Nortel Communication Server 1000

SIP Line Fundamentals

Release: 6.0
Document Revision: 01.08

www.nortel.com

NN43001-508

Nortel Communication Server 1000
Release: 6.0
Publication: NN43001-508
Document release date: 9 February 2010

Contents

New in this release

The following sections detail what's new in *SIP Line Fundamentals* (NN43001-508) for Nortel Communication Server 1000 Release 6.0:

- "Features" (page 8)
- "Other changes" (page 9)

Features

The Nortel IP Phone 1535 is supported on CS 1000 Release 6.0. For more information about the Nortel IP Phone 1535, see “Supported SIP IP Phones” (page 29).

Other changes

Revision history

February 2010	Standard 01.08. This document is up-issued for changes in technical content. Information about the IP Phone 1200 series phones and the SIP Tone V phone is removed from this document.
February 2010	Standard 01.07. This document is updated for Communication Server 1000 Release 6.0.
January 2010	Standard 01.06. This document is updated for Communication Server 1000 Release 6.0.
November 2009	Standard 01.05. This document is updated for changes in technical content. IP.Phone 1535 is added to"Supported SIP IP Phones" (page 29).
September 2009	Standard 01.04. This document is updated for Communication Server 1000 Release 6.0.
June 2009	Standard 01.03. This document is updated for Communication Server 1000 Release 6.0.
May 2009	Standard 01.02. This document is updated for Communication Server 1000 Release 6.0.
May 2009	Standard 01.01. This document is a new NTP for Communication Server 1000 Release 6.0.

How to get help

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

Getting help from the Nortel Web site

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

www.nortel.com/support

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

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

Getting help over the telephone from a Nortel Solutions Center

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

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

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

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

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

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

Introduction

This document contains the following topics:

Subject

This document describes the SIP Line Service and how to implement SIP Line as part of your system.

Note on legacy products and releases

This NTP contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 6.0 (or later) software. For more information about legacy products and releases, click the **Technical Documentation** link under **Support & Training** on the Nortel home page:

www.nortel.com

Applicable systems

This document applies to the following systems:

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

Intended audience

This document is intended for individuals who administer CS 1000 systems.

Conventions

Terminology

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

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

Unless specifically stated otherwise, the term Element Manager refers to the CS 1000 Element Manager.

Related information

This section lists information sources that relate to this document.

Technical documentation

This document references the following technical documents:

- *Features and Services Fundamentals* (NN43001-106)
- *Unified Communications Management Common Services Fundamentals* (NN43001-116)
- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *Network Routing Service Fundamentals* (NN43001-130)
- *Converging the Data Network with VoIP Fundamentals* (NN43001-260)
- *IP Peer Networking Installation and Commissioning* (NN43001-313)
- *Branch Office Installation and Commissioning* (NN43001-314)
- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *Hospitality Features Fundamentals* (NN43001-553)
- *Security Management Fundamentals* (NN43001-604)

- *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* (NN43021-310)
- *Communication Server 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458)
- *Communication Server 1000E Installation and Commissioning* (NN43041-310)
- *Communication Server 1000E Software Upgrades* (NN43041-458)

Online

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

www.nortel.com

CD-ROM

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

SIP Line Service overview

The Communication Server 1000 (CS 1000) is a feature-rich hybrid Internet Protocol Private Branch Exchange (IP PBX) solution, which delivers Business Grade Telephony features and functionality to IP endpoints. The SIP Line Service fully integrates Session Initiation Protocol (SIP) endpoints in the CS 1000 system and extends the CS 1000 telephony features to the SIP IP Phones.

The SIP Line Service comprises three components:

- The SIP Line Universal Extension (UEXT) called SIPL on the Call Server.

  Note: The CS 1000 Release 6.0 SIPL Universal Extension is different from the UEXT used in CS 1000 Release 5.5.

- The SIP Line Gateway (SLG) application.
- The system management interface (Element Manager) used to configure and manage the SIP Line Service.

This section contains information about the following topics:

SIP Line architecture

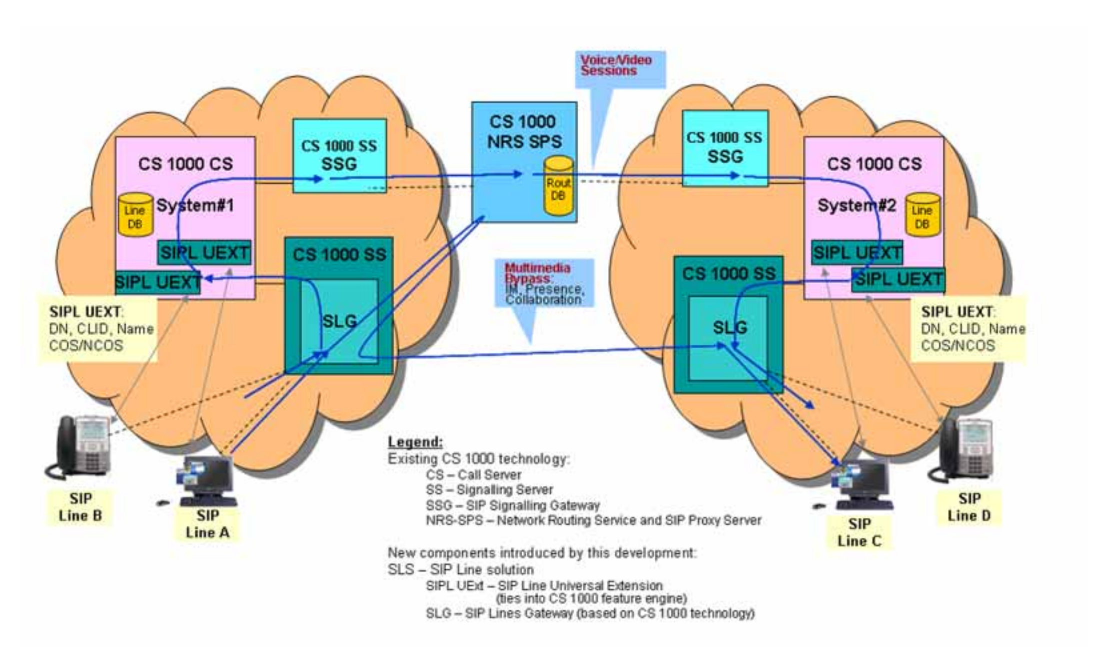
The SIP Line Service is embedded in each CS 1000 system and directly manages a number of SIP IP Phones. The Universal Extensions (UEXT) line type provides CS 1000 Line appearance to the supported SIP IP Phones and this extends the existing CS 1000 Networking and Line services to these SIP IP Phones.

The inclusion of SIP endpoints in the CS 1000 system is based on the SIPL UEXT. Universal Extensions are used to represent devices and clients that are external to the CS 1000 system. Universal Extensions use virtual TNs.

> **ATTENTION**
> You must configure the SIP IP Phones with the CS 1000 SIPL UEXT Universal Extension SIPL subtype, which provides a line appearance to the SIP IP Phones.

The following figure illustrates the architecture of the SIP Line Service.

Figure 1
SIP Line architecture



This figure demonstrates the complete SIP Line architecture of CS 1000 and this architecture is implemented in phases. The SIP Line Gateway (SLG) is the SIP Line signaling gateway, which communicates between the CS 1000 Call Server (CS) and the SIP side of the signaling. The SIP Line Gateway (SLG) serves as a SIP Registrar and a SIP Proxy server to users. The SLG uses voice signaling messages to communicate internally with the Call Server.

A Call Server hosts each SIP line instance. This means each SIPL UEXT represents one SIP IP Phone.

The SIP IP Phones supported by CS 1000 behave either as a regular Universal Extensions or as a SIP Line. The behavior of the IP Phone and the invocation of the SIP Line Service depends on the configuration of SIP Line in LD 11.

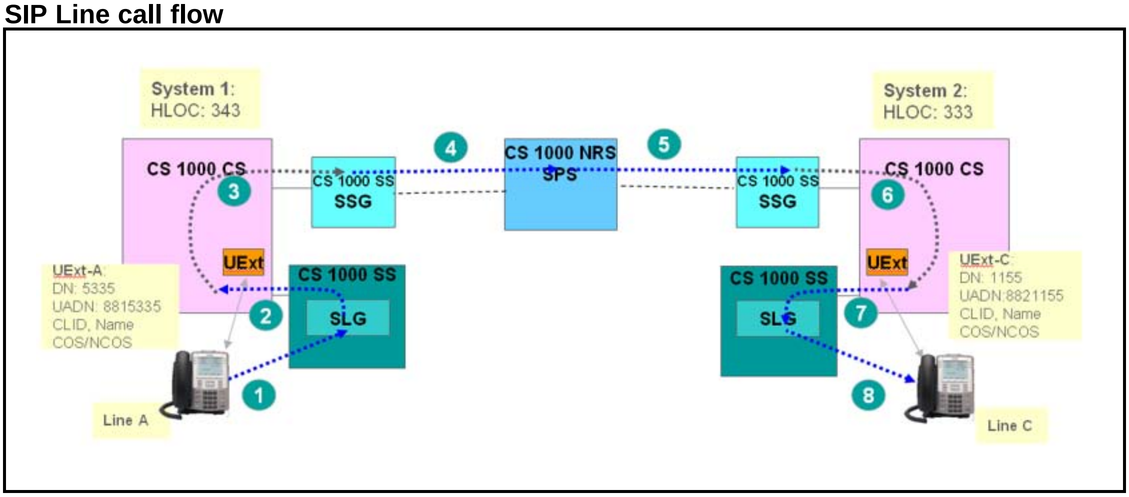
- If you enter SIPN (SIP Line for Nortel IP Phones) at the UXTY prompt, then the phones behave like regular Universal Extensions. Only trunk features are provided to such IP Phones.
- If you enter SIPL (SIP Line) at the UXTY prompt and 1 0 0 0 at the Maximum Client Count Limit (MCCL) prompt, then the phones behave as a SIP Line.

SIP Line call flow

The following figure shows an example of a SIP Line to SIP Line call over a SIP Line trunk.

The actual trunk type that connects two systems can be any trunk type, including H.323 trunks and TDM trunks (such as Primary Rate Interface [PRI] or Digital Trunk Interface [DTI]). Routing a SIP Line call from one system to another system does not differ from the call routing of any other phone types.

Figure 2
SIP Line call flow



The following steps describe the call flow between Line A (on System 1) and Line C (on System 2):

1. Line A dials 63331155. A SIP INVITE message is sent to the SIP Line Gateway (SLG), and then the SLG authenticates the originating SIP Line.
2. The SLG presents the call to the CS 1000 Call Server (that is, CS 1000 CS on System 1).
3. The Call Server applies all line call origination rules to the call as indicated in the Universal Extensions (SIPL UExt-A) settings.
4. Based on the dialing plan rules (for example, LOC 333), the call is routed to the remote system. The route used to reach the far-end depends on the dialing plan configuration. It can be either an IP VTRK (for example, H.323, SIP) or TDM trunks (for example, PRI, DTI). In this example, SIP trunk is used.
   - The SIPL UExt-A must have the required access privileges for the call to be routed.
   - The Calling Line Identification (CLID) Name and Network Class of Service (NCOS) attributes of the call are configured as indicated in the SIPL UExt-A settings.
5. The call is routed to the target system. In this call flow example, the call is routed using the SIP Proxy Server. However, the Gatekeeper or direct TDM trunk connections can be used. (How a call is routed depends on the customer's configuration.)
6. The Call Server tries to terminate the call on the SIPL UExt-C. It applies all line termination features as indicated in the SIPL UExt-C settings.

   An attempt to terminate the call on a SIPL UEXT triggers a SIP call using the SIP Line route associated with the user.
7. The call is delivered to the SLG associated with the SIP Line route.
8. Based on the existing registration record of Line C, the SLG routes the call towards Line C.

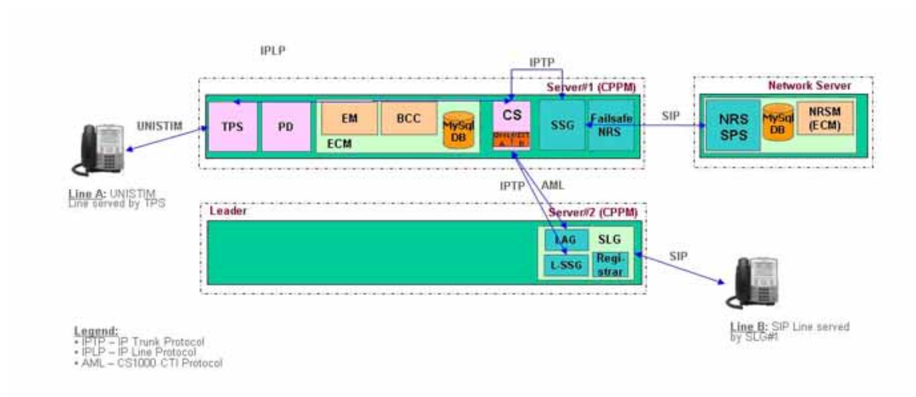
Deployment models

Some sample SIP Line deployment models are shown in the following sections.

CS 1000E co-resident system with SIP Line with IP Networking

The following figure shows a CS 1000E co-resident system with the SIP Line Service and IP Networking.

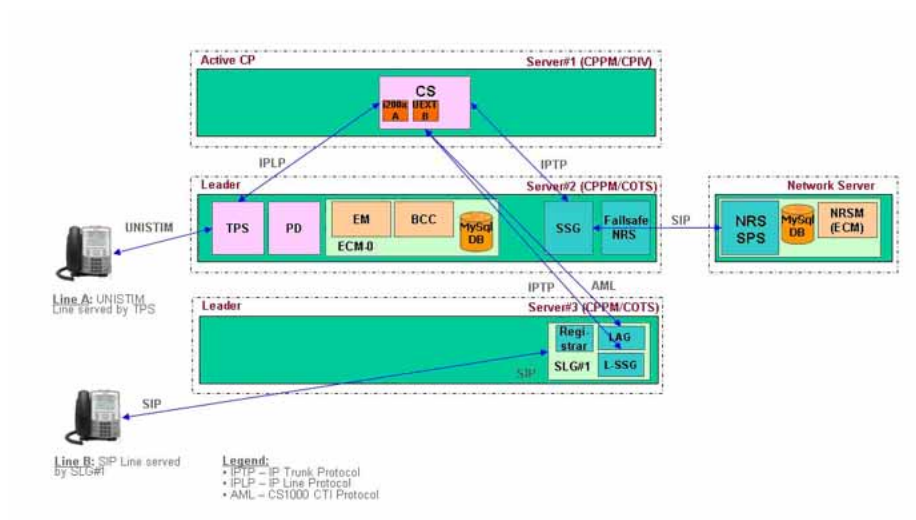
Figure 3
CS 1000E Co-resident system with SIP Line (with IP Networking)



CS 1000 system with three servers

The following figure shows a CS 1000 system comprising three servers. This system includes a server for the Call Server, another server for the SIP Line Gateway (SLG), and a third server for Signaling Server applications such as the Line Terminal Proxy Server (LTPS) or with other virtual trunk applications (such as SIP Gateway or H.323 Gateway).

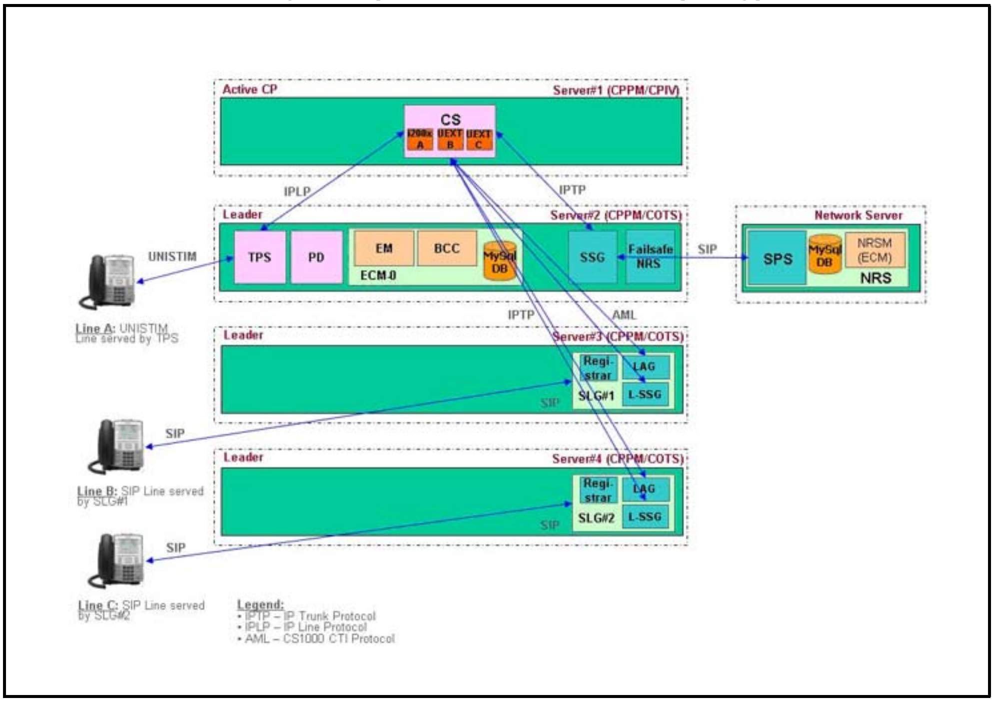
Figure 4
Three-server CS 1000 system



CS 1000 system with four servers with double SIP Line capacity

The following figure shows a CS 1000 system comprising four servers with double SIP Line capacity. The four-server deployment is the same as the three-server deployment; however, you can have two SIP Line Gateways (SLG) in the same node to achieve SLG redundancy.

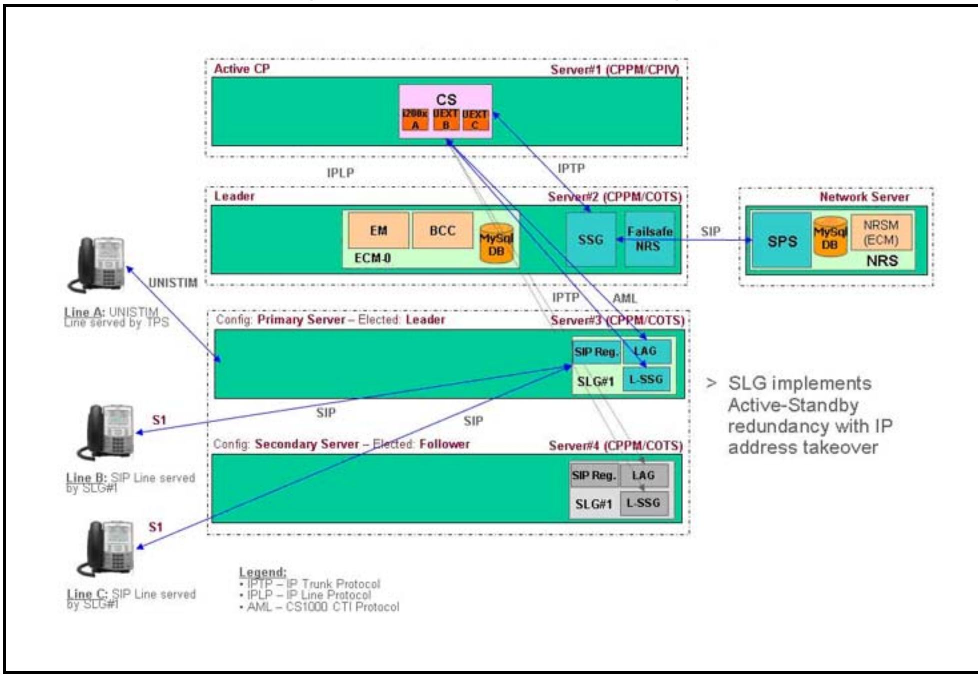
Figure 5
Four-server CS 1000 system (with double SIP Line capacity)



High Availability CS 1000E System with SIP Line configuration

The following figure shows a High Availability (HA) CS 1000E system with a SIP Line configuration.

Figure 6
CS 1000 system with High Availability SIP Line configuration



Hardware and software requirements

The SIP Line Service comprises three major software components: Call Server (CS), SIP Line Gateway (SLG), and Element Manager. Software changes on the Call Server are bundled within the SIP Line Service Package (SIP_LINES PACKAGE, 417) and reside on the supported hardware platforms with the addition of the commercial off-the-shelf (COTS) and Common Processor Pentium Mobile (CP PM) Call Processor. Both the SIP Line Gateway and Element Manager reside on the Linux COTS or CP PM servers.

Support is available for the following hardware platforms:

- HP 320 G4
- IBM x306M
- Dell R300
- IBM x3350
- Nortel Common Processor Pentium Mobile (CP PM)

The following table outlines the minimum requirements for all supported platform types:

Table 1
Hardware minimum requirements

Hardware	Minimum requirement
Hard drive size	40 GB
Memory size	2 GB

The minimum requirements of the CP PM card are:

- BIOS: Version 18 (or later)
- Hard drive size: 40 GB
- Memory: 2 GB

The minimum requirement for the Removable Media Device Compact Flash (RMD CF) card (as installed media) is 1 GB.

ATTENTION
In CS 1000 Release 6.0, the SIP Line Service cannot co-reside with the Line Terminal Proxy Server (LTPS) or with other Virtual Trunk applications (such as the SIP Gateway or H.323 Gateway). In Element Manager, you cannot configure the SIP Line Service with other application services.

Codec selection and negotiation

The SIP Line Service follows the same codec negotiation and selection as the SIP Gateway (SIP GW). The following codecs are supported.

Table 2
Supported codecs and payload sizes

Codec	Payload size
G.711 u-law/a-law	10 ms, 20 ms (default), and 30 ms
G.729 A/AB	10 ms, 20 ms (default), 30 ms, 40 ms, and 50 ms
G.723.1	30 ms (default) (Can limit the number of DSP channels available.)
T.38 for FAX	Supported for fax calls on gateway channels

By default, support for the G.711 codec must exist at both ends of a call. Unrecognized codecs (including video codecs) are forwarded to far end through the Session Description Protocol Transparency (SDP-T) feature.

The SIP Line Gateway sends the codec list of the offerer (in order of preference) and the receiver selects one common codec based on its list of preferred codecs. The receiver always performs the codec selection and selects one common codec based on the Best Bandwidth selection mechanism. If a specific payload size is configured different from the default payload size, a packet time (ptime) is included in the offer. In this version of SDP, only one ptime is available for each codec. If no ptime is included in the SDP, the default payload size is used.

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

Bandwidth management

The SIP Line Service is incorporated in the existing Bandwidth Management (BWM) functionality on the Call Server where the devices in the network belong to some logically defined zone (usually the geographic location of the device). Several aspects of interworking between the devices (and between the zones) are managed by the Bandwidth Management feature such as the following:

- bandwidth limits and current usage
- preferred codec selection
- alternate routes decision

The following sections describe bandwidth management operation for SIP Line.

Bandwidth Management configuration for SIP Line is divided into the following two steps:

1. “Planning zone setup for SIP Line clients and configuration using LD 117 utilities” (page 25)
2. “Configuring SIP Line clients with a SIPL zone” (page 26)

Planning zone setup for SIP Line clients and configuration using LD 117 utilities

Before SIP Line clients are configured in a bandwidth zone, the zone must be represented in the zone table. LD 117 maintains the zone table configuration.

The system administrator must select the zone number to use for SIP Line clients. The SIP Line zone must not be the same as VTRK zone. You must configure the SIP Line zone with an intrazone and interzone policy, which is either Best Quality (BQ) or Best Bandwidth (BB). Also, based on the network characteristics, you must configure the bandwidth limits for intrazone (Local Area Network [LAN]) and interzone (Wide Area Network [WAN]) calls.

Example:

```
>ld 117
>new zone 1 1000000 BQ 1000000 BB
```

After you add the zone in the zone table and you configure all parameters, use LD 43 to issue the Equipment Data Dump (EDD) command. This command updates the zone.db file with recent changes.

Configuring SIP Line clients with a SIPL zone

The SIP Line Service considers the SIP Line Universal Extension (SIPL UEXT) as the representation of the SIP Line client on the Call Server. Each SIP Line client has a SIPL UEXT block that stores the corresponding configuration for the Call Server. Each SIP Line client must have a zone number field that the bandwidth management feature handles. This number shows the zone (in the zone table) to use in bandwidth management call processing.

The SIPL UEXT is a subtype of the Business Communication Sets (BCS) block. The ZONE prompt represents this parameter in LD 11 for all types of IP resources. This allows the ZONE prompt configuration for SIPL UEXT type to be the SIPL subtype. No additional limitations are placed on the zone of SIPL UEXT (compared with the IP set zone). Configure the SIP Line client in the same zone as other devices (IP Phones, Voice Gateway channels; except for virtual trunk zones). In the case of the SIPL UEXT type, the easy-change routine is also available for ZONE prompt. You can use LD 11 and LD 20 to print the ZONE prompt.

SIPL VTRK zone

A regular (non-SIP Line) Virtual Trunk (VTRK) route is configured with a special zone (VTRK zone intent) that has significant meaning in bandwidth management processing of VTRK calls. The VTRK route is used for initial bandwidth and codec-list processing when the far end zone is not known.

The zone configured in LD 16 for SIPL VTRK routes and trunks does not participate in bandwidth management processing for SIP Line; the zone is used for other purposes such as resource counting. The SIPL VTRK zone also has VTRK zone intent and can be the same regular VTRK zone or a different zone.

Zone operation

Calls that involve a SIPL UEXT are calculated against the respective zone configuration. This zone operation is the same as for other telephone types (for example, UNIStim telephones).

Codec negotiation

Only supported codecs are used in the calculations in bandwidth management modules. The SIP Line clients must have at least one supported codec configured. SIP Line clients can negotiate other codecs (those not listed in the supported codec list) in the following scenarios:

- SIP Line-to-SIP Line audio and video call
- SIP Line-to-Third-party SIP entity audio and video calls

If an unsupported codec is negotiated for a SIP Line call, then bandwidth management ignores the unsupported codec and tries to select a supported codec (based on the codec lists). Bandwidth management calculations are inaccurate in such scenarios. For deployments where accurate bandwidth management calculation is more important than the codec selection, you must configure the SIP IP Phones with the codecs supported by CS 1000.

Codec selection

Two models of codec selection are available for Bandwidth Management:

- Local codec selection—The codec is selected based on the policies of the zones involved. The selected policy (Best Bandwidth [BB] or Best Quality [BQ]) determines the order in the codec list and the first codec in the list is chosen. For example:
  - — Zone 1: Intrazone policy is BQ and interzone policy is BB.
  - — Zone 10: Intrazone policy is BQ and interzone policy is BQ.
  - — Zone 100: Intrazone policy Is BQ, interzone policy is BQ.

  For calls between zone 1 and zone 10, the Best Bandwidth policy is selected. For calls between zone 10 and zone 100, the Best Quality policy is selected.
- IP Peer codec selection—The IP Peer codec selection consists of the Best Bandwidth and Master/Slave approaches, where the codec selection occurs separately on both sides based on local and received codec lists. For more information about codec selection, see *IP Peer Networking Installation and Commissioning* (NN43001-313).

The SIP Line side of a call is considered the local side to the Call Server (despite that a SIPL VTRK trunk is involved). Therefore, a SIP Line-to-SIP Line call is also considered as a local call.

For SIP Line terminating calls, the codec list is sorted based on the policies of the originating zone and the SIPL zone (which is from the SIPL UEXT block) and is sent to the SIP client.

For SIP Line originating calls, the following activities occur:

- Local calls to a UNIStim IP Phone/TDM device—The codec list of SIP Line client and codec list of IP Phone and Voice Gateway (VGW) channel are used to find matching codecs. The codec is selected based on the zone policies.
- Local calls to other SIP Line clients—The codec list of SIP Line client is used for initial codec selection (because the codec list of the terminating side is not known). The initial codec is selected based on policies of both zones but only from the originator codec list. This type of call falls under the responsibility of the Session Description Protocol Transparency (SDP-T) feature.
- IP Peer (H.323 and SIP) calls over VTRK—The codec list of the SIP Line client is sorted based on SIP Line client interzone policy because the VTRK interzone policy must be Best Quality (BQ).

Limitations

The following codec selection limitations exist:

- Session Description Protocol Transparency (SDP-T) limitation (video media stream)—The codec negotiation for calls that fall under the responsibility of the SDP-T feature can be inaccurate (such as tandem SIP calls including SIP Line to and from SIP Virtual Trunk, and SIP Line to SIP Line). The Call Server deals only with supported codecs, while the SDP body for such calls is tunneled through the Call Server. The endpoints can choose a dynamic codec which is filtered out on the SLG/SSG. In this case, the bandwidth management procedures calculate bandwidth usage based on the remainder of the entire list. Also the media information for a particular session (call) is not displayed for tandem calls. This is also true for a SIPL user to SIPL user local call.
- SIP codec preference limitation—A SIP endpoint cannot be told the order of preference in codec list during negotiation. In general, the order in the codec list received in the initial INVITE message does not guarantee the order in preferences during codec negotiation.

CS 1000 bandwidth management for SIP Line attempts to use all efforts sorting the codecs based on the zone policies and selecting the codec locally. However, due to these two previous limitations, the SIP client selects the real codecs. You must configure the SIP Line clients with codec lists and codec preferences synchronized as closely as possible with the CS 1000 zone policy configuration. For more information see, “Codec selection and negotiation” (page 24).

Call Admission Control (CAC) VTRK forecast schema

IP Peer calls use forecast schema on bandwidth limit restriction where special flags are passed in the information element (IE) to the far end. The outgoing calls to the VTRK are never initially blocked on the originating side; however, only the flags are configured. This schema is removed for SIPL VTRK calls because the SIP Line side is local to the Call Server and the real far-end zone is already known. The zone of SIPL UEXT is used for bandwidth limit checks.

Bandwidth management-based features

With the zone configured in the SIP Line Universal Extensions (SIPL UEXT) block, all zone-based features (such Branch Office Fallback-to-PSTN or Alternate Routing for BWM) are supported for SIP Line. SIP Line is represented to the Call Processor in the same manner as any other line; therefore, the zone works in the same way.

Adaptive bandwidth management

Adaptive bandwidth management is not implemented for SIP Line because SIP Line (and the SIP client) does not support the Quality of Service (QoS) feature. A SIP client can be located and configured in the same zone with other IP resources and no restrictions exist for enabling adaptive bandwidth management for this zone. SIP IP Phones can be affected by the adaptive bandwidth management operation from other IP resources in the same zone (such QoS alarms reporting, sliding maximum decrease, and call blocking) during network congestion and poor quality but not vise versa.

Network-wide Virtual Office

Network-wide Virtual Office (NWVO) login is not supported for SIP Line.

Supported SIP IP Phones

The following SIP IP Phones are supported in this release:

- Nortel IP Phone 1120E
- Nortel IP Phone 1140E
- Nortel IP Phone 1535
- Nortel IP Softphone 3456
- Teledex 2200
- Teledex 4200

The following table lists the SIP client capabilities that can potentially affect a user’s experience with various features. For more information about the SIP Line features, see “SIP Line features” (page 39).

Table 3
SIP IP Phone capabilities

IP Phone and Message	Nortel IP Phone 1120E and 1140E	Teledex ND2200/LD4200 (with display)	Nortel IP Phone 1535	Nortel IP Softphone 3456
Firmware version	2.2.x	3.6.4.8	00.2.76	—
Unregistration enforcement	Not supported	Not supported	Not supported	Not supported
MWI support	200/481 SUBSCRIBE and NOTIFY methods	200 NOTIFY method	200 Supported: MWI displayed	200 NOTIFY method
Conference	Local and server	Local	Server	Local
Blind Transfer	REFER method	REFER method	REFER method	REFER method
Call Transfer with Consultation	REFER-REPLACE method	REFER-REPLACE method	Not supported	REFER-REPLACE method
CWI presentation	Supported	Supported	Supported	Supported
Multi-Proxy support (for GR and SBO applications)	Multiple (Does not detect that a proxy is down until the next registration.)	Two lines register to two proxies	Single	Supports multiple lines at the same time. Each account is a single proxy.
Proxy registration redir ection (301/302/305)	Supported	Not supported	Supported	Not supported
Proxy use after redirecti on (301/302/305)	Redirected to proxy	N/A	Originally configured proxy	Originally configured proxy
Registration Timer	1 hour to 31 days	300 seconds to 1 hour	60 seconds to 24 hours	Unlimited
Behavior after registration timeout	Relies on keepalive message	Re-registers	Re-registers	Re-registers
IP Phone keepalive	SIP PING	No	STUN	STUN
Transport	UDP	TCP/UDP	UDP	UDP
Codec	G.711 and G.729	G.711 and G.729	G.711 and G.729 (>=20ms)	G.711 and G.729
Ptime supported	>=10 ms	>=20 ms	>=20 ms	>=20 ms
GR/BO support	Supports S1/S2 configuration	Not supported	Not supported	Not supported

Table 3
SIP IP Phone capabilities (cont'd.)

IP Phone and Message	Nortel IP Phone 1120E and 1140E	Teledex ND2200/LD4200 (with display)	Nortel IP Phone 1535	Nortel IP Softphone 3456
DTMF	Yes	Yes	Yes	Yes
# Code Dialing	With "# Ends Dialing: OFF", # goes as a dialed digit. With "# Ends Dialing: ON", # does not go as a dialed digit.	# can only be pressed if IP Phone is on an active call (goes as DTMF).	# does not go as a dialed digit.	# is sent as a dialed digit. For example: INVITE sip:4090%23@testbed1.com SIP/2.0
RGA (FFC)	Supported (Receives missed call notification)	Supported (Receives missed call notification))	Supported (Receives missed call notification)	Supported (Receives missed call notification)
Make Set Busy (MSB) (FFC)	Supported	Responds with a 400 Invalid message summary to the NOTIFY for MSB.	Supported	Responds with 400 Bad Request message to the NOTIFY for MSB.
Call Server Make Set Busy (MSB) notification	Not supported	Not supported	Not supported	Not supported
CFW All Calls (FFC)	Supported	Not supported You cannot enter more than four digits.	Supported	Supported
CPND	Yes. (Update for simple call and CFAC only.)	No for ND2200 Yes for LD420	Yes. (Update for simple call and CFAC only.)	Yes

SIP IP Phone configuration

The following sections provide configuration information for the supported SIP IP Phones.

ATTENTION
Nortel recommends that you only enable the CS 1000 supported voice codecs on each type of client.

Nortel IP Phone 1120E and 1140E configuration

The following configuration must be performed for the Nortel IP Phone 1120E and 1140E:

- Convert the UNIStim IP Phone to a SIP IP Phone. To do this you must upgrade and convert the IP Phone 1120E and 1140E firmware.
- Provision the SIP firmware on the IP Phone using the provisioning server.

For more information on these tasks, see *SIP Firmware Release 2.0 for IP Phone 1120E Administration* (NN43112-300) and *SIP Firmware Release 2.0 for IP Phone 1140E Administration* (NN43113-300).

The configuration files for the IP Phone 1120E and 1140E must also be configured correctly:

- Ensure the 1120eSIP.cfg file and 1140eSIP.cfg file are properly configured. For more information, see "1140eSIP.cfg file" (page 32).
- Ensure the DeviceConfig.dat file is properly configured. For more information see, "deviceConfig.dat file" (page 33).
- Ensure the 11x0e.cfg file is configured properly. For more information, see "1120e.cfg" (page 34).
- Ensure the dial plan is configured properly. For more information, see "Sample dial plan" (page 35).

For the IP Phone 1120E and 1140E, the UEXT TN configuration must have the following:

```
UXTY SIPL
MCCL YES
SIPN 1
```

1140eSIP.cfg file

The following example shows the 1140eSIP.cfg file with the 1140E SIP Firmware that has a filename of SIP1140e02.02.13.bin.

```
[FW]
DOWNLOAD_MODE AUTO
VERSION SIP1140e02.02.13
PROTOCOL TFTP
FILENAME SIP1140e02.02.13.bin

[DEVICE_CONFIG]
DOWNLOAD_MODE FORCED
VERSION 000200
FILENAME DeviceConfig.dat
```

```
[DIALING_PLAN]
DOWNLOAD_MODE AUTO
VERSION 000200
FILENAME dialplan.txt
```

deviceConfig.dat file

The following deviceConfig.dat file shows the recommended default configuration file for the IP Phone 1120E and 1140E.

> **ATTENTION**
> If the IP Phone 1120E and 1140E are configured at the Branch Office or Survivable Media Gateway (SMG), you must include the following entries in DeviceConfig.dat file:
>
> `REDIRECT_TYPE MCS`
>
> `PROXY_CHECKING NO`

```
SIP_DOMAIN1 nortel.com

SERVER_IP1_1 47.11.142.78
SERVER_PORT1_1 5070

SERVER_RETRIES1 3
SERVER_RETRIES2 3

#***************Mandatory Device settings**************

ENABLE_SERVICE_PACKAGE NO
CONFERENCE_URI1 conference@nortel.com
ADHOC_ENABLED1 YES
MAX_ADHOC_PORTS1 6

AUDIO_CODEC1 PCMA standard a-law
AUDIO_CODEC2 PCMU standard u-law
AUDIO_CODEC3 G729 729 codec
AUDIO_CODEC4 G723 high-compression codec

FORCE_BANNER YES
BANNER NORTEL-SLG
UPDATE_USERS NO
SIP_PING YES

AUTOLOGIN_ENABLE YES
EXP_MODULE_ENABLE YES
ENABLE_UPDATE YES
ENABLE_PRACK YES
RTP_MIN_PORT 50000
```

```
RTP_MAX_PORT 50100

# Time configuration
DST_ENABLED YES
TIMEZONE_OFFSET -18000

VMAIL 2300
VMAIL_DELAY 300

AUTO_UPDATE YES
AUTO_UPDATE_TIME 3600
AUTO_UPDATE_RANGE 1

DEF_LANG English
MAX_INBOX_ENTRIES 50
MAX_OUTBOX_ENTRIES 50
MAX_REJECTREASONS 5
MAX_PRESENCENOTE 5
MAX_CALLSUBJECT 5

ENABLE_BT YES

ADMIN_PASSWORD 26567*738

ENABLE_3WAY_CALL YES
TRANSFER_TYPE STANDARD
REDIRECT_TYPE MCS
DISABLE_PRIVACY_UI YES
IM_MODE DISABLED
SNTP_ENABLE YES
SNTP_SERVER ntp-toronto-3.ca.nortel.com
```

1120e.cfg

The following is an example of the 1120e.cfg file:

```
[DEVICE_CONFIG]
DOWNLOAD_MODE AUTO
VERSION 000090
FILENAME 1120DeviceConfig.dat

[FW]
DOWNLOAD_MODE AUTO
VERSION SIP1120E02.01
PROTOCOL TFTP
FILENAME SIP1120e02.01.06.00.bin

[LANGUAGE]
```

```
DOWNLOAD_MODE AUTO
DELETE_FILES 1
VERSION 000d04
FILENAME Francais.lng
FILENAME Portuguese.lng
FILENAME Swedish.lng
FILENAME Czech.lng
```

Sample dial plan

The following file show a sample dial plan.

```
/* ------------------------------------------- */
/* Generic dial plan - Assumes AC1 is 9 */
/* ------------------------------------------- */
$n="domain.com" /* Enter Customer Internal Domain Name */
$t=300
$s=0

%%
/* DIGITMAP: External Operator call */
(90)|(90)# && sip:$$@$n;user=phone &&
/* DIGITMAP: Information, Example for Other SPN's */
(91411)|(91411)# && sip:$$@$n;user=phone &&
(9411)|(9411)# && sip:$$@$n;user=phone &&
/* DIGITMAP: Emergency call */
(9911)|(9911)# && sip:$$@$n;user=phone && t=100
/* DIGITMAP: Example Private intra-location call or CDP, no
access code 7 digit, lock on first 5 digits */
(69665x{2})|(69665x{2})# && sip:$$@$n;user=phone &&
/* DIGITMAP: Public local call, access code 10 digits, AC1,
first gigit of NPA, second digit not 0 or 2-9 */
(99[^023456789]x{8})|(99[^023456789]x{8})# &&
sip:$$@$n;user=phone &&
(98[^023456789]]x{8})|(98[^023456789]x{8})# &&
sip:$$@$n;user=phone &&
/* DIGITMAP: Public national call, access code 10 digits */
(91x{10})|(91x{10})# && sip:$$@$n;user=phone &&
```

Nortel IP Phone 1535 configuration

The following configuration must be done for the IP Phone 1535:

- Configure the phone as SIPN UEXT type on the Call Server.
- Configure Proxy type to CS2K on the IP Phone:
  - — On the IP Phone, 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:
  - On the IP Phone, select Main Menu, Settings, VoIP Settings, Proxy, NAT Timer, Disable.
- Disable Stun:
  - On the IP Phone, select Main Menu, Settings, VoIP Settings, Proxy, STUN, Disable.

Teledex configuration

For the Teledex phone, you must implement the following configuration details:

- Ensure the UEXT configuration has MCCL with SIP3 equal to 1.
- Configure the phone using the following Web page: http://<IP address of phone:8080>

Nortel IP Softphone 3456 configuration

For the Nortel IP Softphone 3456, you must implement the following configuration details:

- Ensure the UEXT configuration has MCCL with SIPN equal to 1.
- Disable the provisioning server on the phone. On the phone, navigate to Preferences > Advanced > No login server available.
- Nortel recommends that you only enable the CS 1000 supported voice codecs under Preferences > Voice Codec.
- Ensure that the fixed port range is defined. Navigate to Account Settings > Topology > Range of port used on this computer.
- Ensure the registration refresh time is set to 5 minutes. This keeps the registration timer short enough to recover quickly in case of network failure.
- To ensure the IP Softphone 3456 DTMF works with the Media Application Server (MAS), ensure that SIP > Account > Topology > Enable ICE is not selected.

For more information about the IP Softphone 3456, see the following documents:

- *Nortel IP Softphone 3456 User Guide* (NN43080-100)
- *Nortel IP Softphone 3456 Administration Guide* (NN43080-300)
- *Nortel IP Softphone 3456 Configuration Guide* (NN43080-600)

Redundancy

For redundancy, you can configure a leader-follower arrangement for a SIP Line Gateway (SLG) node with both of the servers sharing the same node IP address. However, clients on the same node can register only on current node master. No load sharing occurs between the two gateways.

Geographic Redundancy and Branch Office

Geographic Redundancy (GR) and Survivable Branch Office use the Geographic Redundancy N-Way data replication model. All Call Servers including the Main Office (MO), Geographically Redundant Main Office (GRMO), and Branch Office (BO) must have the same data stored based on this model.

For more information about Geographic Redundancy and Branch Office and for configuration information for the SIP IP Phones, see *Branch Office Installation and Commissioning* (NN43001-314).

SIP Line features

The following table lists the Line features provided to SIP Line Service.

Note: Features that are marked as not applicable in the following table have the same feature operation as other clients.

Table 4
Supported SIP Line features

Feature	See the following section or document	Notes
Account Code Capabilities and Forced Authentication Code	*Features and Services Fundamentals* (NN43001-106)	The server provides this feature using LD 88 configuration. No user invocation is required.
Attendant Console	*Features and Services Fundamentals* (NN43001-106)	No SIP Attendant Console.
Background Terminal	*Hospitality Features Fundamentals* (NN43001-553)	The SIP Line cannot be a Background Terminal (Hospitality feature).
Barge-in and Privacy	*Features and Services Fundamentals* (NN43001-106)	This feature is the Attendant Barge-in and Privacy to a call involved with SIP Line user. No user invocation is required.
Attendant Break-in	*Features and Services Fundamentals* (NN43001-106)	Supports Attendant Break-in into a SIP Line call.
Call Forward by Call Type	*Features and Services Fundamentals* (NN43001-106)	Call Forward by Call Type is defined by Class of Service (CLS) and External Flexible DN (EFD), HUNT, External Hunt (EHD), and Last Hunt Key (LHK). No user invocation is required.

Table 4
Supported SIP Line features (cont'd.)

Feature	See the following section or document	Notes
Call Forward All Calls (on Server)	"Call Forward All Calls - Server Side" (page 45)	On the server side, Call Forward All Calls (CFAC) is activated and deactivated by Flexible Feature Codes (FFC).
Call Forward All Calls (on Phone)	"Call Forward All Calls - Local" (page 46)	Call Forward All Calls (CFAC) on the client is defined on the local phone.
Call Forward Busy (on Server)	*Features and Services Fundamentals* (NN43001-106)	This feature is defined on the server using Class of Server (CLS) and Hunt DN. No user invocation is required.
Call Forward Busy (on Phone)	"Call Forward Busy—Client-Local " (page 47)	Call Forward Busy (CFB) on client is defined on local phone.
Call Forward – Don't Answer	*Features and Services Fundamentals* (NN43001-106)	This feature is defined on the server using Class of Server (CLS) and Hunt DN. No user invocation is required.
Call Hold	Local feature to the client. Refer to the client user guide.	Call Hold/Retrieve is implemented by pressing the Hold button on the telephone. No specific call processing occurs on the Call Server (this is only a media update activity).
Call Number Information Messages	*Features and Services Fundamentals* (NN43001-106)	This Hospitality feature is enabled by Class of Service (CLS). No user invocation is required.
Call Park and Retrieve	"Call Park/Retrieve" (page 47)	—
Call Pickup (Group) and Retrieve	"Group Call Pickup" (page 48)	—
Call Priority and Preemption	*Features and Services Fundamentals* (NN43001-106)	The Attendant Call Preemption feature is used to preempt a SIP Line user involved in a call. No special handling is required.
Call Transfer (Blind Transfer)	"Blind Transfer" (page 49)	A user uses the Transfer key on the client to invoke a transfer on the server.

Table 4
Supported SIP Line features (cont'd.)

Feature	See the following section or document	Notes
Call Transfer with Consultation	"Call Transfer with Consultation" (page 49)	A user uses the Transfer key on client to invoke a transfer on the server.
Call Conference, Server	"Server Conference" (page 50)	A client can select either server conference or local conference.
Call Conference, Local	"Local Conference" (page 51)	A client can select either server conference or local conference.
Call Waiting	"Call Waiting" (page 52)	—
Caller ID (Number/Text)	*Features and Services Fundamentals* (NN43001-106)	Delivery as in Call Party Name Display (CPND) configuration. No user invocation is required.
Calling number delivery	*Features and Services Fundamentals* (NN43001-106)	Delivery as in Call Party Name Display (CPND) configuration. No user invocation is required.
Calling name delivery	*Features and Services Fundamentals* (NN43001-106)	Delivery as in Call Party Name Display (CPND) configuration. No user invocation is required.
Calling Party Name Display Denied	*Features and Services Fundamentals* (NN43001-106)	CPND is denied for a user.
Charge Account Forced	"Forced Charge Account " (page 53)	Hospitality feature
Client password change	"Client password change" (page 65)	—
Client registration	"Client registration" (page 64)	Description of client registration and authentication.
Charge Accounting and Calling Party Number	"Charge Account and Calling Party Number" (page 54)	Hospitality feature
Controlled Class of Service	*Features and Services Fundamentals* (NN43001-106)	Hospitality feature. SIP user cannot be a controlling phone.
Direct Inward Dialing (DID) and Direct Outward Dialing (DOD)	*Features and Services Fundamentals* (NN43001-106)	DID and DOD are system-defined feature. No user invocation is required.
Directory access	Local feature to the client. Refer to the client user guide.	This feature depends on the client to have a local directory or access to a Lightweight Directory Access Protocol (LDAP) server. No service is provided by the SIP Line Gateway or Call Server.

Table 4
Supported SIP Line features (cont'd.)

Feature	See the following section or document	Notes
Distinctive ringing	Local feature to the client. Refer to the client user guide.	Distinctive ringing is a local phone feature. No service is provided by the SIP Line Gateway or Call Server.
Do Not Disturb (Make Set Busy) – Server	"Make Set Busy" (page 56)	Attendant Do Not Disturb (DND) is enabled and disabled on the Attendant Console. A user can also have individual Make Set Busy (MSB) functionality enabled by Flexible Feature Codes (FFC) dialing. The MSB/DND status is sent to user using a NOTIFY message.
Extension Mobility – ability to use unassigned phones	Not applicable	Lets a user register on any available phone. This feature is granted by default. A user registers with a user ID and password.
Flexible Direct Inward Dialing	*Hospitality Features Fundamentals* (NN43001-553)	This Hospitality feature is provided by system-level setup and provisioning. No user invocation is required.
Guest Entry of Automatic Wake-Up	"Guest Entry of Auto Wake Up" (page 57)	—
Hunting	"Call Forward Busy—Client-Local " (page 47)	This feature is defined by Class of Service (CLS) and Hunt DN for UEXT. Hunting is the same as Call Forward Busy (CFB).
Intercept Treatment	*Features and Services Fundamentals* (NN43001-106)	—
Last internal/external number redials	Local feature to the client. Refer to the client user guide.	Last number redial is supported only by the phone. This is a local feature.
Maid Identification	"Maid Identification " (page 58)	Hospitality feature
Meridian Hospitality Voice Services	*Hospitality Features Fundamentals* (NN43001-553)	Hospitality Feature. Provides voice mail to guests. No user invocation is required.

Table 4
Supported SIP Line features (cont'd.)

Feature	See the following section or document	Notes
Message Registration	*Hospitality Features Fundamentals* (NN43001-553)	This Hospitality feature is based on Class of Service (CLS). No user invocation is required.
Message Waiting Indication	"Message Waiting Indication" (page 59)	—
Message Waiting Indication Key Message Indication Key (MIK) and Message Cancellation Key (MCK)	*Features and Services Fundamentals* (NN43001-106)	This feature is supported only to let other clients use MIK and MCK (to turn the MWI lamp on or off) on a SIP Line phone. The SIP Line client cannot use the MIK/MCK key.
Multi-language Wake-Up	*Hospitality Features Fundamentals* (NN43001-553)	This Hospitality feature is provisioned by the administrator. The Multi-language Wake-Up feature can be selected by guests using the automatic wake-up setup. No user invocation is required.
Multi-tenant service	*Hospitality Features Fundamentals* (NN43001-553)	Multi-tenant service is a system-provided feature.
Multiple line appearances	"Multiple Line Appearance" (page 60)	You can configure multiple DNs for each user using Alias; however, you cannot make calls from a different DN. (Because Station Loop Preemption [SLP] always assumes calling from a primary DN.) Supports only identification of incoming calls on a different DN.
Music on Hold	*Features and Services Fundamentals* (NN43001-106)	MOH is a system-provided feature using a configured Recorded Announcement (RAN) route. No special operation required.
Missed call indication	Local feature to the client. Refer to the client user guide.	Missed call indication is a local phone feature. This feature depends on whether the phone has a missed call log.

Table 4
Supported SIP Line features (cont'd.)

Feature	See the following section or document	Notes
Pre-Translation	*Hospitality Features Fundamentals* (NN43001-553)	This Hospitality feature is similar to Speed Call operation. Pretranslation is defined by the administrator.
Property Management System Interface	*Hospitality Features Fundamentals* (NN43001-553)	This Hospitality feature is a system-provided feature. No interaction with SIP Line.
Ring Again Busy	"Ring Again Busy" (page 60)	This feature depends on whether the phone has a missed call log.
Ring Again No Answer	"Ring Again No Answer" (page 61)	This feature depends on whether the phone has a missed call log.
Room Status	"Room Status" (page 62)	Hospitality feature.
Shared Extensions on Multiple Phones	"Shared extensions on multiple phones" (page 62)	Multiple Appearance Directory Number (MADN) is supported only between SIP Line and other non-SIP Line telephones. Two or more SIP Line telephones within one MADN is not supported.
Single Digit Access to Hotel Services	*Hospitality Features Fundamentals* (NN43001-553)	This Hospitality feature allows single-digit dialing in hotel rooms. No special handling is required.
Speed dialing	"Speed Dial" (page 63)	—
Standard Boss-Secretary features	"Standard Boss Secretary" (page 64)	—
VIP Automatic Wake-Up	*Hospitality Features Fundamentals* (NN43001-553)	This Hospitality feature routes automatic wake-up calls for special guests to an attendant providing special services. This is system-provided feature. No special handling is required for SIP Line.

Call Forward All Calls - Server Side

Call Forward All Calls (CFAC) automatically forwards incoming calls to another destination, within or outside the system.

Feature implementation

Server-side CFAC is enabled and disabled by dialing the corresponding Flexible Feature Codes (FFC) (Call Forward Activate (CFWA) and Call Forward Deactivate (CFWD)) followed by the call forward to DN. After CFAC is enabled, all future calls are redirected immediately within the Call Server, no INVITE is sent to the SIP client.

Feature operation

Enable the CFAC feature on DN 3001. The CFWA FFC is defined as 5607 and CFWD FFC is defined as 5608.

Step	Action
1	Dial CFWA FFC + DN, for example, 56073001.
2	Listen for a confirmation tone (or dial tone, if no tone resource is available) to indicate that CFAC to the DN is enabled.
3	If you hear the busy or overflow tone then CFAC failed. Refer to the SIP response sent to the client for the failure: • 404 Not found—May due to FFC not defined. • 603 Declined—May due to access restriction.

--End--

Change CFAC to another DN.

Step	Action
1	Dial CFWA FFC + new DN, for example, 56073002. The CFAC DN changes to 3002.

--End--

Cancel CFAC to a DN.

Step	Action
1	Dial CFWD FFC + new DN, for example, 56083002.

The CFAC DN changes to 3002.

2 Listen for a confirmation tone (or dial tone, if no tone resource is available) to indicate that CFAC to the DN is disabled.

--End--

Note: You can use the PRT command in LD 11 to review the CFW DN.

Client behavior variant

All supported SIP IP Phones share the same operation when using CFWA FFC to enable CFAC.

CFWD FFC for deactivation accepts the FFC code for the IP Phone 1120E and 1140E.

Call Forward All Calls - Local

Call Forward All Calls (CFAC) automatically forwards incoming calls to another destination, within or outside the system.

Feature implementation

The SIP client can forward all calls to another DN. Refer to the user guide for the SIP client to enable or disable CFAC.

Feature operation

After client-local CFAC is enabled, the SIP client sends a 302 (Moved Temporarily) response to all incoming calls. The Call Server and SIP Line Gateway (SLG) treat this response similar to the CFAC feature on the server side and the following behavior is expected:

- Because extra messages are exchanged between the client and SLG and Call Server, the called party phone does not ring immediately (compared to server-side CFAC operation).
- The client can configure CFAC to any DN without DN validation or proper access restriction validation. This is standard practice. As a result, the call is not guaranteed to be successful. If the call fails (due to invalid DN or restricted access), the caller receives a ring back tone until the Call Forward No Answer (CFNA) feature is activated.

Note: To avoid user confusion, Nortel does not recommend client-local CFAC.

Client behavior variant

All supported SIP IP Phones share the same operation.

Call Forward Busy—Client-Local

Call Forward Busy (CFB) automatically routes incoming Direct Inward Dialing (DID) calls to the attendant console if a telephone is busy. This feature is allowed or denied in the Class of Service (Forward Busy Allowed [FBA] and Forward Busy Denied [FBD]) of the telephone.

Feature implementation

You can configure some phones to Call Forward to a DN if the client is busy. However, because all incoming calls go through the Call Server and the phone status is synchronized between the Call Server and the client, then client-local call forward busy is not triggered.

Client behavior variant

All supported SIP IP Phones share the same operation.

Call Park/Retrieve

Call Park (CPRK) places a call in a parked state, similar to hold, where it can be retrieved by an attendant console or telephone.

Feature implementation

There is no change for SIPL UEXT on the Call Park/Retrieve feature. For more information about this feature, see *Features and Services Fundamentals* (NN43001-106).

> ***Note:*** A Special Prefix (SPRE) code is required.

Feature operation

Park a call.

Step	Action
1	Initiate a blind transfer.
2	Dial SPRE + 71 followed by park to DN.
3	After you receive the ring back tone, complete the transfer.

--End--

Retrieve a parked call:

Step	Action
1	Dial SPRE + 72 followed by park to DN.

--End--

Zone Based Dialing support for Call Park and Call Retrieve

The Flexible Feature Code (FFC) must be used for Call Park/Retrieve to support Zone Based Dialing (ZBD) which always adds the zone prefix to a dial digit. To avoid the modification of the digit dialed, the FFC can be configured with a asterisk (*) at the beginning. The operation to park/retrieve a call is still the same except that FFC is used instead of SPRE.

Park a call.

Step	Action
1	Initiate a blind transfer.
2	Dial FFC CPRK code (for example, *123) followed by park to DN.
3	After you receive the ring back tone, complete the transfer.

--End--

Retrieve a parked call:

Step	Action
1	Dial FFC CPAC code (for example, *124) followed by park to DN.

--End--

Client behavior variant

All supported SIP IP Phones share the same operation.

Group Call Pickup

Call Pickup Group allows members of the same group to answer a call.

Feature implementation

The Group Call Pickup feature for SIP Line is implemented by using Call Pickup FFC (Pick Up Ringing Number code [PURN]). The related provisioning is the same as a regular UNIStim telephones:

- Define CO trunk priority in Element Manager (LD 15).
- Define pickup FFC in LD 57
- Define pickup group number and CLS in LD 11.

Feature operation

Pick up a ringing call in the same group.

Step	Action
1	Dial PURN FFC + DN to pick up a ringing call in the same group.

--End--

Client behavior variant

All supported SIP IP Phones share the same operation.

Blind Transfer

A blind transfer is a call that is transferred in one step.

Feature implementation

Transfer is enabled for all SIP IP Phones. No special implementation is required.

Feature operation

Enable a blind transfer.

Step	Action
1	During an active call, press the Transfer key provided by the SIP Line client.
2	Initiate a new call.
3	To complete the transfer, press the Transfer key again during ringing (blind transfer).

--End--

Client behavior variant

All supported SIP IP Phones share the same operation.

Call Transfer with Consultation

To activate the Call Transfer with Consultation feature, use the Transfer key on the SIP client to invoke call transfer on the server.

Feature implementation

Transfer is enabled for all SIP IP Phones. No special implementation is required.

Feature operation

Enable a consultive transfer.

Step	Action
1	During an active call, press the Transfer key provided by the SIP Line client.
2	Initiate a new call.
3	To complete the transfer, press the Transfer key again after transfer-to party answers (consultative transfer).

--End--

Client behavior variant

All supported SIP IP Phones share the same operation.

Server Conference

Conference adds additional parties to an established call.

Server Conference is only supported on the following SIP IP Phones:

- Nortel IP Phone 1120E
- Nortel IP Phone 1140E

Only local conference is available for the other SIP IP Phones.

Feature implementation

Server Conference is automatically enabled for all SIP IP Phones. No special implementation on the server is required. The Server Conference option must be selected on the SIP client.

Feature operation

Enable a Server Conference.

Step	Action
1	During an active call, press the Conference key provided by the SIP client.
2	Initiate a new call.
3	Press the Conf key to complete the conference.

--End--

The feature operation for the Nortel IP Phone 1120E and 1140E phones is as follows:

1. Establish the first call.
2. On the phone, select Action > New call / Conference.
3. Dial the destination of the second call.

   The second call is established.
4. Press Join.

   (The available options are 1.) Conference and 2.) 3-way call.)
5. Select 1 (to start Server Conference).

IP Phone behavior variant

Support for the Server Conference feature depends on whether the IP Phonehas the feature enabled. After the feature is enabled, all conference calls use the server resources; otherwise, the local conference resource is used. For server conference support of individual IP Phone types, see Table 3 "SIP IP Phone capabilities" (page 30).

Local Conference

Local Conference adds additional parties to an established call.

Local Conference is only supported on the following SIP IP Phones:

- Nortel IP Phone 1120E
- Nortel IP Phone 1140E

Feature implementation

Conference is enabled for all SIP IP Phones. No special implementation is required.

Feature operation

Enable a Local Conference.

Step	Action
1	During an active call, press the Conference (Conf) key provided by the SIP client.
2	Initiate a new call.
3	Press the Conf key to complete the conference.

--End--

The feature operation for the Nortel IP Phone 1120E and 1140E phones is as follows:

1. Establish the first call.
2. On the phone, select Action > New call / Conference.
3. Dial the destination of the second call.

   The second call is established.
4. Press Join.

   (The available options are 1.) Conference and 2.) 3-way call.)
5. Select 3 (to start a 3-way call [local conference]).

IP Phone behavior variant

Local Conference support is enabled on all IP Phone types. Some clients support both the Server Conference and Local Conference features. After Local Conference is enabled, all conference calls use the local conference resource on the phone. For server conference support of individual IP Phone types, see Table 3 "SIP IP Phone capabilities" (page 30).

> ***Note 1:*** In the local conference scenario, when a IP Phone is doing media mixing, it is the IP Phone’s responsibility and capability to send RFC 2833 digits received from one participant as RFC 2833 digits to other participants in the local conference. If an IP Phone does not have this capability, certain local conference capabilities will fail if one of the participants is expecting digits (e.g., when ICP or IVR is local conferenced).
>
> ***Note 2:*** When a participant in a local conference using SIP Line presses digits, the digits are sent as RFC 2833 to the SIP telephone. The SIP telephone performs the media mixing and converts the digits to in-band media. This imposes a limitation when interworking with a device that does not support in-band DTMF.

Call Waiting

Call Waiting notifies an active telephone that a second call is waiting to be answered on that Directory Number (DN).

Feature implementation

To enable the Call Waiting feature, you must configure Call Waiting Allowed (CWA) Class of Service (CLS) and Call Waiting (CWT) key on UEXT. Otherwise, the busy treatment is given.

Feature operation

If a user is active on a call, a new incoming call creates a new INVITE to the client. The client can accept the new call by placing the current call on Hold and answering the second call. The user can switch between two calls by pressing the DN key.

> ***Note:*** Instead of using Call Waiting, a two-line call can occur by configuring two DN keys of the same number on one UEXT to receive the second call.

Client behavior variant

All supported SIP IP Phones share the same operation. No specific configuration is required on the client with the exception on Teledex client.

To invoke Call Waiting on the Teledex client, do the following:

1. Enable Call waiting through the configuration portal.
2. Press Submit.
3. Go to the Advanced tab.
4. Select MLA Enabled.
5. Press Submit.
6. Reboot the Teledex set.

If the Teledex is in call on Line 1, do the following to place a call to a second line:

1. Initiate a second call to Teledex. (LED against second line glow. The Teledex is still in a call with first phone.)
2. Press the HOLD key on the Teledex to put first call on hold.
3. Press the second line key to answer the second call.
4. To go back to the call on Line 1, press the HOLD key to put Line 2 call on hold and then press Line 1 key to retrieve the original call.

Forced Charge Account

Forced Charge Account (FCA) temporarily overrides Class of Service limitations for toll-denied users. Use Forced Charge Account long-distance calls to an account number when you call from a telephone that is restricted from making long-distance calls. The unrestricted Class of Service provided by FCA applies for the duration of the call.

Feature implementation

The Forced Charge Account feature implementation for SIP Line is the same as for other phone types. The implementation steps are as follows:

- Define Forced Charge Account (FCA) in Element Manager (LD 15).
- Define Special Prefix (SPRE) code in Element Manager (LD 15).
- Disable Forced Charge Account Restriction (FCAR) in LD 11.

Feature operation

To initiate a forced charge account call from a SIP Client, use SPRE code as described in the following procedure.

Step	Action
1	To initiate a call, enter the SPRE + 5 + charge account number + # + E.164 number, for example: • SPRE = 369 • Charge account number = 1234 • E.164 number = 011918040217120 for international call You enter the following for an international call: 36951234#0119 18040217120
2	Press Send.

--End--

Client behavior variant

Some phones (for example, Nortel IP Phone 1100 Series) treat the number symbol (#) as the end of dialed digits. For the feature to operate properly, the user must enter the full string before pressing the DN key.

Charge Account and Calling Party Number

Used with Call Detail Recording (CDR), Charge Account bills calls directly to specific accounts or charge numbers instead of Directory Numbers (DN).

Feature implementation

The Charge Account feature implementation for SIP Line is the same as other phone types and uses the following steps:

- Define Forced Charge Account (FCA) in Element Manager (LD 15).
- Define Special Prefix (SPRE) code in Element Manager (LD 15).
- Disable Forced Charge Account Restriction (FCAR) in LD 11.

Feature operation

Initiate a charge account call from a SIP client.

Step	Action
1	Enter the SPRE + 5 + charge account number + # + E.164 number, for example: • SPRE = 369 • charge account number = 1234 • E.164 number = 011918040217120 for an international call You enter 36951234#011918040217120.
2	Press Send.

--End--

The following operations are not supported for SIP Line:

- Enter the charge number during an established call.
- Enter the charge number to transfer or conference a call.
- Record the calling party number for accounting purposes.

Client behavior variant

Some phones (for example, Nortel IP Phone 1100 Series) treat the number symbol (#) symbol as the end of dialed digits. For the feature to operate properly, the user must to enter the full string before pressing he DN key.

Call Party Name Display

Call Party Name Display (CPND) identifies the calling or called number in addition to the DN. The identifier (for example, the name) associated with a DN on telephones with an alphanumeric display is defined in LD 95.

Feature implementation

The CPND for the SIP Line configuration is the same as for other client types and uses the following steps:

- Define CPND allowed or denied CLS in LD 11.
- Define name display for UEXT in LD 11.
- Enable Network Calling Name Allowed (NCNA) and Network Call Redirection (NCRD) for SIP Line route in LD 16.
- Configure ND2 for RCAP for the D-Channel of the SIP Line route.

Feature operation

CPND is delivered to SIP Line as part of the call setup in the INVITE message.

Client behavior variant

CPND and Calling Line Identification (CLID) are not updated for Call Transfer because none of the SIP IP Phones update the display upon receiving a REINVITE message. Only the IP Phone 1120E and IP Phone 1140E phones update the display for simple calls and CFW calls. For CPND to work with a SIP client, the client must support P-Asserted-Identity header as described in RFC3325.

The entire SIP URL string, including phone-context, is shown on the IP Phone 1120E and 1140E. While other client types only display the digits (without phone-context). As a result, the “dialing from call-log” behaves differently for various clients. (In particular, for UDP dialing because UDP does not have the AC1 or AC2 codes in the SIP URL.) User manual dialing is required. This is the same behavior as IP Phone’s Personal Directory (PD) operation, where the caller’s number on PD only shows the DN without AC1.

Make Set Busy

The Make Set Busy (MSB) feature ensures a telephone appears busy to all incoming calls. Outgoing calls can still be made from the telephone.

Feature implementation

To make a set busy, use the following steps:

- Define MSB key in LD 11.
- Define Make Set Busy Allowed (MSBA) and Make Set Busy Denied (MSBD) FFC in LD 57.

Feature operation

To enable MSB, dial MABA FFC, then hang up after you receive the confirmation tone or ring back tone.

To disable MSB, dial MSBD FFC, then hang up after you receive the confirmation tone or ring back tone.

Client-Local Make Set Busy

Many clients have built-in Make Set Busy (MSB) or Do Not Disturb (DND) features. Because of this local behavior, the SIP Line servers are not notified about the activity. As a result, incoming calls to this type of SIP client do not receive the busy treatment; instead, Call Forward No Answer (CFNA) is given if it is configured. If CFNA is not configured, the caller hears only the ring back tone.

Guest Entry of Auto Wake Up

An attendant can enter a wake-up request on the Background Terminal (BGD); a guest can enter a wake-up call on the room telephone.

Feature implementation

The Auto Wake Up feature implementation for SIP Line is the same as for other phone types, with one additional step to configure Auto Wake-up FFC (Automatic Wake Up Allowed [AWUA], Automatic Wake Up Denied [AWUD], and Automatic Wake Up Verify [AWUV]) in LD 57.

Feature operation

Enable the Auto Wake Up feature.

Step	Action
1	Dial AWUA FFC + HHMM (where HHMM is the time in hours and minutes).
2	Listen for a confirmation tone or ring back tone to indicate that Auto Wake Up is enabled.
3	Hang up.

--End--

Disable Auto Wake Up.

Step	Action
1	Dial AWUD FFC + HHMM (where HHMM is the time in hours and minutes).

2	Listen for a confirmation tone or ring back tone to indicate that Auto Wake Up is cancelled.
3	Hang up.

--End--

Verify a wake-up setting.

Step	Action
1	Dial AWUV FFC + HHMM (where HHMM is the time in hours and minutes).
2	Listen for a confirmation tone or ring back tone to indicate that Auto Wake-up is enabled.
3	Hang up.

--End--

Client behavior variant

All supported SIP IP Phones share the same operation.

Maid Identification

The Maid Identification, or Maid ID, feature makes it easy to track which maids clean which rooms.

Feature implementation

The Maid Identification feature implementation for SIP Line is the same as for other phone types, with one additional step to configure Room Status (RMST) FFC in LD 57.

Feature operation

Enable the Maid Identification feature.

Step	Action
1	Dial RMST FFC + Room Status code + * + MaidID + #.
2	Listen for a confirmation tone or ring back tone, which indicates that the feature is successfully invoked.
3	Hang up.

--End--

Client behavior variant

All supported SIP IP Phones share the same operation.

Message Waiting Indication

The Message Waiting Indicator indicates that a message was left for the user. This indicator also flashes after the phone ringer is on.

Feature implementation

Message Waiting Indication (MWI) is delivered to a client after voice mail is configured. The configuration is the same configuration as for other phone types.

Feature operation

MWI is delivered to a phone by using implicit NOTIFY. No special user interaction is required.

Client behavior variant

See the user guide for the SIP Line client for MWI indication location and description.

Multiple Appearance DN (MADN)

For SIP Line, a SIP user can only have one DN. The appearance of multiple DNs on a single SIP client is not supported.

If you have two SIP IP Phones, use MADN to tie two TNs to one single DN. The SIP client only shows one DN; however, when one DN rings, both SIP IP Phones ring. The active session is on the phone where the call is answered.

Feature implementation

You can configure different TNs with the same DN in a MADN group. If you configure two SIP Line users in one MADN group, they must be on a different UEXT with a different user ID defined.

Feature operation

The feature operation is maintained, and if the Multiple Appearance Directory Number Redirection Prime (MARP) is enabled, the same MARP rule applies to the SIPL UEXT.

Client behavior variant

All supported SIP IP Phones share the same operation.

Multiple Line Appearance

For SIP Line, the Multiple Line Appearance (MLA) feature refers to multiple DN keys defined on one UEXT, the TNs has to be the same DN for SIPL UEXT. (However, with UNIStim telephones, the MLA can have different DN keys showing on the same TN.)

Feature implementation

Each SIP Line user can have only one DN. If Multiple Line Appearance is required, all DNs must be the same on a single UEXT.

Note: Multiple Line Appearance on one TN is a special case of MADN.

Feature operation

Newly received incoming calls create a new INVITE message and send the message to the phone (similar to a call waiting operation).

Client behavior variant

All supported SIP IP Phones share the same operation.

Ring Again Busy

Ring Again (RGA) gives you the opportunity, after you encounter a busy Directory Number (DN), to ring the DN again after it becomes free. If a dialed DN is busy, or if all trunks are busy, pressing the Ring Again key asks the system to monitor the dialed DN or trunk. You are notified (by the system) after the DN becomes available. The call is automatically dialed again after you press the Ring Again key a second time.

Feature implementation

Configure the Ring Again Activate (RGAA) and Ring Again Deactivate (RGAD) FFC in LD 57.

The original call gets the busy status and hangs up. The SIP call dialog is gone. As a result, after the far-end idle indication is sent to client, it replies (on the client) and tells the client to call back using its missed call log.

Feature operation

Enable the Ring Again Busy feature.

Step	Action
1	Dial the DN.
2	Hang up if you receive a BUSY response from the far end.
3	Dial FFC RGAA code within 30 seconds to enable RGA.
4	If RGA Busy is enabled using FFC, the SIP Line client receives a call back after the other party is free.

5	The SIP Line client then can use the missed-call-log to dial back.
6	The same Ring Again Busy operation applies to target over a trunk interface as well, including Meridian Customer Defined Network (MCDN) and QSIG interfaces.

--End--

RGA can be cancelled if the user dialed RGAD FFC (Ring Again Disable) before RGA is invoked. Dialing RGAD FFC after RGA was invoked does not have any impact on the call.

Client behavior variant

All supported SIP IP Phones share the same operation.

Ring Again No Answer

The Ring Again No Answer (RANA) feature extends the capabilities of Ring Again for stand-alone applications, and Network Ring Again for Integrated Services Digital Network (ISDN) applications. The feature allows Ring Again to be applied to a station that does not answer.

Feature implementation

Configure RGAA and RGAD FFC in LD 57, and enable the RNA option in Element Manager (LD 15).

The original call receives the busy status and hangs up. The SIP call dialog is gone. As a result, after the far end idle indication is sent to the client, it replies (on the client) and tells the client to call back using the missed call log.

Feature operation

Enable the Ring Again No Answer feature.

Step	Action
1	Dial the DN.
2	Hang up if the far end does not answer.
3	Dial FFC RGAA code within 30 seconds to enable RGA.
4	If RGA No Answer is enabled using FFC, the SIP Line client receives a call back after the other party makes a call.
5	The SIP Line client then can use the missed call log to dial back.

--End--

RGA can be cancelled if the user dialed RGAD FFC (Ring Again Disable) before RGA is invoked. Dialing RGAD FFC after RGA was invoked does not have any impact on the call.

Client behavior variant

All supported SIP IP Phones share the same operation.

Room Status

The Room Status (RMS) feature sets conditions on rooms such as whether a room requires cleaning, or whether a room is occupied or vacant. Room Status is managed through the Background Terminal (BGD).

Feature implementation

Room Status feature implementation for SIP Line follows the same as other phone types, with one additional step to configure Room Status (RMST) FFC in LD 57.

Feature operation

Enable the Room Status feature.

Step	Action
1	Dial RMST FFC + Room Status code.
2	Listen for a confirmation tone or ring back tone, which indicates that the feature is successfully invoked.
3	Hang up.

--End--

Client behavior variant

All supported SIP IP Phones share the same operation.

Shared extensions on multiple phones

Feature implementation

Configure the SIPL UEXT within any Multiple Appearance DN (MADN) group. No special provisioning is required for SIP Line.

Feature operation

SIP Line in a MADN group has the same feature operation as for other phone types, except for the following:

- SIPL UEXT follows the same Multiple Appearance Directory Number Redirection Prime (MARP) rule as other phone types.
- Two SIPL UEXT can share the same DN; however, the user IDs must be different.

Client behavior variant

All supported SIP IP Phones share the same operation.

Speed Dial

If a user wants to initiate outgoing dialing, and the system expects a phone number, the user can enter a special prefix to indicate the use of short dialing features, followed by one to three digits indicating which number to use.

Feature implementation

The Speed Dial feature provisioning for SIP Line is the same as for other telephone types, with one additional step to configure the Speed Call User (SPCU) FFC in LD 57.

> ***Note:*** Only one Speed Call User (SCU) key is supported. If you configure more than one SCU key, the lowest configured key is used.

Only the Speed Call user is supported for the SIP Line client. Use Speed Call to place calls by dialing a one-, two-, or three-digit code. You can use Speed Call for internal and external calls. Speed Call Controller is an administrative feature that is not available for SIP Line users.

Feature operation

Enable the Speed Dial feature.

Step	Action
1	Enter SPCU FFC + speed call index as a single string.
2	Press Send.

--End--

Client behavior variant

All supported SIP IP Phones share the same operation.

Standard Boss Secretary

A boss can forward incoming calls to a secretary or multiple secretaries for screening.

Feature implementation

Configure the SIPL UEXT as either a boss phone or a secretary phone. Configuration is the same as for other phone types, with one additional step to define Secretarial Filtering Access (SFAC) FFC in LD 57.

Feature operation

Enable the Standard Boss Secretary feature.

Step	Action
1	Dial SFAC FFC + filter code.
2	Listen for a confirmation tone or ring back tone that indicates that the feature is operating successfully.
3	Hang up.

--End--

Client behavior variant

All supported SIP IP Phones share the same operation.

Client registration

Client registration requires a password. All client passwords are defined as a Station Control Password (SCPW) in LD 11. To obtain the SCPW prompt in LD 11, you must configure the Station Control Password Length (SCPL) to the desired number of digits in FFC data in LD 15. You must also configure DFLT_SCPW to NO (which is the default value).

Feature implementation

Define UEXT for each SIP user. See "Configure SIP Line users" (page 100).

Feature operation

Enable the client registration feature.

Step	Action
1	Connect the client to the network.

2 Configure the following options:

- Proxy IP address and port
- User ID and password

3 Log on.

--End--

Client behavior variant

Each client type has different configuration steps for the proxy, user ID, and password. For specific SIP client configuration details, see the user guide for the SIP client.

The standard recovery strategy for any registration failure is to log off of the previous SIP client. If the SIP Line Gateway misses the log off by the original SIP client, then a different client cannot register. The solution is to apply the standard procedure for logging on and logging off the original SIP client.

If the client experiences a power failure or a LAN failure, the registration record remains active on both the SIP Line Gateway and Call Server until the registration timer expires.

The Teledex phones do not have the logout capability. As a result, you must reboot the phone to force it re-register. There is no mechanism to force the phone to unregister from the SIP Line Gateway (SLG) and Call Server (unless you unplug the phone and wait for its old registration record on SLG to timeout).

The Teledex phones do not send a keepalive message to the SLG. As a result, if the SLG is restarted, then the Teledex phone must be manually restarted to force it to re-register with the SLG.

Client password change

The administrator initially defines all client passwords as a Station Control Password (SCPW) in LD 11.

Feature implementation

A client can change the password after the password is successfully registered with the SIP Line Gateway by using the Station Control Password Change (SCPC) FFC.

Feature operation

Change a client password.

```
<FFC> <old password> <new password> <new password>
```

Step	Action
1	Enter the SCPC FFC code to change the SCPW followed by the old SCPW.
2	Enter the new SCPW.
3	Enter the new SCPW again.
4	Press Send.
5	Listen for the confirmation tone, and then press the Release key.

--End--

Client behavior variant

The Station Control Password (SCPW) must be only digits. The password is either four or eight digits in length (which is defined by LD 15).

To change the SCPW, the client dialing buffer must accommodate the following digit string of length: FFC+OldPwd+NewPwd+NewPwd. The following table shows the dialing buffer size for each phone.

Table 5
Dialing buffer sizes

Telephone	Dialing buffer size
Nortel IP Softphone 3456	Buffer greater than 100
Nortel IP Phone 1120E and 1140E	Buffer of 25

In general, you cannot change an eight-digit password on an IP Phone 1120E or 1140E because the number of digits (FFC+8+8+8) exceeds the display buffer.

Client-based call decline

Most of the SIP IP Phones have the built-in functionality to dynamically decline an incoming call, by either sending a 486 Busy response or a 603 Decline response back to the INVITE message. Upon receiving such response, the call is dropped on the SIP side; however, the client UEXT PDN remains busy.

The following behavior is expected:

- The caller hears the ringback tone all the time, until Call Forward No Answer (CFNA) treatment starts (if CFNA is configured)
- The called SIP Line client cannot receive or make phone calls until the caller hangs up or CFNA starts.

Feature implementation

The following feature behavior is expected:

- The caller hears the ringback tone all the time, until Call Forward No Answer (CFNA) treatment starts (if CFNA is configured)
- The called SIP Line client cannot receive or make phone calls until the caller hangs up or CFNA starts.

Feature operation

Depending on the SIP client type, you can select Decline to reject an incoming call during the ringing phase.

Zone Based Dialing support

SIP Line is supported for Zone Based Dialing (ZBD) where a Call Server centrally routes calls for all its gateways by assigning them to different numbering zones with unique zone prefixes for identification. The ZBD feature is transparent to SIP Line except that the zone prefix of the originating party is always added to the dialed digits. Therefore, SIP Line works as existing set types in a ZBD environment except for the following features/functions:

- DN display for idle client
- Call Park and Call Retrieve

DN display for idle client

For existing clients, its DN is displayed when it is idle. For ZBD, the DN is a 7-digit DN with the first few (for example, 3) digits representing the zone prefix.

For users in the same zone (for example, the same office), they can dial four digits to reach one another. Therefore, it is expected in a ZBD environment that the DN display for an idle client is four digits.

For existing clients, the displayed DN is sent by the Call Server and Terminal Proxy Server (TPS) to the client and the zone prefix is removed before it is sent to the client in a ZBD environment.

No DN is displayed for a SIP client. The SIP client displays the user name which is entered directly in it. For SIP Line, this user name must be the same as the name that is configured in the Call Server. Usually, the user name is alphanumeric; however, in some cases, the name can be equal to the 7-digit DN. There is no mechanism to remove the first 3 digits for display. It is out of the control of the Call Server. Therefore, all 7 digits are displayed in this case.

Call Park and Call Retrieve

You must use the Flexible Feature Code (FFC) instead of the Special Prefix (SPRE) code to park and retrieve calls from a SIP Line IP Phone. For more information, see "Zone Based Dialing support for Call Park and Call Retrieve" (page 48).

Planning and engineering

The CS 1000 telephony features provided by SIP Line operate differently on various SIP IP Phones and the functionality of the feature depends of the capabilities of the SIP IP Phone. For more information, see "SIP Line features" (page 39).

This section contains the following topics:

SIP Line Service packaging

The SIP Line Service depends on the following packages to be enabled in the keycode.

Table 6
Feature packaging

Package mnemonic	Package number	Package description	Package type	Applicable market
SIP_LINES	417	SIP Line Service package	New package	Global
FFC	139	Flexible Feature Codes	Existing package	Global
SIPL_NORTEL	415	Nortel SIP Line package	Existing package	—
SIPL_3RDPARTY	416	Third-party SIP Line package	Existing package	—

The FFC package is required only to enabled FFC features. The Nortel SIP Line and Third-Party SIP Line packages are needed only if SIP Line supports the respective IP Phone type.

SIP Line is bound by SIP_LINES package (417). This package must be enabled to perform the following activities:

- Configure SIP Line IP Phones.
- Enable the SIP Line feature.

Use Element Manager or LD 22 to view the state (enabled or disabled) of the SIP_LINES package (417). To enable the SIP_LINES package, see "Enable the SIP Line Service and configuring the root domain " (page 80).

RFC standard compliance

The SIP Line Service complies with the following Request for Comments (RFC):

- RFC3261—SIP: Session Initiation Protocol
- RFC3264—An Offer/Answer Model with Session Description Protocol (SDP)
- RFC3265—Session Initiation Protocol (SIP)-Specific Event Notification (Subscribe/Notify)
- RFC3515—The Session Initiation Protocol (SIP) Refer Method
- RFC3891—The Session Initiation Protocol (SIP) Replaces Header
- RFC4244 —An Extension to the Session Initiation Protocol (SIP) for Request History Information
- SIP System Requirement Document (SRD) version 4.3

Capacity

The *Communication Server 1000E Planning and Engineering* (NN43041-220) and *CP PM Co-resident Call Server and Signaling Server Fundamentals* (NN43001-509) describe the maximum number of SIP Line users for each SIP Line Gateway and the maximum number of SIP Line users for each system.

For TN space planning, each SIPL UEXT requires one SIP Line Virtual Trunk (VTRK) on each call for the duration of the call. SIP Line VTRK is not calculated against Incremental Software Management (ISM) licenses. There must be a 1:1 ratio between SIPL UEXT and SIPL VTRK TN.

Configure all SIP Line users as the SIPL UEXT type and they operate the same as other line types, with the exception that you must assign one additional SIP Access Point for each user. Otherwise, in terms of TN planning and traffic planning, the same line and trunk calculations apply to the SIP Line feature.

For each SIP Line user, two TNs are involved from Call Server perspective. For the SIP Line user to work properly, two TNs are involved: one for the SIP Line and the other for the SIP Line virtual trunk.

Operating parameters

The SIP Line feature has the following operating parameters:

- The SIP Line Service (in CS 1000 Release 6.0) cannot co-reside with other applications. The SIP Line Service is a stand-alone application and cannot co-reside with UNIStim LTPS or Gateway applications such as SIP Gateway or H.323 Gateway.
- Only one IP Phone for each user ID can be registered at a time. A second registration attempt (while first IP Phone is still registered) is rejected.
- The Make Set Busy (MSB) lamp status update depends on the supported the phone types.
- The Ring Again On Busy and Ring Again No Answer (RANA) feature notifications depend on whether the phone has a missed call log.
- The Flexible Feature Codes (FFC)-enabled feature suite only applies to the features listed in Table 3 "SIP IP Phone capabilities" (page 30).
- SIP Line cannot be converged desktop user.
- SIP Line cannot be in the same MADN group as converged desktop (since SIP Line cannot be converged desktop user and converged desktop requires all TNs in the same MADN group has the same CLS).
- SIP Line supports Multiple Appearance Directory Number (MADN). However, for SIP Line users, MADN is supported only when using two SIPL UEXT with two different user IDs. Also, MADN is supported on the single IP Phone with two lines but only with the same DN.
- Multiple Line Appearance is supported only with the same DN. Specifically, only one DN can appear on a SIP Line phone, but it may appear more than once.
- The SIP Line feature cannot be on an Automatic Call Distribution (ACD) agent phone.
- This release does not support the following features:
  - Name dial
  - Proactive Voice Quality Management (PVQM)
  - Media security: The SIP Line IP Phones and trunks do not support media security. The Class of Service (CLS) must be set to Media Security Never (MSNV) for SIP Line UEXT and SIP Line trunks.

(This ensures that SIP media security negotiation issues do not occur.)

- HELD SDP sent by the Nortel IP Phone 1120E or 1140E is not RFC2543 and RFC3264 compliant. As a result, SIP endpoints which strictly follow RFC 3264 can have issues when the phone holds the call.

Robustness

The Teledex phone has some vulnerabilities when deployed in hotel guest rooms.

- If the data network to which the Teledex phones are connected is isolated such that room-to-room data traffic is restricted, then the vulnerabilities identified only expose the phone within a guest to attack by the room occupant which would be of little value. In this type of deployment, the vulnerabilities are not an issue.
- The planned use of 802.1x in the Teledex phones to authenticate these devices onto the network will not prevent the core network from an attack originating within a guest room. This is known as a man-in-the-middle attack. The data network must be designed to restrict access to the core network from the guest rooms by way of the LAN connection to these (or any other) IP room phones.

  Note: After the victim computer has authenticated and the switch port is open, the attacker can connect to resources on the protected network because there is no per-packet authentication of the traffic once the port is open. Since the shadow computer has the same MAC and IP addresses as the victim computer, from the point of view of the switch it appears only as if there is a single computer connected to the port. This man-in-the-middle attack occurs because 802.1x does not follow-up per-packet authentication. 802.1x only authenticates the connection and assumes all traffic that is flowing over the connection is legitimate.

Installation

You install the SIP Line application using the Centralized Deployment Manager (a component of Unified Communications Management [UCM]). The Centralized Deployment Manager is used to remotely deploy application software to the Linux servers from a central location (using the primary security server). See Figure 7 "CS 1000 task flow" (page 74).

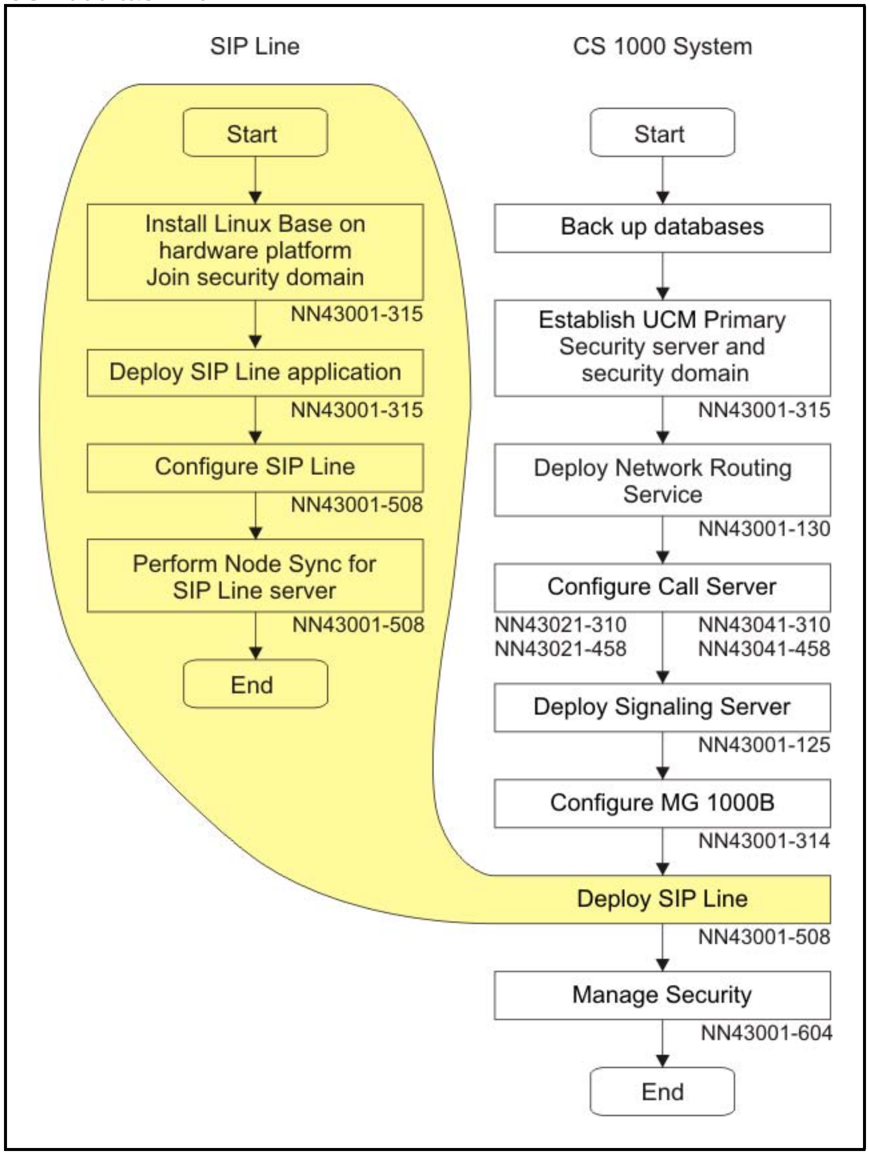
You must upgrade the CS 1000 system to Release 6.0 to enable and configure the SIP Line feature. The SIP Line Gateway and SIP Line Service form one software bundle in CS 1000 Release 6.0. You must select this software bundle when you install SIP Line.

> ***Note:*** In CS 1000 Release 6.0, the SIP Line application must be a stand-alone application. SIP Line cannot co-reside with the Line Terminal Proxy Server (LTPS) or with other virtual trunk applications (such as SIP Gateway or H.323 Gateway). For more information, see "Configuration using Element Manager" (page 79).

CS 1000 task flow

This section provides a high-level task flow for the installation or upgrade of a CS 1000 system. The task flow indicates the recommended sequence of events to follow when configuring a system and provides the NTP number that contains the detailed procedures required for the task.

Figure 7
CS 1000 task flow



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

- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)
- *Network Routing Service Fundamentals* (NN43001-130)
- *Communication Server 1000M and Meridian 1 Large System Installation and Commissioning* (NN43021-310)
- *Communication Server 1000M and Meridian 1 Large System Upgrades Overview* (NN43021-458)

- *Communication Server 1000E Installation and Commissioning* (NN43041-310)
- *Communication Server 1000E Software Upgrades* (NN43041-458)
- *Signaling Server IP Line Applications Fundamentals* (NN43001-125)
- *Branch Office Installation and Commissioning* (NN43001-314)
- *Security Management Fundamentals* (NN43001-604)

Upgrades

You must upgrade the CS 1000 system to Release 6.0 to enable and configure the SIP Line feature. In CS 1000 Release 6.0, the SIP IP Phone telephony users are configured as Universal Extensions of subtype SIPL. The SIP Line Gateway (SLG) is configured using Element Manager. For more information, see "Configuration using Element Manager" (page 79)

For more information, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Configuration using Element Manager

Use Element Manager to enable and configure the SIP Line Service on CS 1000.

You must perform the following tasks to configure the SIP Line Service:

- Enabling the SIP Line services and configuring the root domain.
- Configure the SIP Line gateway.
- Configure the D-channel over IP.
- Configure the AML over ELAN links.
- Configure the VAS ID association with AML over ELAN link.
- Configure the SIP Line routes.
- Configure the SIP Line Virtual Trunks.
- Configure the SIP Line users.
- Configure the Universal Extensions of subtype SIPL.

A command line interface (CLI) option is available to provision the SIP Line application on CS 1000 system. For detailed information about the Call Server overlays associated with enabling the SIP Line application on CS 1000, see "Configuration using Call Server configuration overlays" (page 109).

Log in to Unified Communications Management and Element Manager

Before you can start Element Manager, you must first log on to the Unified Communications Management (UCM).

Procedure 1
Logging on to UCM and Element Manager

Step	Action
1	Open the Web browser.

2 Enter one of the following in the Address bar, and then press **Enter**:

- UCM framework IP address—After you enter the UCM framework IP address, a Web page appears stating that you must access Unified Communications Management by using the Fully Qualified Domain Name (FQDN) for the UCM server. Click the link on this Web page to use the FQDN for the UCM server.
- FQDN for the UCM server.

3 Click **OK** or **Yes** to accept the security windows that appear.

The **UCM Login** Web page appears.

4 In the **User ID** field, enter your user ID.

5 In the **Password** field, enter your password.

6 Click **Log In**.

The default navigation Web page for UCM appears.

7 On the **Elements** page of Unified Communications Management, under the **Element Name** column, click the server name to navigate to Element Manager for that server.

The CS 1000 Element Manager page appears.

--End--

Enable the SIP Line Service and configuring the root domain

The SIP Line Service Package (417) must be equipped to enable the SIP Line feature on a CS 1000 system. Within Element Manager, you must then enable the SIP Line Service and configure the root domain at the customer level.

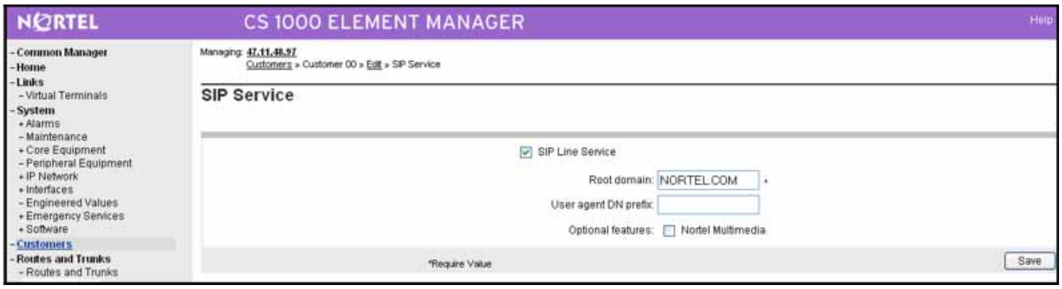
Perform the following procedure to enable the SIP Line Service and to configure the root domain.

Procedure 2
Enabling the SIP Line Service and configuring the root domain

Step	Action
1	Log on to Element Manager. See Procedure 1 “Logging on to UCM and Element Manager” (page 79).
2	In the navigation pane, select **Customers**.
3	On the **Customers** page, click the customer number.
4	On the **Edit** page, click **SIP Line Service**.

The SIP Service page appears.

Figure 8
SIP Service



5 On the **SIP Service** page, select the **SIP Line Service** check box.

The other parameters on the screen are enabled after you select the SIP Line Service check box.

6 In the **Root domain** field, enter domain name of the root domain for the SIP Line service. The domain name can be a maximum of 15 characters in length. It can include any of the 52 alphabetic characters A–Z (upper case) and a–z (lower case), and the digits 0–9. The hyphen (-) is allowed; however, the underscore (_) cannot be used in the domain name.

7 In the **User agent DN prefix** field, enter a DN prefix to build the HOT U key information for SIP Line phones.

The DN cannot conflict with the current system.

> ***Note:*** The User Agent DN prefix field is the same as the UAPR prompt in LD 15 and is used on the Phones page in Element Manager. For more information User agent DN prefix and HOT U key, see Step 17 in Procedure 11 “Configuring SIP Line users in Element Manager” (page 101). For more information about the UAPR prompt, see Table 10 "LD 15 Configure SLS_DATA" (page 111).

8 Ensure the **Nortel Multimedia** check box is cleared.

> ***Note:*** This check box is not used in CS 1000 Release 6.0 and is reserved for future development. This check box will enable the use of Nortel multimedia features on the phones (instead of using third-party multimedia features).

9 Click **Save**.

--End--

Configure the SIP Line Gateway service

Enable and configure the SIP Line Gateway (SLG) service within Element Manager.

The SLG application requires parameters to be stored inside the config.ini file. In the config.ini file, the SLG-specific configuration parameters are stored in the SIP Line Service section.

WARNING
Use Element Manager to manage the config.ini file. Do not manually edit the config.ini file.

Use the IP Telephony Node page in Element Manager to add or edit nodes. This page displays each node that is saved on the Call Server where Element Manager starts and provides details about the node such as node ID, components, configured application services, IP address information, and over status of the node. The node status provides information about whether the node is synchronized, changed, or failed:

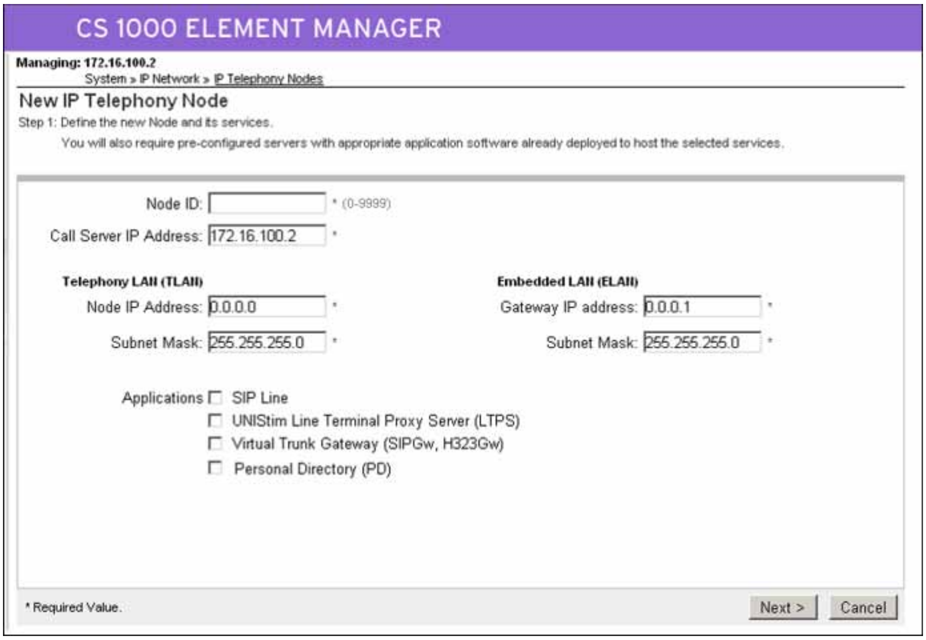
- Synchronized status: Indicates that all node elements are updated with the most recent configuration files from the Call Server.
- Changed status: Indicates that the configuration has changed on the Call Server; however, the elements are not updated.
- Failed status: Indicates that the transfer of the configuration files to the node element failed upon last attempt.

ATTENTION
As part of the SIP Line Gateway configuration, you must restart the applications for the SIP Line Service to operate properly.

Procedure 3
Configuring the SIP Line Gateway service

Step	Action
1	In the navigation pane, select **System > IP Network > Nodes: Servers, Media Cards**.
2	On the **IP Telephony Nodes** page, click **Add**. The **New IP Telephony Nodes** page appears.

Figure 9
New IP Telephony Node



3 On the **New IP Telephony Nodes** page, in the **Node ID** field, enter the node ID. The range is 0 to 9999.

4 In the **Call Server IP Address** field, enter the ELAN IP address of the Call Server.

5 Under the **Telephony LAN (TLAN)** section, enter the **Node IP Address** and **Subnet Mask** of the TLAN.

> ***Note:*** That this is not the TLAN Ethernet IP address but the node IP address.

6 Under the **Embedded LAN (ELAN)** section, enter the **Gateway IP address** and **Subnet Mask** of the ELAN.

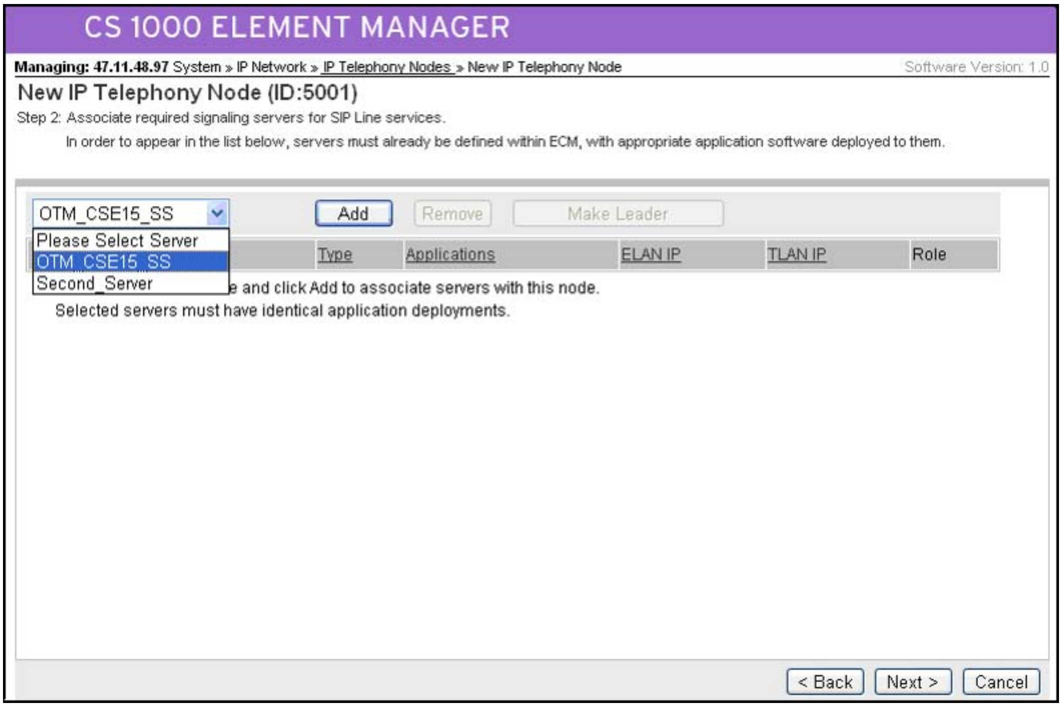
7 Under **Applications**, select the **SIP Line** check box.

> ***Note:*** The SIP Line feature is a stand-alone feature and cannot co-reside with UNIStim Line Terminal Proxy Server (LTPS), other gateway applications such as SIP Gateway (SIPGw) or H.323 Gateway (H323Gw), or the Personal Directory (PD).

8 Click **Next**.

The page to add servers to the node appears.

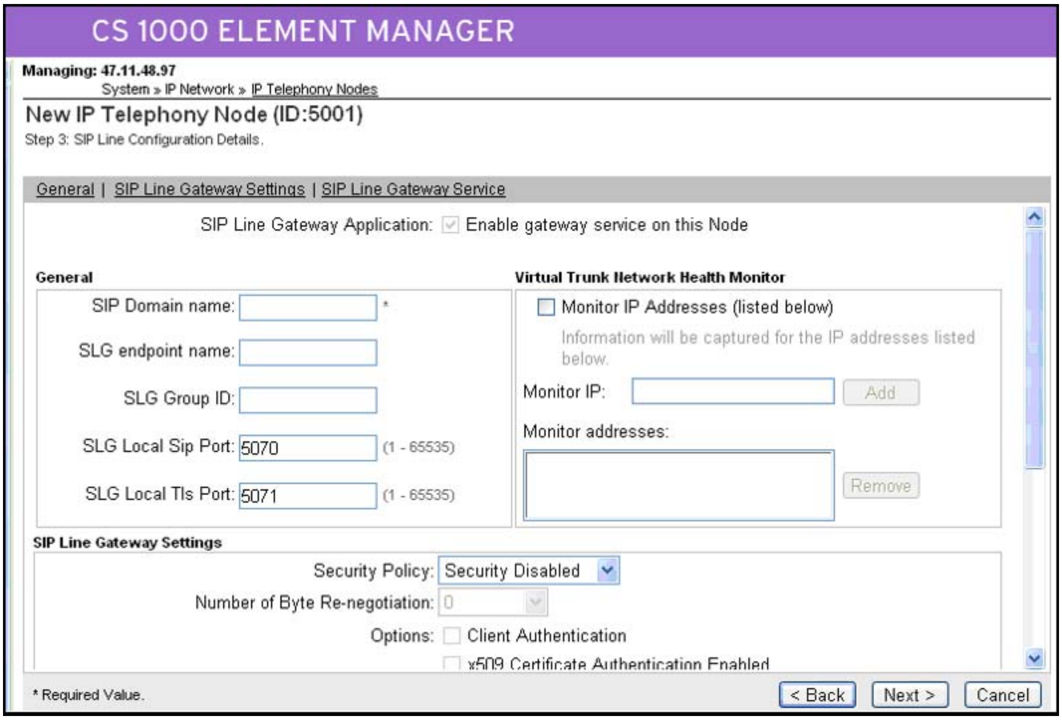
Figure 10
New IP Telephony Node–Add Server



9. On **Add Server** page, from the **Please Select Server** list, select the server to add to the node.
10. Click **Add**. (Do not click the Next button.)
11. Select the check box next to the newly added server, and click **Make Leader**.
12. Click **Next**.

    The SIP Line Configuration Detail page appears.

Figure 11
New IP Telephony Node–SIP Line Configuration Details



13 On the **SIP Line Configuration Details** page, verify that the **SIP Line Gateway Application** check box is selected (default). This check box enables the gateway service on this node.

14 Under the **General** section, in the **SIP Domain name** field, enter the name of the SIP domain.

> ***Note:*** If the domain name is configured in LD 15, ensure the same domain name is entered for the SIP Domain name. The SIP IP Phones use the domain name configured in LD 15 (instead of this field on the IP Node page), while registering with the SLG application. The domain name used in the IP Node section is in consideration of the future migration of supporting multiple domains and customers for each Signaling Server. The SLG requires IP Phone registration to include the domain name because the SIP standard verifies and challenges the login.

15 Leave the **SLG endpoint name** field blank. (This field is not used in CS 1000 Release 6.0. The endpoint name is the same endpoint name as the SIP Line Gateway and will be used for SIP gateway registration.)

16 In the **SLG Group ID** field, enter the node ID. The SLG Group ID field is optional and is used in GR/BO configuration. It identifies whether a particular SIP Line user at the Branch Office belongs to a group when it registers at the Main Office.

17 In the **SLG Local Sip Port** field, verify the local SIP port number of the SIP Line Gateway. (If the port number is different from the provided default value [5070], enter the new port number). The range is 1-65535. This field is mandatory for the SLG configuration. The SIP Line Gateways listens on the local SIP port. The SIP IP Phones use this port for registration purposes.

18 In the **SLG Local Tls Port** field, verify the local TLS port number of the SIP Line Gateway (if the port number is different from the provided default value [5071], enter the new port number). The range is 1-65535. This field is mandatory for the SLG configuration. The SIP Line Gateways listens on the local TLS port. The SIP IP Phones use this port for registration purposes.

19 Under the **Virtual Trunk Network Health Monitor** section, select the **Monitor IP Addresses** check box. (Optional)

20 In the **Monitor IP** field, enter the IP address of the server to monitor, and click **Add**. (Optional)

The IP address is added to the Monitored addresses list. The system will monitor activities on the specified server IP address. The monitored IP address serves the same purpose as for other virtual trunk-based applications. It is default to the TLAN gateway of a given Signaling Server, for checking the sanity of a TLAN network. If the monitored IP address does not respond, it is assumed that network connectivity is down. As a result, the application renders the VTRK service by disabling its own service.

Addresses are removed by first selecting the IP address and then clicking Remove.

21 Under the **SIP Line Gateway Settings** section, from the **Security Policy** list, select the security policy for the SIP Line Gateway. The security policy settings are used for Transport Layer Security (TLS) support. TLS is used to secure signaling between SIP endpoints. The policy selected depends on the IP Phone capability to support TLS.

- Security Disabled: Turns SIP TLS off.
- Best Effort: Turns SIP TLS on. The SIP Line Gateway will listen on its TLS, TCP, and UDP ports.
- Secure Local: Turns SIP TLS on. However, the SIP Line Gateway will listen only on its TLS port. (Uses TLS only if both ends support it.)
- Secure End to End: Nortel does not recommend enabling end-to-end security on the SIP Line Gateway, because all IP Phones may not have the TLS capability. If you enable end-to-end security on the SLG, some IP Phones cannot

be registered (when the IP Phones are using UDP or TCP transport).

For more information about security, see *Security Management Fundamentals* (NN43001-604).

22 If security is enabled, configure the following:

- From the **Number of Bytes Re-negotiation** list, select the number of bytes to be used for renegotiation. With this option, the session key used for the SIP TLS connection is renegotiated periodically. Renegotiation is triggered after the number of bytes specified have passed over the connection.
- To enable IP Phone authentication, select the **Client Authentication** check box. Enable this option if you want both sides to authenticate; when it is disabled, authentication is one-way. If you enable this option, sessions require greater overhead.
- To enable x509 certificate authentication, select the **x509 Certificate Authentication Enabled** check box. Enable this option to cause SIP TLS to provide both encryption and identity verification. Disable this option to allow the system, when operating on the IP Phone side of the SIP/TLS connection, to accept self-signed certificates from the server side. If you disable x509 Certificate Authentication, the system provides encryption only (it does not verify identity). If you select X509 Certificate Authentication, you cannot use self-signed certificates with SIP TLS.

23 Under the **SIP Line Gateway Service (Branch Office / GR Office Settings)** section, from the **SLG Role** list, select the role of the node:

- MO = Main Office: When the SLG Role is set to MO, you do not need to enter any MO or GR settings. These settings are not required or mandatory.
- GR = Geographically Redundant: When the SLG Role is set to GR, you must enter all the MO SLG settings (IP address, port and protocol).
- BO = Branch Office: When the SLG Role is set to BO, you must enter both the MO and GR settings (IP address, port and protocol).

24 From the **SLG Mode** list, select **S1/S2** (SIP Proxy Server 1 and Server 2).

25 If the role is GR or BO, in the **MO SLG IP** field, enter the MO SLG (Node) IP address of the Main Office.

26 If the role is GR or BO, in the **MO SLG Port** field, either leave the default value for the port or change the port number.

27 If the role is GR or BO, from the **MO SLG Transport** list, select the transport type.

28 If the role is BO, in the **GR SLG IP** field, enter the GR SLG (Node) IP address.

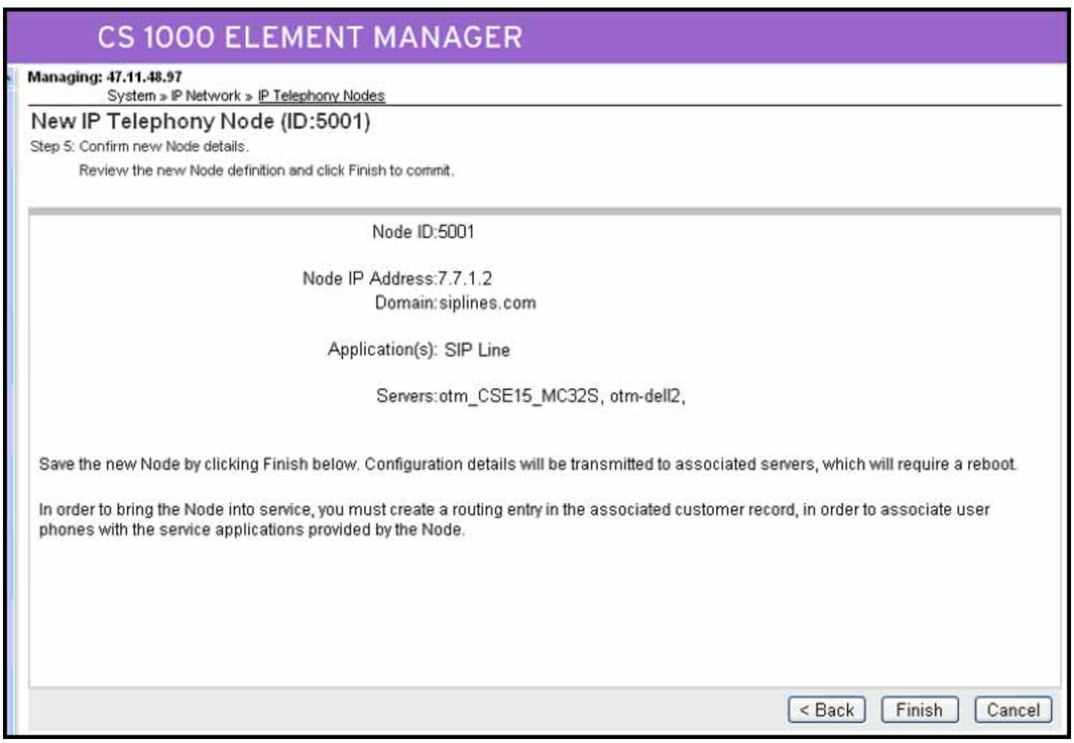
29 If the role is BO, in the **GR SLG Port** field, use the default value for the port or change the port number.

30 If the role is BO, from the **GR SLG Transport** list, select the transport type.

31 Click **Next**.

The Confirm new Node details page appears.

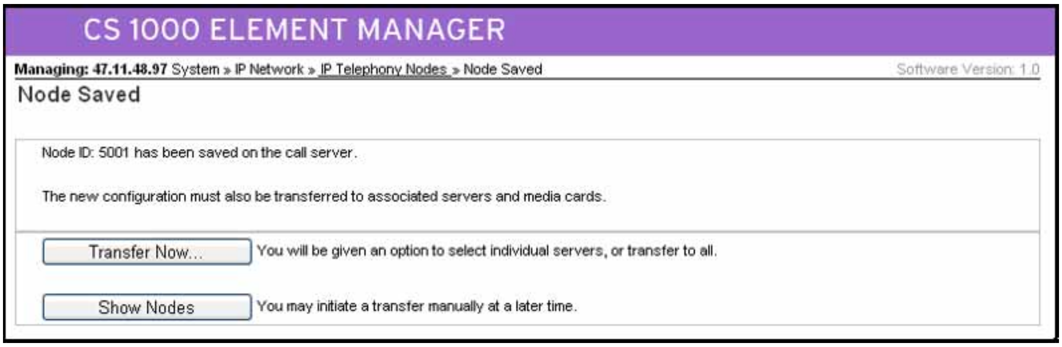
Figure 12
Confirm new Node details



32 Verify the configuration details, and click **Finish** to save the configuration files on the Call Server. (Wait while the configuration details are saving [at least 3 minutes]. Do not click Finish again.)

The Node Saved page appears.

Figure 13
Node Saved



33 On the **Node Saved** page, click **Show Nodes** to view the configuration for the node.

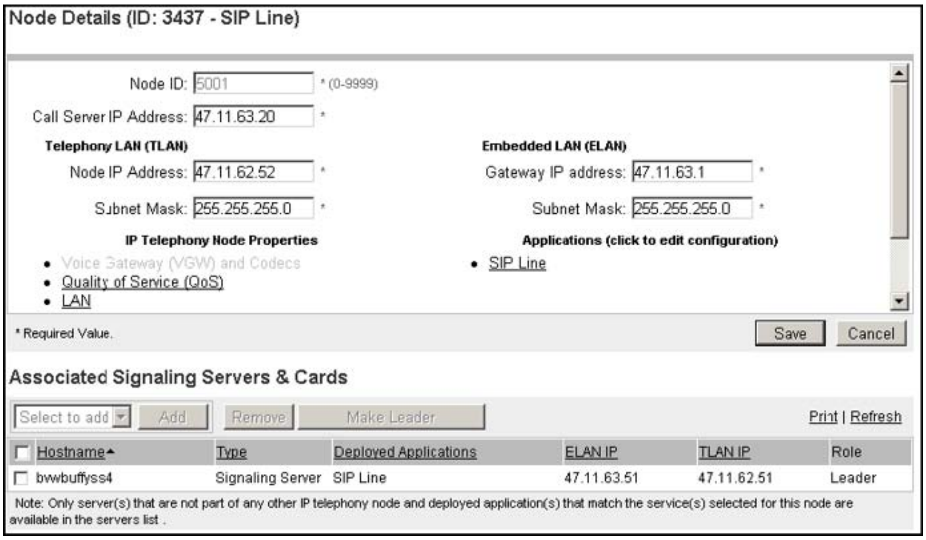
The IP Telephony Node summary page appears.

> ***Note:*** Alternatively, you can click the **Transfer Now** button on the Node Saved page. If you click the Transfer Now button, the Synchronize Configuration Files (Node ID <x>) page appears. You can select some or all of the node elements and then click Start Sync to transfer the configuration files to the selected servers.

Figure 14
IP Telephony Node summary page

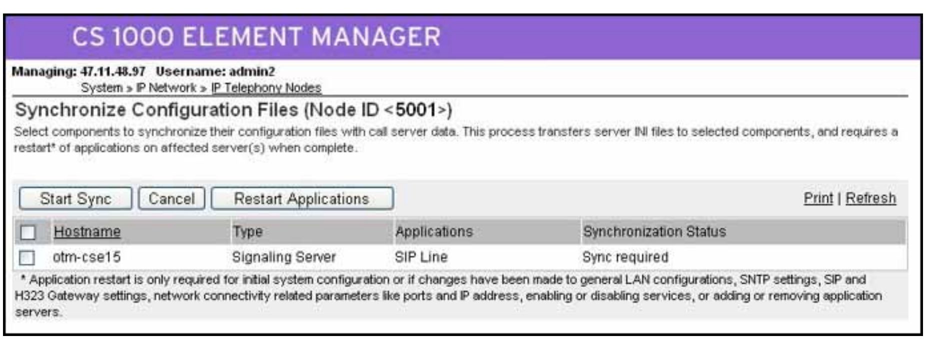
If you want to view the configuration for the node, select the node ID link under the Node ID column. The Node Details page appears.

Figure 15
Review node configuration



On the IP Telephony Node summary page, the Status column displays the status of the entire node. If the configuration status changes and this change is not transmitted, then the status is indicated as Changed. If you click the Changed link, the Synchronize Configuration Files (Node ID <x>) page appears where you can initiate the transfer to all or selected Node elements.

Figure 16
Synchronize Configuration Files page



34 Click **Changed**.

35 On the **Synchronize Configuration Files (Node ID <x>)** page, select the elements requiring synchronization, and then click **Start Sync**.

The configuration files are transferred to the selected server.

After the synchronization finishes, the status column displays Synchronized for the node element.

36 Verify that the **Synchronization Status** is **Synchronized**.

37 Select the check box for the node, and then click the **Restart Applications** to start the SIP Line Service.

WARNING
You must click Restart Application for the SIP Line Service to function correctly.

--End--

Configure a D-channel over IP

The SIP Line Gateway (SLG) application requires a D-channel over IP to communicate with the CS 1000 system. The SIP Line routes are associated with the D-channels and the SLG application running on a Linux server. The SIP Line route is used to communicate with the Call Server.

Procedure 4
Configuring D-channel over IP

Step	Action

1 Log on to Element Manager. See Procedure 1 “Logging on to UCM and Element Manager” (page 79).

2 In the navigation pane, select **Routes and Trunks > D-Channels**.

> ***Note:*** If this is the first time that this Web page is accessed, a message indicates that no D-channels are configured. Click OK.

The D-Channels page appears.

3 Under the **Configuration** section, from the **Choose a D-channel Number** list, select a D-Channel number.

4 From the **type** list, select the type of D-Channel.

5 Click **to-Add**.

The D-Channels xx Property Configuration page appears. The D-channel number is denoted by xx. Required fields are indicated with a green asterisk.

6 From the **D channel Card Type (CYTP)** list, select **D-Channel is over IP (DCIP)**.

7 From the **Interface type for D-channel (IFC)** list, select **Meridian Meridian1 (SL1)**.

8 If you are defining the Network Name Display, from the **Release ID of the switch at the far end (RLS)** list, select the release ID of the switch.

9 Click the **Basic options (BSCOPT)** link.

The Basic options (BSCOPT) list expands.

10 Configure **Remote Capabilities (RCAP)** by clicking **Edit**.

The Remote Capabilities Configuration page appears.

11 Select the **Message waiting interworking with DMS-100 (MWI)** check box.

12 Select the **Network name display method 2 (ND2)** check box.

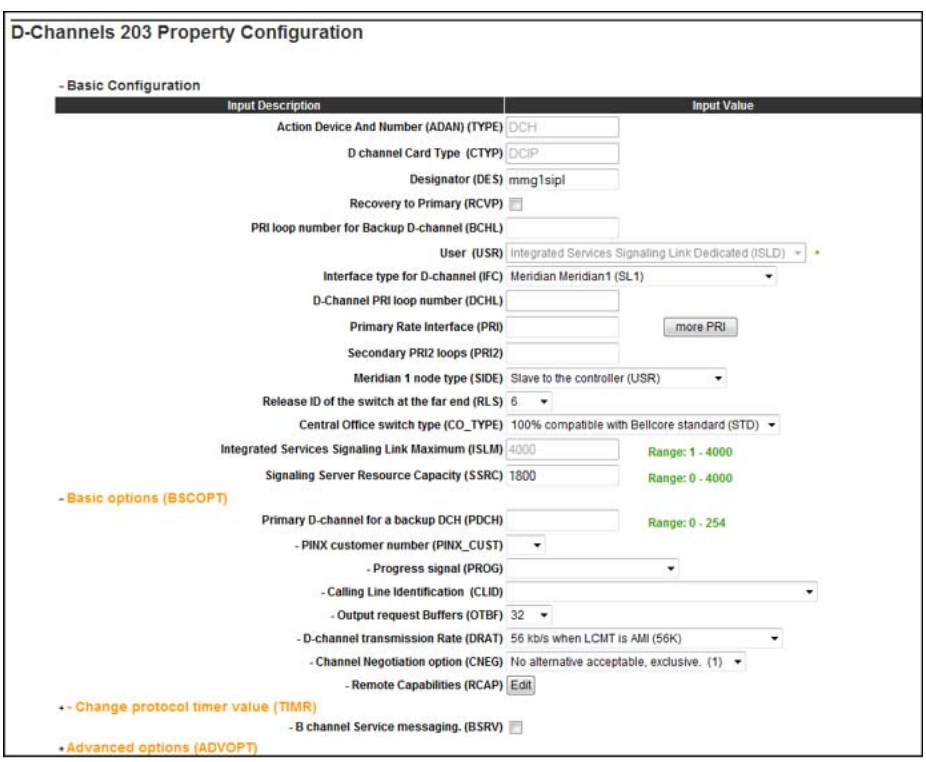
13 At the bottom of the **Remote Capabilities Configuration** page, click **Return - Remote Capabilities**.

The D-Channel xx Property Configuration page reappears.

14 Click **Submit** to save the changes.

The D-Channels page reappears with the changes.

Figure 17
D-Channels xxx Property Configuration page



--End--

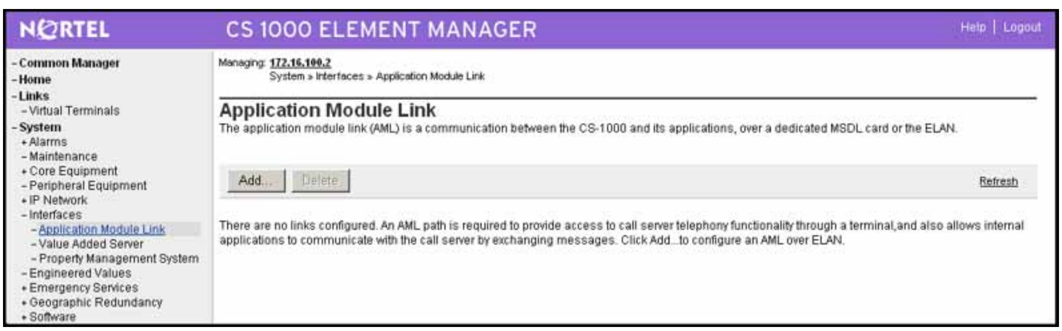
Configure AML over ELAN

The SLG application uses the AML over ELAN link to establish a pbxlink (AML over ELAN) connection with the CS 1000 system. The SLG application can control the SIPL UEXT using AML messages with the pbxlink established.

Procedure 5
Configuring AML over ELAN

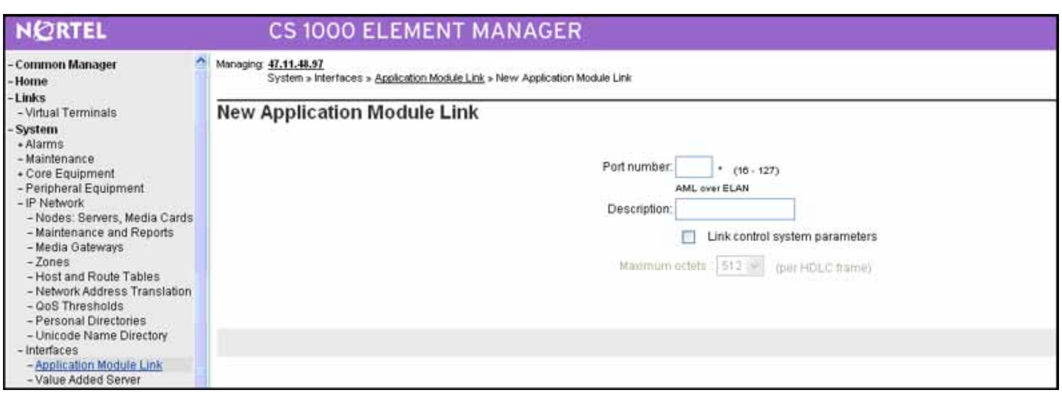
Step	Action
1	In the navigation pane, select **System > Interfaces > Application Module Link**. The Application Module Link page appears.

Figure 18
Application Module Link



Step	Action
2	On the **Application Module Link** page, click **Add**. The New Application Module Link page appears.

Figure 19
New Application Module Link



Step	Action
3	On the **New Application Module Link** page, in the **Port number** field, enter the port number. The SIP Line service uses ports 32 to 127.

Step	Action
4	In the **Description** field, enter a description for the AML.
5	Select the **Link control system parameters** check box to enable the Maximum octets list.
6	From the **Maximum octets** list, select the maximum number of octets for each High-level Data Link Control (HDLC) frame. (The default is 512.)
7	Click **Save**.

--End--

Configure VAS ID association with AML over ELAN link

Every AML over ELAN link configured on the CS 1000 system requires a Value Added Server (VAS) ID for the AML messages to be sent. Use the following procedure to associate a Value Added Server (VAS) with AML over ELAN.

Procedure 6
Configuring VAS ID association with AML over ELAN link

Step	Action
1	In the navigation pane, select **System > Interfaces > Value Added Server**.
2	On the **Value Added Server** page, click **Add**.
3	On the **Add Value Added Server** page, click **Ethernet LAN Link**.
4	On the **Ethernet Link** page, in the **Value Added Server ID** field, enter the ID of the VAS. The range is 16–127. The VAS ID entered must be greater than or equal to 32.
5	From the **Ethernet LAN Link** list, you must select a link number greater than or equal to 32 (the ELAN port configured in ADAN must be greater than or equal to 32). ***Note:*** To configure using Call Server Overlays see Table 8 "LD 17 Configure ELAN AML links" (page 110).
6	Ensure the **Application Security** check box is cleared.
7	To enter a time interval for checking the link for overload (in 5 second increments), ensure that **1** is selected in the **Interval** list.
8	Ensure that the **Message Count Threshold** field is **9999** (the default value). (The range is 10–9999.)

9 Click **Save**.

--End--

Configure a virtual trunk zone

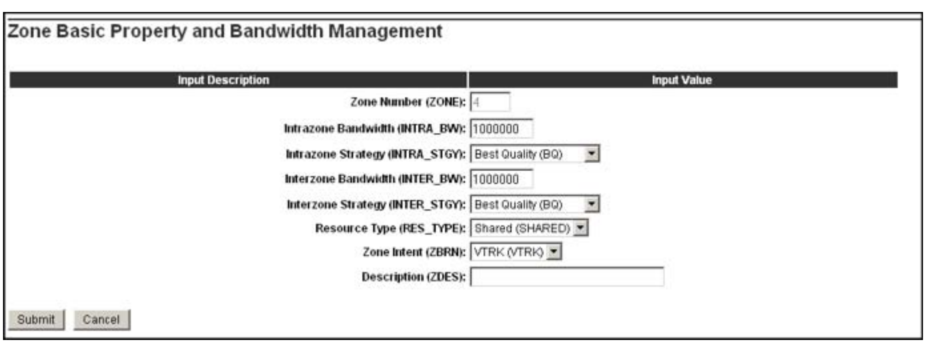
You must configure a virtual trunk zone for the SIP Line route to work properly.

For more information about zones, see "Bandwidth management" (page 25)and also see *Converging the Data Network with VoIP Fundamentals* (NN43001-260).

Procedure 7
Configuring a virutal trunk zone

Step	Action
1	In the navigation pane, select **System > IP Network > Zones**.
2	On the **Zones** page, select **Bandwidth Zones**.
3	On the **Bandwidth Zones** page, select a Bandwidth Zone number from the list, and click **to Add**.
4	On the **Zone Basic Property and Bandwidth Management** page, set the zone properties based on bandwidth availability.

Figure 20
Zone Basic Property and Bandwidth Management



5	From the **Zone Intent (ZBRN)** list, select **VTRK (VTRK)**.
6	In the **Description (ZDES)** field, enter a brief description of the zone (spaces are not allowed).
7	Click **Submit**.
	The new zone is added to the Bandwidth Zones page.

--End--

Configure SIP Line routes

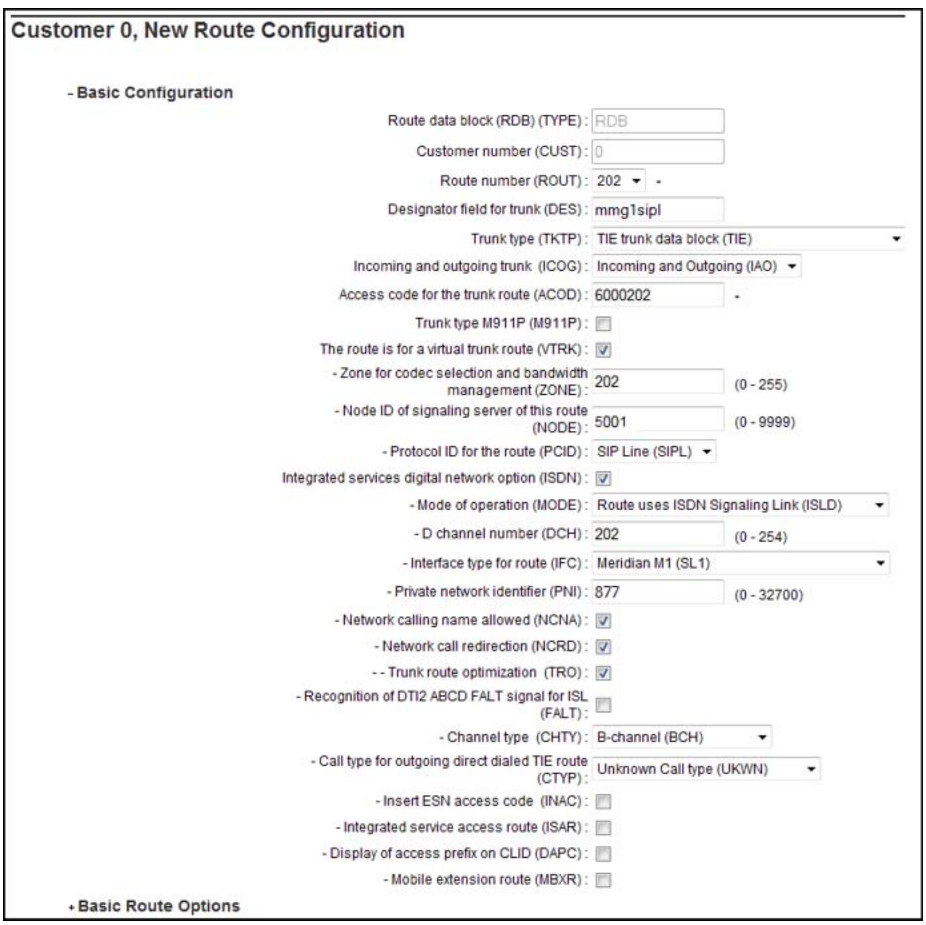
You configure a SIP Line route similar to the way you configure a virtual trunk route, such as H.323, SIP, or MGCP.

A virtual trunk zone is required for the SIP Line route to work. Ensure you have configured a virtual trunk zone (see Procedure 7 “Configuring a virutal trunk zone” (page 95)).

Procedure 8
Configuring SIP Line routes

Step	Action
1	In the navigation pane, select **Routes and Trunk > Routes and Trunks**.
2	On the **Routes and Trunks** page, click the **Add route** button for the customer number.

Figure 21
Customer x, New Route Configuration



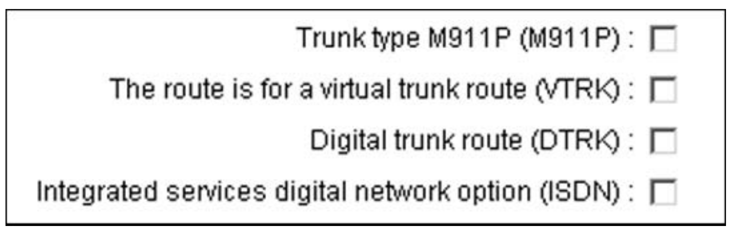
3 On the **Customer xx, New Route Configuration** page, from the **Route number (ROUT)** list, select a route number.

4 From the **Trunk type (TKTP)** list, select **TIE trunk data block (TIE)**.

When Trunk Type (TKTP) is selected, the following options appear:

- Trunk type M911P (M911P)
- The route is for a virtual trunk route (VTRK)
- Digital trunk route (DTRK)
- Integrated services digital network option (ISDN)

Figure 22
TIE trunk data block options

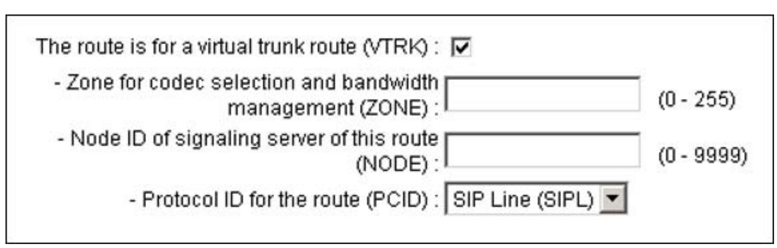


5 From the **Incoming and outgoing trunk (ICOG**) field, select **Incoming and Outgoing (IAO)**.

6 In the **Access code for the trunk route (ACOD)** field, enter the access code.

7 Select **The route is for virtual trunk route (VTRK)** check box.

Figure 23
VTRK option



8 In the **Zone for codec selection and bandwidth management (ZONE)** field, enter the zone number. (Use the same zone as configured in Procedure 7 "Configuring a virutal trunk zone" (page 95).)

9 In the **Node ID of signaling server of this route (NODE)** field, enter the node ID of the SIP Line Gateway.

10 From the **Protocol ID for the route (PCID)** list, select **SIP Line (SIPL)**.

11 Select the **Integrated services digital network option (ISDN)** check box.

12 From the **Mode of operation (MODE)** list, select **Route uses ISDN Signaling Link (ISLD)**.

13 In the **D channel number (DCH)** field, enter the D-channel number.

14 From the **Interface type for route (IFC)** list, select **Meridian M1 (SL1)**.

15 Ensure the **Network calling name allowed (NCNA)** check box is selected.

16 Select the **Network call redirection (NCRD)** check box.

17 Select the **Trunk route optimization (TRO)** check box. (Optional)

18 Enter the appropriate information in the **Basic Route Options**, **Network Options**, **General Options**, and **Advanced Configurations** sections.

19 Click **Save**.

--End--

Configure SIP Line Virtual Trunks

SIP Line routes use the existing IP virtual trunks while establishing calls to and from the SIP IP Phones. Use Element Manager to configure IP trunks of type VTRK.

Procedure 9
Configuring SIP Line Virtual Trunks

Step	Action
1	In the navigation pane, select **Routes and Trunk > Routes and Trunks**.
2	On the **Routes and Trunks** page, select the customer for which you are configuring Virtual Trunks.
3	Click **Add trunk** associated with the route listing to add new trunk members. The Customer xx, Route yy, New Trunk Configuration Web page appears.
4	Choose **Multiple trunk input number (MTINPUT)** if you are using more than one trunk.

5 From the **Trunk data block (TYPE)** list, select **IP Trunk (IPTI)**.

6 In the **Terminal Number (TN)** field, enter a TN.

7 Enter a **Route number, Member number (RTMB)**.

8 Enter a **Trunk Group Access Restriction (TGAR)** value.

9 In the **Channel ID for this trunk (CHID)** field, enter a channel ID (where the range is 1 to 382).

10 To specify a **Class of Service (CLS)** for the trunk, click **Edit**.

The Class of Service Configuration Web page appears.

11 Select a **Class of Service**.

12 Click **Return Class of Service** to return to the New Trunk Configuration Web page.

13 Select **Basic Configuration**.

The Basic Configuration list expands.

14 From the **Start arrangement Incoming (STRI)** list, select a value for the start arrangement for incoming calls.

15 From the **Start arrangement Outgoing (STRO)** list, select a value for the start arrangement for outgoing calls.

16 Select **Advanced Trunk Configurations**.

The Advanced Trunk Configurations list expands.

17 Configure **Network Class of Service group (NCOS)**.

18 Click **Save**.

The Customer Explorer Web page reappears, showing the new trunk members.

--End--

Verify your configuration

Use the following procedure verify your configuration to ensure your SIP Line Server is configured and running correctly before configuring users.

Procedure 10
Verifying your configuration

Step	Action
1	In LD 48, enter the **`stat elan`** command.
2	Ensure you receive output similar to the following:

```
SERVER TASK: ENABLED
ELAN #:  035 DES: SIPL
```

```
APPL_IP_ID: 47 .11 .247 .46 :  0000F800 LYR7:
ACTIVE EMPTY APPL ACTIVE
```

If you do not receive similar output, review the following:

- Procedure 5 “Configuring AML over ELAN” (page 93)
- Procedure 6 “Configuring VAS ID association with AML over ELAN link” (page 94)
- Ensure that you can ping from the Call Server to the SIPL ELAN.
- Ensure that you can ping from the SIPL to the Call Server ELAN.

3 In LD 96, enter the **stat dch** command.

4 Ensure you receive output similar to the following:

```
DCH 020 :  OPER EST ACTV AUTO DES : SIPL
```

If you do not receive similar output, review the following:

- Procedure 3 “Configuring the SIP Line Gateway service” (page 82)
- Procedure 4 “Configuring D-channel over IP” (page 91)

--End--

Configure SIP Line users

The SIP Line service requires the new SIPL Universal Extension (in LD 11). The CS 1000 Universal Extension provides a CS 1000 IP Line appearance to SIP IP Phones and, as a result, extends CS 1000 Line services to the SIP IP Phones. The SIP IP Phones configured as SIPL UEXT contain all CS 1000 attributes such as Directory Number (DN), Class of Service (CLS), Calling Line ID, Network Class of Service (NCOS), and standard Key configurations.

You can configure SIP Line users in two ways on the CS 1000 system:

- You can configure SIP Line users in the Phones section (in Element Manager). This method is the most common way to add phones.
- Alternatively, you can create default phones by using Subscriber Manager.

The following mandatory configuration items are required for UEXT SIPL TNs:

- Key 0 DN
- Key 1 HOT U UADN (For more information about User Agent Directory Number (UADN), see Step 17.)
- SIP User Name
- Station Control Password (SCPW) (Ensure that LD 15 is configured for SCPW.)

For more information about configuration of the SIP IP Phones, see "SIP IP Phone configuration" (page 31).

Phones section in Element Manager

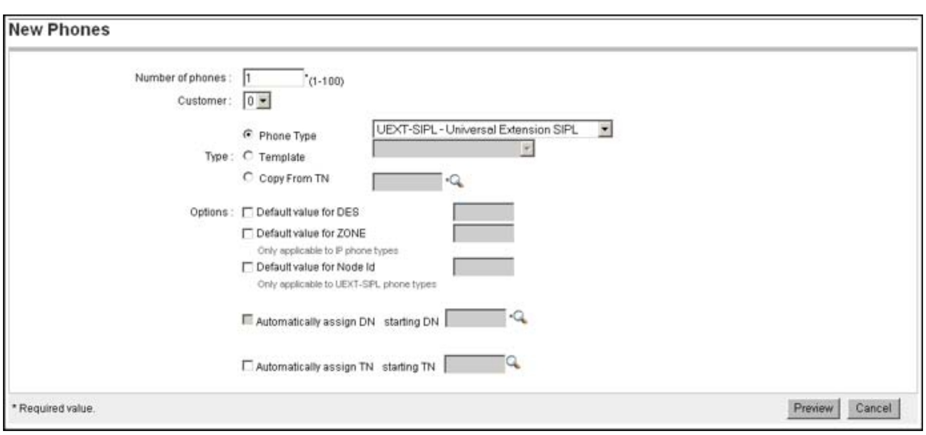
Configure SIP Line users in Element Manager (Phones).

You can also configure a template for the SIP Line IP Phones. In Element Manager, go to Phones > Templates. Make sure the that Telephone Type is set to UEXT-SIPL-Universal Extension SIPL. Key 0 must be the DN key and any key > 0 can be the HOT U key.

Procedure 11
Configuring SIP Line users in Element Manager

Step	Action
1	In the navigation pane, select **Phones**.
2	On the **Search for Phones** page, under the **Phones** section, click **Add**.
3	On the **New Phones** page, in the **Number of phones** field, enter the number of phones you want to configure.

Figure 24
New Phones



Step	Action
4	From the **Customer** list, select the customer number.

5 In **Type** area, from the **Phone Type** list, select **UEXT-SIPL - Universal Extension SIPL** from the list.

If you do not see the UEXT-SIPL - Universal Extension SIPL option in the Phone Type list, check the following:

- Ensure Package 417 (SIP Line Service) is available. (For more information, see “SIP Line Service packaging” (page 69).)
- Ensure the SIP Line Service is enabled. (For more information, see “Enable the SIP Line Service and configuring the root domain ” (page 80).)
- Ensure the Phone properties are updated in Element Manager. (In Element Manager, got to **Phones > Properties**. On the **Properties** page, click **Update**.)

6 Select the **Default value for DES** check box and type the value in the text box.

7 Select the **Default value for ZONE** check box and type the value in the text box.

8 Select the **Default value for Node Id** check box and type the SIP Line Gateway Node ID value in the text box.

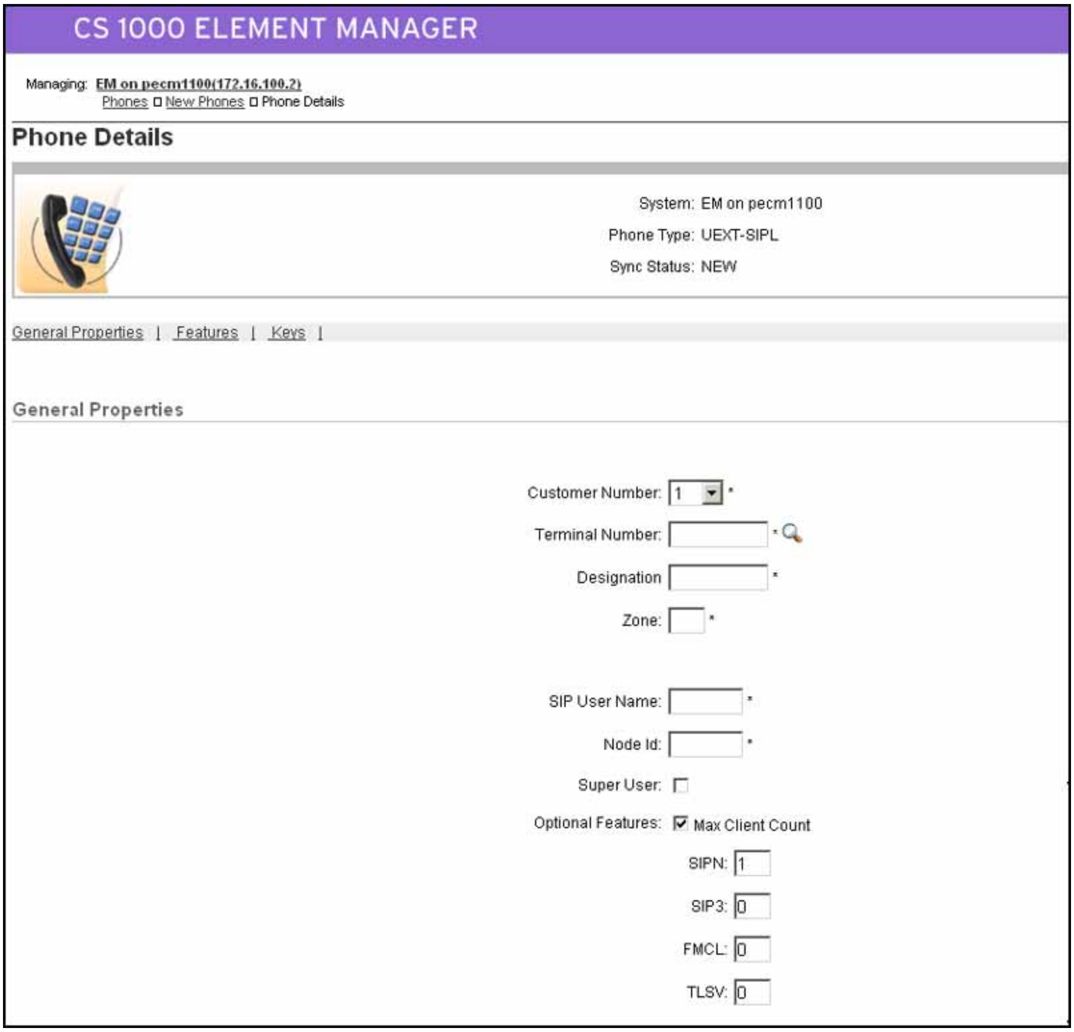
This check box is used only for UEXT-SIPL phone types.

9 Select the **Automatically assign TN** check box to automatically assign the next TN from the **starting TN** value.

10 Click **Preview**.

The Phone Details page appears and this page has three sections: General properties, Features, and Keys.

Figure 25
Phone Details



11 On the **General Properties** page, from the **Customer Number** list, select the customer number.

12 In the **SIP User Name** field, enter the user name of the SIP IP Phone. The user name is used by the SIP IP Phone when it connects to the SIP Line Server.

13 Ensure the **Super User** check box is not selected.

14 From the **Optional Features** section, select the **Max Client Count** check box. The SIPN, SIP3, FMCL, and TLSV fields appear.

- SIPN = SIP Line for Nortel IP Phones (The SIPN value is 1.)
- SIP3 = SIP Line for third-party IP Phones (The SIP3 value is 0.)

- FMCL = Fixed Mobility Converged Line (The FMCL value is 0.)
- TLSV = Telephony Services (The TLSV value is 0.)

15 In the **Features** section, define the SCPW (Station Control Password) feature as dictated from LD 15 Flexible Feature Code (FCC_DATA) configuration. This password is used by the SIP IP Phone when it connects to the SIP Line Server.

16 In the **Features** section, select any other desired features for the SIP IP Phone.

17 In the **Keys** section, you must configure the following keys.

- Configure key 0 as the DN key (for example, SCR)
- Configure any key > 0 as the HOT U key

ATTENTION

A HOT U key label is available when UXTY is SIPL. The HOT U key is also known as the User Agent Directory Number (UADN) key. The UADN key is used to make and receive calls between the SIP Line Gateway and the Universal Extensions. However, this key is used only by the SIP Line Gateway (SLG) application. (The UADN is not dialed by end users. It is only used internally between the Call Server and the SIP Line Gateway application.)

The configuration is `Key <num> HOT U <DN>` where the <num> parameter can be any key except 0.

The User Agent Prefix (UAPR) prompt can be provisioned in the Customer Data Block (CDB - LD 15). See Table 10 "LD 15 Configure SLS_DATA" (page 111) and Procedure 2 “Enabling the SIP Line Service and configuring the root domain” (page 80).

If the User Agent Prefix (UAPR) prompt is provisioned in the CDB, while you are configuring the new SIPL TN in Element Manager (after the PDN [Key 0 Primary DN] is configured), then the system generates a UADN (combining the Prefix and PDN). The HOT U DN is autogenerated (that is, it is created and stored in the database). However, it is not automatically displayed during configuration. The combination of UAPR+HOT U DN is only displayed when you print the TN. Element Manager does not automatically pre-populate your HOT U key with the UAPR.

While configuring HOT U KEY, you can do any of the following:

—Manually configure the same DN as the UADN (if UAPR was configured).

—Configure a different DN as the UADN.

—Press Enter. The system automatically fills the UADN with a generated entry. The system generates an error if the UAPR is not found or if the UAPR is available but a valid UADN cannot be made.

(If UAPR is not provisioned in the customer data block (CDB) , then you cannot press Enter for a HOT U key without configuring UADN.)

If the total length of UAPR and PDN are longer than 7 digits, the UADN is not automatically created. You must manually configure the UADN in this case. You cannot configure the PDN and UADN as the same number. The UADN cannot be used as a redirection DN (for example, FDN, HUNT, or CFW to DN).

The <DN> must fit into the customer dialing plan no matter if the <DN> is manually entered or if it is automatically entered by the software (if UAPR is configured in LD 15). After the DN is created by the software, the <DN> = <UAPR> + <Primary DN of universal extension>. UADN must be unique. That is, it cannot be the same number as another PDN or UADN for the same customer.

18 Click **Validate** to validate the new telephone.

The status of the Validation process appears listing any validation errors that occur. If validation errors occur, repeat the relevant sections of this procedure to correct the errors.

19 Click **Finish** to add the new telephone to the database.

--End--

Subscriber Manager

Configure SIP Line users in Subscriber Manager.

When adding a SIP Line IP Phone for a subscriber in Subscriber Manager, the SIP user name of SIP Line IP Phone is updated from the user name, last name, first name, or preferred name of subscriber using the following four rules:

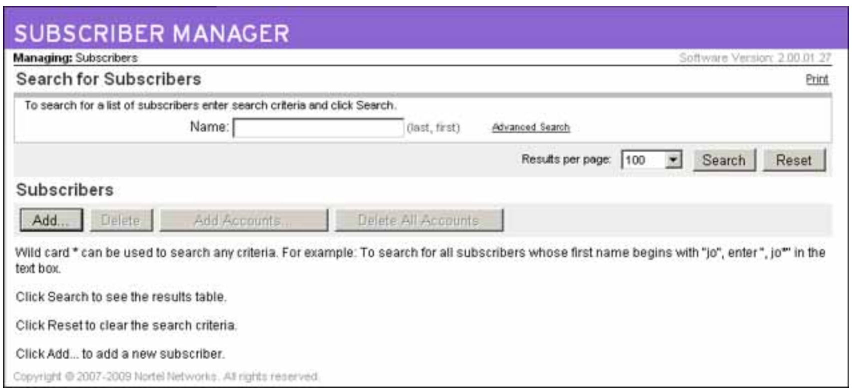
1. The SIP user name will be the Subscriber user name (if it is available).
2. If the subscriber does not have user name and if the subscriber has preferred name, then the preferred name will be set as the SIP user name.
3. If the subscriber does not have user name or preferred name and if the subscriber has first name and last name, then the subscriber first name will be set as SIP user name.
4. If the subscriber does not have a user name, a preferred name, or a first name, then the subscriber’s last name will be set as the SIP user name.

For detailed information about Subscriber Manager, see *Subscriber Manager Fundamentals* (NN43001-120).

Procedure 12
Configuring SIP Line users in Subscriber Manager

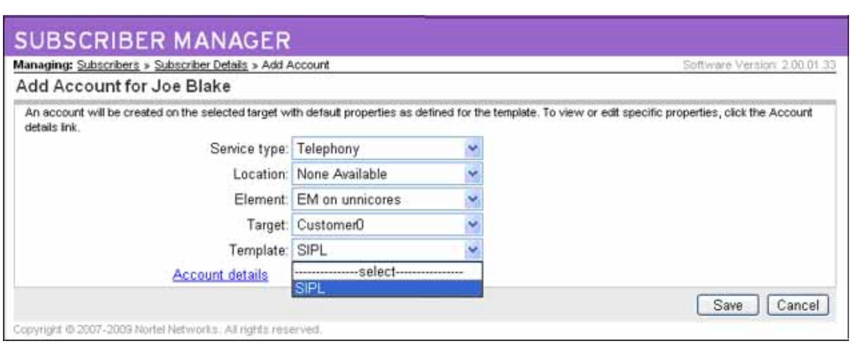
Step	Action
1	Log into UCM and select **Subscriber Manager** in the left pane. The Subscriber Manager main page appears.

Figure 26
Subscriber Manager main page



Step	Action
2	Click **Add** to add a new subscriber.
3	On the **New Subscriber** page, complete the details for the new subscriber.
4	Click **Apply**.
5	Under the **Accounts** section, click **Add** to add an account for this subscriber.
6	On the **Add Account for [Subscriber Name]** page, from the **Template** list, select **SIPL**.

Figure 27
Add Account



Step	Action
7	Click **Save**. The Phone Details page appears.

8 Configure the phone (General Properties, Features, and Keys).

--End--

Configuration using Call Server configuration overlays

Use the implementation tables in this chapter to configure the SIP Line feature using the command line interface (CLI).

Task summary

The following is a summary of the tasks in this chapter:

1. Enable SIP Line on a CS 1000 at the customer level.
2. Configure the root domain.
3. Define a zone.
4. Configure SIP Line routes.
5. Configure D-channel over IP.
6. Configure AML over ELAN links.
7. Configure the SIPL Universal Extension.
8. Configure SIP Line clusters.

LD tables

Table 7
LD 17– Configure D-channel over IP

Prompt	Response	Description
REQ:	CHG	Change existing data
TYPE:	ADAN	Action Device And Number
- ADAN	NEW/CHG DCH xx	Action Device And Number, where xx is 0–63.
CAB_TYPE	 IP FIBR	Cabinet Type IP Expansion Cabinet or Media Gateway Fiber Expansion Cabinet

Table 7
LD 17– Configure D-channel over IP (cont'd.)

Prompt	Response	Description
- CTYP	DCIP	Card Type D-channel over IP
BANR	YES	Enable security banner printing option
- IFC	SL1	Interface type for D-channel

Table 8
LD 17 Configure ELAN AML links

Prompt	Response	Description
REQ:	CHG	Change existing data
TYPE:	ADAN	Action Device And Number
- ADAN	NEW ELAN elan#	Action Device And Number, where elan# is the link number and must be greater than or equal to 32.
CAB_TYPE	 IP FIBR	Cabinet Type IP Expansion Cabinet or Media Gateway Fiber Expansion Cabinet
- CTYP	ELAN	Card Type AML over Ethernet card

Table 9
LD 17 Configure VAS ID for AML link

Prompt	Response	Description
REQ:	CHG	Change existing data
TYPE:	VAS	Value Added Server
VAS	NEW	New Value Added Server data block
- VSID	0-15	VAS identifier

Table 9
LD 17 Configure VAS ID for AML link (cont'd.)

Prompt	Response	Description
- ELAN	x=ELAN#	Associate Value Added Server ID (VSID) x with Application Module Link over Ethernet (ELAN subnet) x The ELAN number must match the number configured in the previous step.
- SECU	NO	Security for Meridian Link applications The security check must be disabled for SIP Line VAS and ELAN.

Table 10
LD 15 Configure SLS_DATA

Prompt	Response	Description
REQ:	NEW/CHG	New data block or change existing data
TYPE:	SLS_DATA	If the customer data block (CDB0 is created, you can modify the SLS_DATA directly.
CUST	xx	Customer number
SIPL_ON	YES (NO)	Enables or disable the SIP Line server. The default is NO (disabled).
SIPD	Domain name	The SIP domain name. The domain name can be 16 characters in length. Valid characters are 0–9, A–Z, a–z, and the period (.).
UAPR	DN prefix	User Agent Prefix. DN prefix used to automatically generate the UADN for all SIP Line IP Phones for this customer. This is an optional prompt.

Table 11
LD 117 Define zone data

Command	Description
NEW ZONE <zoneNumber > <intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth> <interZoneStrategy> [<zoneIntent> <zoneResourceType>]	Define a new Zone with parameters. All parameters must be entered: - zoneNumber from 0 to 255. - intraZoneBandwidth from 0 to 0.1Mbps. - intraZoneStrategy is the intrazone preferred strategy where BQ is Best Quality or BB is Best Bandwidth. - interZoneBandwidth from 0-0.1Mbps. - interZoneStrategy is the interzone preferred strategy where BQ is Best Quality and BB is Best Bandwidth. - zoneIntent is the type of zone. The Zone must be set to VTRK, which is a Virtual Trunk zone. - zoneResourceType is resource Intrazone preferred strategy, where shared is shared DSP channels and private is private DSP channels.

Table 12
LD 16 Configure SIPL route

Prompt	**Response**	**Description**
REQ:	CHG/NEW	Change an existing route data block (RDB) or create a new RDB
TYPE:	RDB	Route Data Block
CUST	xx	Customer number associated with this route
ROUT	x..x	Route number, where x...x = 0–511: Large System and CS 1000E System 0–127: Small System, CS 1000S, MG 1000B, and MG 1000T
TKTP	TIE	Trunk type = TIE
VTRK	YES	Virtual Trunk route
ZONE	0-255	Zone for codec selection and bandwidth management

Table 12
LD 16 Configure SIPL route (cont'd.)

Prompt	Response	Description
NODE	xxxx	Node ID of the SIP Line Gateway (SLG)
PCID	SIPL	Protocol ID for the route. Ensure the route is designated for the SIP Line Service.
...		
ISDN	YES	Dedicated Integrated Services Digital Network (ISDN) route.
- MODE	ISLD	Mode of operation = ISLD
- DCH	0-159	D-channel number The number must match the IP D-channel configured in the previous step.
- IFC	SL1	Interface type for route
...		
ICOG	IAO	Incoming and Outgoing trunk
ACOD	x...x	Access Code for trunk route

Table 13
LD 14 Configure trunks for SIPL route

Prompt	Response	Description
REQ	CHG/NEW	Create a new trunk or change an existing trunk.
TYPE	IPTI	Type of data block = IP TIE trunk data block
TN	TN	Terminal number
XTRK	VTRK	Extended Trunk
...		
CUST	xx	Customer number associated with this trunk
RTMB	xxx xxx	Route number, Member number
CHID	xxxx	Channel ID for this trunk.
STRI	IMM	Start arrangement Incoming Immediate

Table 13
LD 14 Configure trunks for SIPL route (cont'd.)

Prompt	Response	Description
...		
STRO	IMM	Start arrangement Outgoing Immediate

Table 14
LD 11 Configure SIPL UEXT

Prompt	Response	Description
REQ:	CHG/NEW	Create a new TN or change an existing TN.
TYPE:	UEXT	Universal extension. Indicates that the TN is used by a universal extension client. Mobile Extension package (412) must be equipped.
TN	l s c u c u	Terminal Number (TN) The TN defines the location of the telephone.
...		
CUST	xx	Customer number associated with this set
UXTY	SIPL	Universal Extension type.
MCCL	YES SIPN 0 SIP3 1 FMCL 0 TLSV 0	The Maximum Client Count Limit, which is the number of IP Phones supported for each SIP type: SIPN type = SIP Line for Nortel IP Phones SIP3 type = SIP Line for 3rd-party IP Phones FMCL type = Fixed Mobility Converged Line TLSV type = Telephony Services
SIPU	userID	The ID for the SIP Line user.
NODE	nodeID	The node number for the SIP Line Gateway (SLG).
SUPR	YES (NO)	Super user. The default is NO.
SCPW	xxxx	Station Control Password Used when logging in from the SIP Line IP Phone.

Table 14
LD 11 Configure SIPL UEXT (cont’d.)

Prompt	Response	Description
KEY	0 scr/mcr DN	Primary key DN.
KEY	1 HOT U UADN	The UADN key number. If UAPR was configured in LD 15, the DN is automatically generated as UAPR+PDN.

Maintenance

This chapter describes maintenance of the SIP Line feature.

Impact of power up and power down on SIP Line

After the system is powered up or powered down, all applications are re-initialized including SIP Line. All data stored in memory is lost.

IP Phone registration data

IP Phone registration is stored in memory on both the Call Server and Signaling Server. As long as the Call Server and Signaling Server are not rebooting at the same time, the registration data synchronizes and the user receives service without having to re-register.

However, if both the Call Server and Signaling Server reboot at the same time, the data in memory is lost. The IP Phone must then detect the server failure or wait for the next re-registration time. For keepalive messages support and re-registration interval settings for each of the various SIP IP Phone types, see Table 3 "SIP IP Phone capabilities" (page 30).

Impact on SIP Line call

The following table describes call activity after the system is powered up or down.

Table 15
Call impact

Call type	Description
Simple, active calls	A simple, active call is a call that is answered and involves only two parties. Simple, active calls are maintained for the duration of the call if the system is powered up or down. • If the call is an IP-to-IP call, the speech path is maintained for the duration of the call. • If the call is a SIP-to-TDM call, the speech path is maintained as long as the DSP is available.
Transient calls	Transient calls are unanswered calls. Transient calls are dropped when the server reboots.
Other calls	All other calls are dropped. The user does not receive a BYE message to clear the signaling path. The BYE message relies on both parties hanging up the call to clear signaling.

Impact of server restart procedure on SIP Line

If the Call Server and Signaling Server are restarted, the SIP Line feature is affected in the same manner as a system power up or power down. For information, see "Impact of power up and power down on SIP Line" (page 117).

Call Server maintenance overlays

Many of the maintenance overlays are updated to support the SIP Line feature. This section contains information about the following topics:

LD 32

LD 32 prints the SIP Line TN information. Only the registered TNs are displayed as part of the IDU command. The output information is printed only for the registered clients and not for all clients configured in LD 11 for that TN.

When the IDU command is executed on any SIPL UEXT TN, the output prints all clients (from 1 to 4) registered to the TN.

Example: TN 62 13 is configured as UEXT TN and 4 clients (1 SIPN, 1 FMCL and 1 SIP3) are registered to the TN.

```
IDU <62 13104 0 2 0>

UEXT TN: 104062 0 00 13002 1300 V
TN ID CODE: SIPL/SIPN
MODEL: <User-Agent string>
SIP CLIENT IP ADDR: 47.11.213.18:5000
TN ID CODE: SIPL/SIP3
MODEL: <User-Agent string>
SIP CLIENT IP ADDR: 47.11.213.19:5000
```

```
TN ID CODE: SIPL/FMCL
MODEL: <User-Agent string>
SIP CLIENT IP ADDR: 47.11.213.20:5000
SLG IP ADR: 47.11.217.235
SLP IP ADR: 47.11.239.50
```
<--when a SIP User registers this SLP info is carried using the REGISTER message

```
NT CODE: N/A
COLOR CODE: 0
RLS CODE: 0
SER NUM: N/A
```

LD 32 is also prints the route type as SIPL for the STAT VTRM command.

LD 80

LD 80 has been changed to modify the set type as UEXT/SIPL in the output.

The following example shows the TRAC command (and response) when the command is issued on an idle TN:

TRAC 0 5000 (Customer, DN)

```
IDLE VTN 061 0 00 20
```

The following example shows the TRAC command (and response) when the command is issued on a busy TN:

TRAC 104 0 2 0

```
VTN 104 0 02 00
KEY 0 MCR MARP ACTIVE VTN 104 0 02 00

ORIG VTN 104 0 02 00 KEY 0 MCR MARP CUST 4 DN 3420 TYPE SLUEXT
TERM VTN 104 0 01 00 KEY 0 SCR MARP CUST 4 DN 3410 TYPE 2004P1
MEDIA ENDPOINT IP: 47.11.215.69 PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF
DIAL DN 3410
MAIN_PM ESTD
TALKSLOT ORIG 22 TERM 22
EES_DATA: NONE
QUEU NONE
CALL ID 0 19968
```

When the TRAC command is issued on active calls, the phone type is printed as the following:

- UEXT for existing non-SIPL UEXT TNs
- SLUEXT for SIPL UEXT TNs

LD 81

LD 81 prints the List (LST) or Count (CNT) of the TNs based on the provided feature (FEAT) input. LD 81 accepts the SIPL input parameter for the FEAT prompt.

The output format of the overlay printing is not changed for SIP Line.

The behavior of the UEXT TNs (non-SIPL) is not changed.

For a SIPL TN, the TYPE of the phone is printed as SIPL.

For CNT output, a new SIPL header is created to print the number of configured SIP Line clients.

LD 83

LD 83 prints the List (LST) of TNs and the TN blocks (TNB).

LD 83 includes the SIP Line output for the LST and TNB commands. The overlay output format is not changed.

Since the LST command lists all the TNs configured in the system, and since there is no generic feature by which the output is sorted (like FEAT prompt in LD 81), the printed TYPE field is modified such that the following occurs:

- For an Universal Extension TN, the configured UXTY type is printed.
- For a SIP Line Universal Extension TN:
  - — The SCTL type configured for the TN (prefixed by SL) is printed.
  - — If multiple clients are configured for the same TN, then all the SCTL names configured are printed for the TYPE field. The SCTL names are separated by a forward slash (/).

LD 83 also includes the SIPL prompts in the TNB output.

LD 117

LD 117 includes SIPL TNs for the following:

- Inventory SETS
- Inventory LOCRPT
- STAT SERV
- STIP commands
- LOCRPT commands

LD 117 commands retrieve client information from the RLM table and since only registered clients have an entry in the RLM table, non-SIPL Universal Extensions do not exist in the RLM table. Only the registered clients are displayed in the output, and not all SCTL clients configured in LD 11. The number of rows output equals the number of clients configured for the TN in LD 11; however, only the data for register clients is printed in the output.

As a result, in the command outputs that follow, there is no differentiation between the TN type for SIPL and non-SIPL Universal Extensions.

Inventory SETS

The output for this command includes the SIPL TNs. The SIPL TNs are also included in the SETS Inventory report.

The SETS inventory output for a SIPL TN is as follows:

- The overall output format is not changed.
- The TYPE field is the SCTL type configured for the TN.
- If the SIP Line TN has multiple SCTL clients configured, then the output has multiple rows (one for each of the client).

Inventory LOCRPT

The Inventory LOCRPT command generates an inventory with the location details for each TN. (This command is added from the ESA perspective.) The command includes the SIPL TNs information.

The following example shows the output for a SIPL TN, 61 0, with 2 clients (SIP3 and SIPN) registered to the TN:

```
LD 117
INV GENERATE LOCRPT
```

This command generates the inventory in the background and displays a message after the inventory is complete.

```
INV PRT LOCRPT
Locrpt inventory:
61 0 0 0,5000,CUST0DES1 , SIP3, REG, N/A, 47.11.84.158:5000
/ <Unavailable>, ,,,"",,
61 0 0 0,5000,DES1CUST0 , SIPN, REG, N/A, 47.11.84.159:5000
/ <Unavailable>, ,,,"",,
```

The Inventory LOCRPT command is modified for SIP Line as follows:

- The command prints multiple entries for a SIPL TN. The number of entries is the based on the number of SCTL clients registered to the TN. However, only the registered clients data is shown in the command printout.
- For different clients, the following fields vary: SCTL Type, Client Hardware ID (TSN), Client IP address.
- The registration status is the registration status of the TN and not the individual client registration status. (There is no special field declared for the client registration status in the sipClientData structure because only the REG TNs are present in the RLM table.)
- The remaining fields such as the location data fields (erl, ecl, etcc) are the same for all clients, since these fields are configured for each TN.
- The HWID is not applicable for a SIPL TN. As a result, the hardcoded string N/A is printed instead of printing the HWID.

STAT SERV

The STAT SERV command prints the APPS as SLG when connected to the SIP Line Gateway (SLG).

The command output also includes the number of registered and busy SIP Line UEXT TNs and Virtual Trunks (VTRKs).

The STAT SERV command can be printed based on the SLG application using the **STAT SERV APP SLG** command.

STIP commands

The STIP commands include the multiple SCTL clients printed in the STIP output. Only registered clients of the TN are printed in the output. The number of rows printed for each TN is equal to the number of SCTL clients configured for the TN in LD 11.

The following example shows the output of the STIP command for a TN, 61 0 with 2 SCTL registered clients:

```
LD 117
STIP TN 61 0
```

```
TN type HWID STATUS HOSTIP SIGNALING IP
61 0 0 0 SIPN MAC: REG 47.11.84.132 47.11.84.158:5000 N/A

CODEC(BW): G711u noVAD(1904)*, G711a noVAD(1904)
MODEL: <USER Agent String>
WID: 0 FWVer:  N/A PEC: NT2K00GI

TN type HWID STATUS HOSTIP SIGNALING IP
61 0 0 0 SIP3 MAC: REG 47.11.84.132 47.11.84.159:5000 N/A

CODEC(BW): G711u noVAD(1904)*, G711a noVAD(1904) MODEL:
<USER Agent String> WID: 0 FWVer:  N/A PEC: NT2K00GI
```

The STIP commands are modified for SIP Line as follows:

- The command prints multiple entries for the SIPL TN. The output contains the same number of entries as the SCTL clients configured for the TN.
- For each entry, the varying fields are: TYPE (SCTL type configured), HWID (TSN data), signaling IP address (client IP address), and the Model (User Agent string of the SIP client)
- The remaining fields in the STIP output are common for all entries.
- For SIPL TNs, the firmware version (FMVER) field is printed as N/A because firmware is not applicable for SIP Line clients.
- The number of entries printed for the command includes the number of entries for each TN.
- Since the HWID is not applicable for a SIPL TN, the hardcoded string N/A is printed instead of printing the HWID.
- The following STIP commands can be queried:

Table 16
STIP commands

Command	Notes
STIP ACF	The STIP command provides the active call failover status for active calls. There is no change to this command for SIP Line.
STIP FW	Firmware (FW) is not applicable for the SIP Line clients. As a result, this command executes a search only for the non-SIPL TNs.
STIP HOSTIP	There is no change to this command for SIP Line, since the host IP address is the same as the SIP Line Gateway (SLG) IP address and the IP address is common for all the entries.

Table 16
STIP commands (cont'd.)

Command	Notes
STIP MODL	This command prints the STIP input for those TNs whose model names match the given input. Since the method used to declare model names for the non-SIPL TNs is different from the User Agent (UA) string of the SIPL TNs, this command also traverses only the non-SIPL TNs.
STIP SIPLUA	This is a new command used to query the SIP Line UA string.
STIP NODE	There is no change to this command for SIP Line.
STIP TERMIP	The term IP for each SIP client is different. As a result, the search criteria is modified to search all SIPL clients to find the match. If a client's term IP matches the input term IP, then the STIP data for that particular client is printed on the TTY.
STIP TN	There is no change to this command for SIP Line.
STIP TYPE	The search criteria is modified to search all SCTL clients to check if any type name matches the input type. If a match is found, then only the STIP report for that particular entry is printed on the TTY.
STIP ZONE	There is no change to this command for SIP Line.

LOCRPT commands

The Location Report (LOCRPT) commands print the SCTL SIP Line client information in the output. Only information for the registered clients is printed. The number of rows printed is equal to the number of clients configured for the TN in LD 11.

The following example shows the output for a SIPL TN with 2 registered clients registered:

```
LD 117
=> LOCRPT ALL
```

```
|           | Prime |                  |     |                    |
|    TN     |  DN   |        Type      |State|        HWID        |
|-----------+-------+------------------+-----+--------------------+
|61  0 0  0 |   5000|SIPN              |REG  |N/A  |
|--------------------------------------------------------------------
|61  0 0  0 |   5000|FMCL              |REG  |N/A  |
|--------------------------------------------------------------------

                              |     |     |      Location       |MAN ND |
      Signaling IP            | ERL | ECL |     Description     |UPD UPD|
------------------------------+-----+-----+---------------------+---+---|
47.11.84.158:5000             |     |     |                     |   |   |
------------------------------------------------------------------------|
47.11.84.142:5000             |     |     |                     |   |   |
------------------------------------------------------------------|

Total number of entries = 2
```

The LOCRPT commands are modified for SIP Line as follows:

- The LOCRPT commands includes all the SCTL clients in the locrpt output. For a SIPL TN, the output has the same number of entries as the number of SCTL clients configured for the TN.
- For each entry, the varying fields are: TYPE (which is the SCTL type), HWID (TSN data), and signaling IP address (IP Phone IP address)
- The remaining data is common for all the IP Phones.
- The number of entries counter is incremented for the number of TNs and this also includes the multiple entries for each SIPL TN.
- The registration (REG) status printed in the output is the registration status of the TN and not the registration status of each IP Phone.
- Since the HWID is not applicable for a SIPL TN, the hardcoded string N/A is printed instead of printing the HWID.
- The following LOCRPT commands can be queried based on different search criteria:

Table 17
LOCRPT command

Command	Notes
LOCRPT ALL	Prints a location report for all registered TN entries in the RLM. By default, this command prints the multiple entries for SIP Line in accordance to the number of SCTL IP Phones configured.
LOCRPT DN	DN is common for the TN and is not specific for each IP Phone.
LOCRPT ECL	ECL is common for the TN and is not specific for each IP Phone.

Table 17
LOCRPT command (cont'd.)

Command	Notes
LOCRPT ERL	ERL is common for the TN and is not specific for each IP Phone.
LOCRPT HWID	Since there is no HWID for the SIP IP Phones, the LOCRPT HWID command search is performed only for the non-SIPL TNs to determine if the input HWID matches with the IP Phone HWID.
LOCRPT IP	If the signaling IP address for any TNs match the input IP address, then the LOCRPT of that TN is printed. The searching function is modified to include the multiple IP Phones for the SIP Line TNs.
LOCRPT MU LOCRPT NU LOCRPT ROAMING LOCRPT TN LOCRPT UNKNOWN LOCRPT UNLOCATED LOCRPT UNREG	These location data fields are common for each TN and are not different for each SIP Line IP Phone. There is no change to these commands for SIP Line.

LD 20

LD 20 includes the SIP Line prompts (SIPL, MCCL, SIPN, SIP3, FMCL, TLSV, SIPU, NDID, SUPR, and HOT U). The overlay also includes the TNB output.

LD 20 is also accepts SIPL as a type. TYPE=SIPL is useful if you want to print any TN based on any SIPU value. A new SIPU prompt is prompted on the TTY, if TYPE=SIPL. If any TNB SIPU matches the input, then that particular TNB is printed. An SCH error is printed if an invalid SIPU is entered.

If TYPE=SIPL is entered, then you must not enter any input for the fields such as TN and CUST, since these fields validate the input with the actual TN type (which is UEXT but not SIPL). As a result, the output does not print the required TN value.

For TYPE=SIPL, you must ensure that the only prompt that can be configured is SIPU (input to SIPU is optional).

LD 20 includes a new SUBR field that indicates the features that the SIP Line IP Phone has subscribed for when it registers (this is done by default for all SIPL UEXT, regardless of IP Phone type). If a SIPL IP Phone is registered, in LD 20, the prt TNB gives the output of SUBR. The included features are Message Waiting Indication (MWI), Ring Again (RGA), Call Waiting (CWI), and Make Set Busy (MSB). The SIP Line Gateway receives a notification message (AML SFN msg) from the Call Server when these features start for a SIPL UEXT.

LD 21

LD 21 accepts SLS (SIP Line Service) as a response for the TYPE prompt.

LD 21 also prints the new prompts introduced in LD 15: SLS, SIPL_ON, SIPD, NMME, and UAPR. These prompts (and their values) are printed when the response to TYPE is CDB or SLS.

LD 21 prints the new SIPL response introduced for the PCID prompt.

Troubleshooting

The following groups of commands are available for troubleshooting the SIP Line service:

- "SLG Application Status commands" (page 129)
- "SLG Trace commands" (page 130)
- "Client/User Status commands" (page 135)
- "Call Server Debug commands" (page 137)

SLG Application Status commands

The SLG Application Status commands include the following:

- slgShow

slgShow

Syntax: slgShow

Description: Shows the summary of the SLG application. This command is a combination of the slgAmlShow, slgTraceShow, and slgAppStatusGet commands.

Example: **`slgShow`**

```
===== General ======
SLG State = AppReady
Total User Registered = 1

===== AML Info ======
hAppBlk TaskName Tid LinkState NumRetry LinkNum Trace
0x18e3aa8 SLG 0xfb00 Up 0 33 0

===== Trace Info ======
No trace enabled
value = 0 = 0x0
```

SLG Trace commands

The SLG Trace commands include the following:

- slgAmlTrace
- slgTraceAdd
- slgTraceRemove
- sipNpmAppDebugSet
- sipNpmAppDataShow

slgAmlTrace

Syntax: vxShell vtrk slgAmlTrace <"tracelevel">

Description: Configures the AML message trace level. The most practical level is 5 to enable message print and full decoding. To turn off AML trace, use level 0.

slgTraceAdd

Syntax: slgTraceAdd <traceType>, <traceValue>

Description: Adds a trace filter. You can add trace filters as needed. All filters are in the “OR” relationship.

The traceType parameter can be one of the following:

- 1= User ID. For example, sipl3420.
- 2 = Contact information, in a format of IP address:port or IP address. For example, 47.11.123.12:5060 or 47.11.123.12.
- 3 = Calling number, DN format. For example, 3420.
- 4 = Called number, DN format. For example, 3420

> ***Note:*** The trace output is sent to the ss_common.log file (the output does not write to TTY). To view the log file, use the following:
> `tail -f /var/log/nortel/ss_common.log`

Example: **`slgTraceAdd 1, sipl3420`**

```
value = 0 = 0x0
->22/10/2006 07:35:31 LOG0006 tSLG: slgTraceAdd_s:  trace
is added, type 1, value sipl3420
```

slgTraceRemove

Syntax: vxShell vtrk slgTraceRemove <traceType>, <traceValue>

Description: Removes a trace filter.

Example: **`vxShell vtrk slgTraceRemove 1, sipl3420`**

```
value = 0 = 0x0
22/10/2006 07:35:44 LOG0006 tSLG: slgTraceRemove_s:  trace
is removed, type 1, value sipl3420
```

sipNpmAppDebugSet

Syntax: vxShell vtrk sipNpmAppDebugSet tSLG <debugField> <debugValue>

Description: Configures a global debug field for SLG (or SSG, if given “tSSG”). The debugField variable is a string name of the debug flag as listed in the following table.

Table 18
debugField variables

debugField variable	Description
rvLogConsole	Prints RVStack trace to console. The value is 0 or 1, where 0 is disable and 1 is enable.
rvLogFile	Prints RVStack trace to file. The value is 0 or 1, where 0 is disable and 1 is enable.
sipMsgMonOut	Prints outgoing message name on callLegMsgToSendEv. The value is 0 or 1, where 0 is disable and 1 is enable.
sipMsgMonIn	Prints incoming message name on callLegMsgReceivedEv. The value is 0 or 1, where 0 is disable and 1 is enable.
sipMsgPrint	Pint SIP msg detail. The value is 0 or 1, where 0 is disable and 1 is enable.
sipCallTraceMsgDetailOn	Prints SIP msg detail for traced call. The value is 0 or 1, where 0 is disable and 1 is enable.
keepAliveMsgPrint	Prints keepalive (OPTIONS) message or not. The value is 0 or 1, where 0 is disable and 1 is enable.
keepAliveSupport	Determines whether keepalive is supported. The value is 0 or 1, where 0 is disable and 1 is enable. The default is 1.
prackSupport	Determines whether PRACK is supported. The value is 0 or 1, where 0 is disable and 1 is enable. The default is 1.
enable415	Determine whether sending 415 is enabled. The value is 0 or 1, where 0 is disable and 1 is enable.

Table 18
debugField variables (cont'd.)

debugField variable	Description
test415	Test sending 415 only. The value is 0 or 1, where 0 is disable and 1 is enable.
gen415Allowed	Determines whether to generate a 415. The value is 0 or 1, where 0 is disable and 1 is enable.
infoSupport	Determines whether the INFO message is supported. The value is 0 or 1, where 0 is disable and 1 is enable. The default is 1.
mcdnUpdate	Determines whether to support an MCDN update. The value is 0 or 1, where 0 is disable and 1 is enable.
mcdnDebug	Enable and print MCDN debug. The value is 0 or 1, where 0 is disable and 1 is enable.
esn5Debug	Enable and print ESN5 debug. The value is 0 or 1, where 0 is disable and 1 is enable.
loopbackSupport	Determines whether loopback is supported. The value is 0 or 1, where 0 is disable and 1 is enable.
maskLoopCode	Masks the code added for loop detection. Set to FALSE to mask it. The value is 0 or 1, where 0 is disable and 1 is enable.
optionSupport	Determines whether OPTIONS is supported. The value is 0 or 1, where 0 is disable and 1 is enable.
renegotiationFlag	Determines whether TLS renegotiation is enabled. The value is 0 or 1, where 0 is disable and 1 is enable.
sdptDebug	Used for SDP-transparancy. The value is 0 or 1, where 0 is disable and 1 is enable.
sslConnectionDebug	Used for SSL connection debug print. The value is 0 or 1, where 0 is disable and 1 is enable.
regTrace	Traces gateway registration. The value is 0 or 1, where 0 is disable and 1 is enable.
sniffPrint	Print sniffer messages. The value is 0 or 1, where 0 is disable and 1 is enable.
tcpPersistency	Used for TCP transport. The value is 0 or 1, where 0 is disable and 1 is enable.
SDescLevel	Syslog level.
mediaTestLogLevel	Syslog level.

Table 18
debugField variables (cont'd.)

debugField variable	Description
eventLogLevel	Syslog level.
forkingLogLevel	Syslog level.
keepAliveLogLevel	Syslog level.
tlsLogLevel	Syslog level.
tlsRenegotiateLogLevel	Syslog level.
traceID	The SIP VTRK channel ID being traced.
acpDebug	Prints ACM messages for a specific Channel ID (CHID).

Example: **`vxShell vtrk sipNpmAppDebugSet tSLG sipMsgPrint 1`**

```
sipMsgPrint changed from 0 to 1
value = 0 = 0x0
```

sipNpmAppDataShow

Syntax: vxShell vtrk sipNpmAppDataShow tSLG <showLevel>

Description: Prints out details of an SIP Network Protocol Manager (SIPNPM)-based application data.

Example: **`vxShell vtrk sipNpmAppDataShow tSLG 5`**

```
Application = tSLG, Category = 0xfb00
MsgQId = 0xfb, MsgType = 0xfb00, MsgQSize = 100000,
MsgQFD=0x3c
GlobalData Address=0x19c9de4, CallBackData Address=0x1
9cf48c

tSLG -- StatusData Address = 0x19c7e38
================================
appInitialized = yes
appStop = no
stackInitialized = yes
proxyRegistered = no

tSLG -- DebugData Address = 0x19c7e48
===============================
rvLogFile = 0
rvLogConsole = 0
sipMsgMonOut = 0
sipMsgMonIn = 0
sipMsgPrint = 1
```

```
sipCallTraceMsgDetailOn = 0
keepAliveMsgPrint = 0
keepAliveSupport = 1
prackSupport = 1
enable415 = 1
test415 = 0
gen415Allowed = 0
infoSupport = 1
mcdnUpdate = 1
mcdnDebug = 0
esn5Debug = 0
loopbackSupport = 0
maskLoopCode = 0
optionSupport = 0
renegotiationFlag = 0
sdptDebug = 0
sslConnectionDebug = 0
regTrace = 0
sniffPrint = 0
snifferFilter = ::0
tcpPersistency = 0
SDescLevel = 7
mediaTestLogLevel = 7
eventLogLevel = 7
forkingLogLevel = 7
keepAliveLogLevel = 7
tlsLogLevel = 7
tlsRenegotiateLogLevel = 7
traceID = -1
acpDebug = 0

tSLG -- ConfigData Address = 0x19c80e8
==============================
Domain = bvwdesign.com
Local Port = 5070
RvSipStackCfg = 0x19c9a1c
RvSdpStackCfg = 0x19c9d60
RvSipMidCfg = 0x19c9d70

tSLG -- StackData Address = 0x19c9da0
==============================
RvSipStackHandle = 0x31be0004
RvSipMsgMgrHandle = 0x2e935f60
RvSipCallLegMgrHandle = 0x2f28ec00
RvSipTransportMgrHandle = 0x2f8e69cc
RvSipTransmitterMgrHandle = 0x2f055be8
RvSipSubsMgrHandle = 0x2f0c67b4
```

```
RvSipMidMgrHandle = 0x2f0364a4
RvSipTranscMgrHandle = 0x2f2df0c8
HRPOOL = 0x193982b4
RV_LOG_Handle = 0x31be0380
RV Log file = /u/log/SlgRvSip.log

tSLG -- GlobalData Address = 0x19c9de4
================================


tSLG -- CallBack Functions = 0x19cf48c
================================
appMsgHandler = 0x15a5f40
cardEventHandler = 0x15a6110
configParaGet = 0x15afef0
tlsConfigGet = 0x15b0270
appInit = 0x15a5ea0
appShutdown = 0x15a5ed0
stackCallbackSet = 0x0
sipUriCreate = 0x15b0740
sipSessionDel = 0x15b08f0
callLegStateChgEv = 0x15ad150
callLegMsgToSendEv = 0x15ad190
transactionStateChangedEv = 0x15ad260
```

value = 0 = 0x0

Client/User Status commands

The Client/User Status commands include the following:

- slgSetShowAll
- slgSetShowByUID
- slgCallShowByUID

slgSetShowAll

Syntax: slgSetShowAll

Description: Provides a brief list all users on this SLG.

Example: **`slgSetShowAll`**

```
UserID TN Clients Calls SetHandle
-------------- -------------- ------- ----- ---------
sipl3420 104-00-02-00 1 0 0x322abcdc
```

slgSetShowByUID

Syntax: slgSetShowByUID userID

Description: Provides a detailed list of user information.

Example: **slgSetShow sipl3420**

```
UserID TN Clients Calls SetHandle
--------------- -------------- ------- ----- ---------
sipl3420 104-00-02-00 1 0 0x322abcdc
StatusFlags = Registered Controlled KeyMapDwld
FeatureMask =
Current Client = 0, Total Clients = 1
Num IP:Port:Trans Type UserAgent x-nt-guid RegDescrip
RegStatus PbxReason SipCode
0 47.11.181.132:5060 :udp SIPN Nortel PCC 4.0.398 Login" 2
OK 200
Key Func Lamp Label
0 3 0 3420
1 6 0
2 2 0 453420
17 16 0
18 18 0
19 27 0
20 19 0
21 52 0
22 25 0
24 11 0
25 30 0
26 31 0
value = 0 = 0x0
```

slgCallShowByUID

Syntax: vxShell vtrk slgCallShowByUID userID

Description: Lists the transient or active calls for a user.

Example: **vxShell vtrk slgCallShowByUID sipl3420**

```
num hParantCall dir type state chid msgId callId
calling(DN:TN:Type) called(DN:TN:Type)
1 0x0 1 1 2 -1 0 0x0 3420:0x6808:  0 3010:0x0:  0 0x2f0af834
1 3 2 31 0 0x7654de5 3420:0x6834:  0 453420:0x6808:  8
0x2f0af834 1 2 2 -1 7 0x7664de4 3420:0x6808:  8 3010:0x0:
0 value = 0 = 0x0
```

The following table describes the dir, type, and state columns in the previous output.

Table 19
Command ouptut description

Column heading	Description of output
Dir	The direction of the call. • 1 = Outgoing call from SIPL • 2 = Incoming call to SIPL
Type	The call or subcall type. • 1 = the main call • 2 = call on Prime Directory Number (PDN) • 3 = call on User Agent Directory Number (UADN)
State	The call state. • 1 = Connecting. This state is a transient state. The call has sent a request (for example, CON to CS or INVITE to SLG) and is waiting for a response (for example, waiting for CRS or SIP). • 2 = Ringing. The called party is ringing. • 3 = Active. The call is established between two parties. • 4 = Merging/Linking. This state is a transient state. The merge/link request is sent and is waiting for a response from the Call Server. • 5 = RlsPending. This state is a transient state. CALLDIS is sent, waiting for CALLDIS OK from the Call Server. • 6 = Completed. The call is released or abandoned by one party. The call structure is cleaned at this state. Typically, you do not see this state. However, if this state is printed, it indicates a memory leak or improper logic in code. • 7 = Cancelled. The call is abandoned by caller before answer. The call structure is cleaned at this state. Typically, you do not see this state. However, if this state is printed, it indicates a memory leak or improper logic in code.

Call Server Debug commands

The Call Server Debug commands include the following:

- rlmShowUext
- rlmSetUserFilters

rlmShowUext

Syntax: rlmShowUext

Description: Prints the registered client information on the Call Server.

Example: **`pdt> rlmShowUext`**

```
TN CUSTOMER STATUS USERID HOSTIP Media IP PORT
_______________________________________________________________
0x6808 00000004 REG sipl3420 47.11.216.242 47.11.170.136
0x13c4 47.11.181.132 0x13c4
```

rlmSetUserFilters

Syntax: rlmSetUserFilters

Description: Configures the registration logs for a user.

Example: **`pdt> su`**

`-> rlmSetUserFilters(0, 0)`
—Turn logging off.

`-> rlmSetUserFilters(1, 0)`
—Turn logging on for all filterUserIds.

`-> rlmSetUserFilters(2, "<filterUserId>")`
—The command to turn logging on for only the filterUserId in the <filterUserId> variable.

SIP Line Gateway Maintenance commands in Element Manager

The SIP Line Gateway (SLG) service provides a set of SIP Line maintenance commands. The General Commands page (in Element Manager) includes a group called SipLine that contains commands related to the maintenance of the SLG service.

Use the following procedure to access the SIP Line maintenance commands in Element Manager.

Procedure 13
Accessing the SIP Line maintenance commands

Step	Action
1	Start Element Manager.
2	In the navigation tree, select **System > IP Network > Maintenance and Reports**. The **Node Maintenance and Reports** page appears.

3 Expand the node.

4 Click **GEN CMD**.

The General Commands page appears.

5 From the **Group** list, select **SipLine**.

The Command list populates with the SIP Line commands.

6 From the **Command** list, select the SIP Line command you want to run.

7 Click **RUN**.

The command output appears in the pane in the lower half of the window.

--End--

Scenarios

The following sections describe troubleshooting scenarios.

AML link is down

If the AML link is down, check the following items:

- Is the ELAN AML properly configured? Check LD 21.
- Is the SIPL trunk properly configured? Check LD 21.
- Is the SLG properly configured? Check the task and thread status. Also check the config.ini parameters.

Client registration is rejected

If a client registration is rejected, one of the following problem can be the reason for the registration rejection:

- 404 – The user ID is not properly configured. This message indicates that a Maximum Client Count Limit (MCCL) type mismatch occurred.
- 400 – Errors occurred during parsing of the REGISTER message. Verify error logs on the SIP Line Gateway (SLG).

SIP Line Conversion Utility

The SIP Line Conversion Utility (SIPLCU) is an off-switch utility that assists in the conversion of CS 1000 Release 5.5 SIP Phone functionality to CS 1000 Release 6.0 SIP Lines. The utility that runs from a Windows PC. The support platforms are Windows 2000, Windows XP, and Windows Vista.

The SIP Line Conversion Utility uses a combination of the current switch configuration and customer supplied user names, passwords, and other pertinent SIP Phone specific information. The data populates an Excel spreadsheet and the utility uses this information to convert UEXT SIPN or SIP3 phones configured on the Call Server to the new UEXT SIPL format. Connection to the target Call Server is by way of the associated Signaling Server (using a telnet connection). The utility provides the greatest benefit to users that have more than 25 UEXT SIP or SIP3 phones.

The SIP Line Conversion Utility includes a built-in Help menu, which provides detailed operating instructions on use of the utility.

Filename and location

The SIP Line Conversion Utility is stored on the Signaling Server and can be downloaded using secure FTP (sFTP) or Secure Copy (SCP).

The filename of the SIP Line Conversion Utility is SIPLCU.msi and the file is located in the following directory: /opt/nortel/vtrk/extra

The username is nortel and the password is specific to your site.

Install the SIP Line Conversion Utility

Use the following procedure to install the SIP Line Conversion Utility.

Procedure 14
Installing the SIP Line Conversion Utility

Step	Action
1	Double click the **My Computer** icon on your desktop.

2. Navigate to the folder where you downloaded the SIPLCU.msi file.
3. Double click the **SIPLCU.msi** installation file.
4. Follow the on-screen instructions to install the SIP Line Conversion Utility application on your computer.

--End--

Nortel Communication Server 1000

SIP Line Fundamentals

Release: 6.0
Publication: NN43001-508
Document revision: 01.08
Document release date: 9 February 2010

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

www.nortel.com

NORTEL