES
- SIP_PING equal to YES
- ENABLE_PRACK YES
- Proxy Checking = NO
- VQMON_PUBLISH NO

For a sample DeviceConfig.dat file, see Table 6 "Sample DeviceConfig.dat file for IP Phone 11xx" (page 114).

Table 6
Sample DeviceConfig.dat file for IP Phone 11xx

```
DNS_DOMAIN opt11c14.com === SIP Line DNS domain
SIP_DOMAIN1 opt11c14.com === SIP Line domain
SIP_DOMAIN2 bell
SIP_DOMAIN3 bell
SIP_DOMAIN4 bell
SIP_DOMAIN5 bell
SERVER_IP1_1 0.0.0.0 === set to 0.0.0.0 to force DNS lookup
SERVER_IP1_2 0.0.0.0 === set to 0.0.0.0 to force DNS lookup
...
SERVER_RETRIES1 2 === keep alive retry counter before switch over
SERVER_RETRIES2 2
…
#****************Device settings******************
FORCE_BANNER YES
BANNER SLG
UPDATE_USERS NO
SIP_PING YES
AUTOLOGIN_ENABLE YES
```

```
# Time configuration
DST_ENABLED YES
TIMEZONE_OFFSET -18000
VMAIL 2300
VMAIL_DELAY 300
AUTO_UPDATE YES
AUTO_UPDATE_TIME 0
DEF_LANG English
MAX_INBOX_ENTRIES 50
MAX_OUTBOX_ENTRIES 50
MAX_REJECTREASONS 5
MAX_PRESENCENOTE 5
MAX_CALLSUBJECT 5
RECOVERY_LEVEL 0
DEF_AUDIO_QUALITY High
DSCP_CONTROL 0
ENABLE_BT YES
#Address book mode - NETWORK, LOCAL, BOTH
ADDR_BOOK_MODE NETWORK
ADMIN_PASSWORD 4321
MAX_IM_ENTRIES 50
ENABLE_3WAY_CALL YES
TRANSFER_TYPE MCS
ENABLE_PRACK YES
ENABLE_UPDATE YES
REDIRECT_TYPE MCS
DISABLE_PRIVACY_UI No
IM_MODE ENCRYPTED
VQMON_PUBLISH NO
VQMON_PUBLISH_IP 47.11.187.125
LISTENING_R_ENABLE YES
LISTENING_R_WARN 1
LISTENING_R_EXCE 1
PACKET_LOSS_ENABLE YES
PACKET_LOSS_WARN 1
PACKET_LOSS_EXCE 1
JITTER_ENABLE YES
JITTER_WARN 1
JITTER_EXCE 1
DELAY_ENABLE YES
DELAY_WARN 1
DELAY_EXCE 1
SESSION_RPT_EN YES
SESSION_RPT_INT 30
MADN_DIALOG YES
MADN_TIMER 15
PROXY_CHECKING NO
```

NORTEL 1535

To configure the Nortel 1535, make the following changes:

- Configure the phone as SIPN UEXT type on the Call Server.
- Configure Proxy type to CS2K in the phone configuration:
  - Select Main Menu, Settings, VoIP Settings, Proxy, Proxy Type.
  - Select CS2K
- Equip the phone with Firmware Version 0.2.76
- Disable the Network Address Translation (NAT) Timer:
  - Select Main Menu, Settings, VoIP Settings, Proxy, NAT Timer, Disable.
- Disable Stun:
  - Select Main Menu, Settings, VoIP Settings, Proxy, STUN, Disable.

Maintenance

Use the information and procedures in this chapter to perform maintenance on your Session Initiation Protocol (SIP) Line deployment.

Viewing the Service Domains

Use the following procedure to view information about Service Domains.

Procedure steps

Step	Action
1	Click the **Configuration** tab on the NRS Manager toolbar.
2	Ensure the **Active DB view** is selected. The Service Domains web page appears.
3	Click a link in the **ID** column of the Service Domains web page. The View Service Domain Property web page appears.
4	Select a domain to view a detailed description.
	--End--

Viewing the L1 Domains (UDP)

Use the following procedure to view information about L1 Domains (UDP).

Procedure steps

Step	Action
1	Click the **Configuration** tab on the NRS Manager toolbar.
2	Ensure the Active DB view is selected.
3	Click **L1 Domains (UDP)** in the navigation tree. The L1 Domains (UDP) web page appears.
4	In the **Service Domains** menu, choose a Service Domain.
5	Click **Show**. A list of configured L1 Domains appears.
6	Click a link in the **ID** column of the L1 domains (UDP) web page. The View L1 domain Property web page appears.
7	Select an L1 domain to view a detailed description.
	--End--

Viewing the L0 Domains (CDP)

Use the following procedure to view information about L0 Domains (CDP).

Procedure steps

Step	Action
1	Click the **Configuration** tab on the NRS Manager toolbar.
2	Ensure the Active DB view is selected.
3	Click **L0 Domains (CDP)** in the navigation tree. The L0 Domains (CDP) web page appears.
4	In the menus, choose a **Service Domain** and **L1 Domain**.
5	Click **Show**. A list of configured L0 Domains appears.
6	Click a link in the **ID** column of the L0 domains (CDP) web page. The View L0 domain Property web page appears.
7	Select an L0 domain to view a detailed description.

--End--

Viewing Gateway Endpoint Dynamic Registration Information

Use the following procedure to view the Gateway Endpoint Dynamic Registration Information.

Procedure steps

Step	Action
1	In the NRS Manager navigation tree, choose **Numbering Plans**, **Endpoints**. The Endpoints web page appears.
2	Ensure **Active database** is selected.
3	The **Limit results to Domain**: lists contain configured Service Domains, L1 Domains and L0 Domains. Select a **Service Domain**, a **L1 Domain** and a **L0 Domain** from the respective lists.
4	Click the **Gateway Endpoints** tab. A list of configured Gateway Endpoints appears in the Endpoints pane. You can sort the Gateway Endpoints in ascending or descending alphabetical order. .
5	Click a link in the **ID** column of the Endpoints pane. The Edit Gateway Endpoint web page appears.
6	Scroll down the page to view **Endpoint Dynamic Registration Information for SIP**.

--End--

Viewing the Gateway Endpoints

Use the following procedure to view information about Gateway Endpoints.

Procedure steps

Step	Action
1	Click the **Configuration** tab on the NRS Manager toolbar.
2	Ensure the **Active DB view** is selected.
3	Click **Gateway Endpoints** in the navigation tree. The Gateway Endpoints web page appears and displays three lists: Service Domain / L1 Domain / L0 Domain.
4	Select a **Service Domain**, **L1 Domain**, and **L0 Domain** from the lists.
5	Click **Show**. The web page expands to display a list of configured Gateway Endpoints.
6	Click a link in the **ID** column of the gateway Endpoints web page. The View Gateway Endpoint Property web page appears.
7	Select a Gateway Endpoint to view a detailed description.
	--End--

Viewing User Endpoint Dynamic Registration Information

Use the following procedure to view information about User Endpoint Dynamic Registration.

Procedure steps

Step	Action
1	In the NRS Manager navigation tree, click **Numbering Plans**, **Endpoints**. The Endpoints web page appears.
2	Ensure **Active database** is selected.
3	Using the menus, choose a **Service Domain**, an **L1 Domain**, and an **L0 Domain**.
4	Click the **User Endpoints** tab. A list of configured User Endpoints appears in the Endpoints pane You can sort the User Endpoints in ascending or descending alphabetical order.
5	Click a link in the **ID** column of the Endpoints pane. The Edit User Endpoint web page appears. If a User Endpoint is configured, then the supported protocol type is dynamic SIP. The NRS Manager displays User Endpoint Dynamic Registration Information after the User Endpoint registers with the NRS. User Endpoint Dynamic Registration information includes the following: SIP IP, Registration expiry time, User agent, and Preference.
6	Scroll down the page to display **User Endpoint Dynamic Registration Information**.

--End--

Viewing a User Endpoint

Use the following procedure to view information about existing User Endpoints.

Procedure steps

Step	Action
1	In the NRS Manager navigation tree, click **Numbering Plans**, **Endpoints**. The Endpoints web page appears.
2	Select the **Active** or **Standby** database. The Active database is used for runtime queries. To modify the database, first ensure that it is in Standby database view. You can switch between Active and Standby database views at any time. You must be an administrator to modify the standby database. The Endpoints web page refreshes.
3	From the menus, choose a **Service Domain**, an **L1 Domain**, and an **L0 Domain**.
4	Click the **User Endpoints** tab. A list of configured User Endpoints appears in the Endpoints pane. You can sort the endpoints in ascending or descending alphabetical order.
5	Click a link in the **ID** column of the Endpoints pane. The Edit User Endpoint web page appears.

--End--

Deleting a User Endpoint

Use the following procedure to delete an existing user endpoint.

Procedure steps

Step	Action
1	In the NRS Manager navigation tree, click **Numbering Plans**, **Endpoints**. The Endpoints web page appears.
2	Ensure Standby database is selected.
3	In the menus, choose a **Service Domain**, an **L1 Domain** and an **L0 Domain**.
4	Click the **User Endpoints** tab. The Endpoints web page appears. You can sort the User Endpoints in ascending or descending alphabetical order.
5	Select a check box beside one or more links in the **ID** column of the Endpoints pane.
6	Click **Delete**. A Confirmation box appears.
7	Click **OK**. The standby database is updated, and the Endpoints web page appears.
8	In the NRS Manager navigation tree, click **System**, **Database**. The Database web page appears.
9	Click **Cut over**. The Cut over command is issued, and the database is placed into a Switched over state.
10	In the NRS Manager navigation tree, click **System**, **Database**. The Database web page appears. The Database status is Switched over.
11	Click **Commit**. The Commit command is issued, and the database is placed into a Committed state.

--End--

Nortel Communication Server 1000

Communication Server 1000E SIP Line Service for Release 5.5

Printed in Canada
Release: 5.5
Publication: NN43041-320
Document revision: 01.01
Document release date: 3 December 2008

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

www.nortel.com