Nortel Communication Server 1000

SIP Trunk Bridge Fundamentals

Release: 7.0
Document Revision: 01.02

www.nortel.com

NN43001-143

Nortel Communication Server 1000
Release: 7.0
Publication: NN43001-143
Document release date: 15 June 2010

Contents

New in this release

The following sections detail what's new in *SIP Trunk Bridge Fundamentals* (NN43001-143) for Nortel Communication Server 1000 Release 7.0:

Features

The *SIP Trunk Bridge Fundamentals* (NN43001-143) is new for Communication Server 1000 Release 7.0.

Other changes

This release contains no other changes. This section contains the following topic:

- “Revision history” (page 9)

Revision history

June 2010	Standard 01.02. This document is issued to support Communication Server 1000 Release 7.0.

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 describes the SIP Trunk Bridge Service and how to implement SIP Trunk Bridge as part of your system.

This document contains the following chapters:

Note on legacy products and releases

This document contains information about systems, components, and features that are compatible with Nortel Communication Server 1000 Release 7.0 (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
- Communication Server 1000M Multi Group
- Communication Server 1000E

Intended audience

This document is intended for individuals who administer Communication Server 1000 SIP Trunk Bridge systems.

Terminology

In this document, the term system refer generically to the following systems:

- Communication Server 1000E
- Communication Server 1000M

Unless specifically stated otherwise, the term Bridge Manager refers to the Communication Server 1000 SIP Trunk Bridge Manager and SIP Trunk Bridge refers to Communication Server 1000 SIP Trunk Bridge.

Related information

This section lists information sources that relate to this document.

Technical documentation

This document references the following technical documents:

- *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 Software Upgrades* (NN43041-458)
- *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

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 Trunk Bridge overview

SIP Trunk Bridge inter-operates Communication Server 1000 with SIP Trunk Carriers or Internet Telephony Service Provider (ITSP).

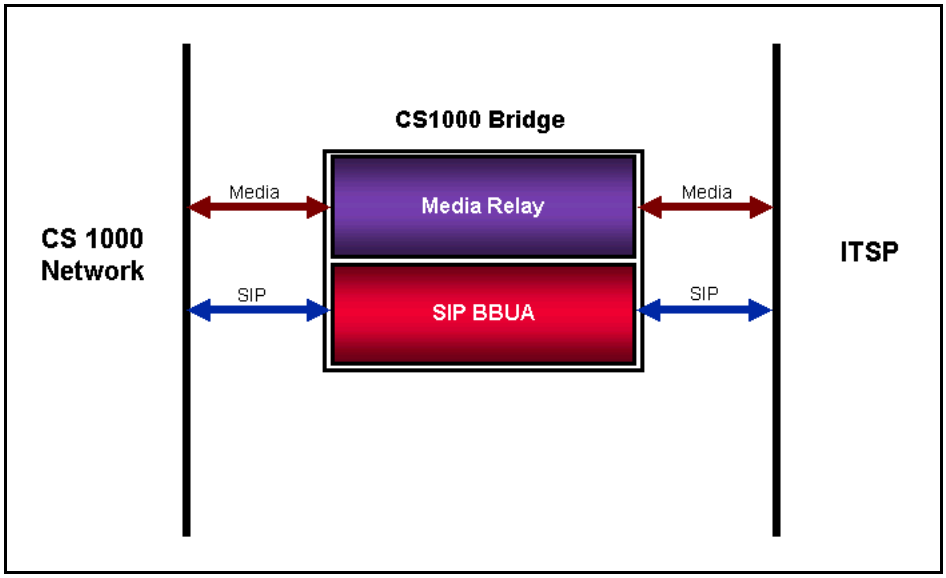
SIP Trunk bridge has the following functionality:

- Mediates SIP signals from Communication Server 1000 to ITSP.
- Mediates SIP signals from ITSP to Communication Server 1000
- Relays the media (for example, Voice, RTP) with specific deployment models.

  For more information about deployment models, see “Deployment models” (page 24).
- Detects Mid Call digit on an IP call. It intercept the RFC2833 digits, continue to pass it through but also send INFO message to the Communication Server 1000 with digits dialed in the RFC2833 to trigger Mid Call features. The Mid Call feature is used in conjunction with the MobileX feature.
- Cost effective solution compared with third party Session Border Controller (SBCs)
- Eliminates the need for a dedicated Signaling Server SIP Gateway with special patches to handle individual carrier inter-operation issues
- Provides a manual ITSP profile configuration. Administrator can configure the parameters for selected ITSP compatibility
- Deals with the NAT traversal

The Communication Server 1000 SIP Trunk Bridge is a light Session Border Controller (SBC). It uses a signaling component SIP back-to-back user agent (BBUA) and a media component media relay to inter-operate the Communication Server 1000 with Internet Telephony Service Providers (ITSPs) or SIP Trunk Carriers as shown in Figure 1 "CS 1000 inter-operate with ITSP" (page 16). It deals with the NAT traversal. In Release 7.0, SIP Trunk Bridge supports UDP and TCP.

Figure 1
CS 1000 inter-operate with ITSP

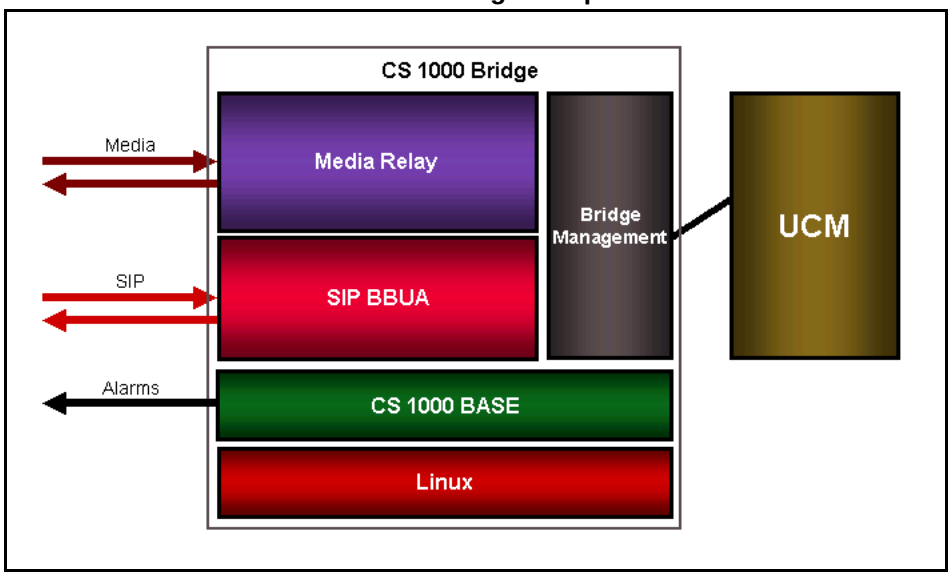


The SIP Trunk Bridge is a cost-effective solution compared with third- party SBCs. It eliminates the need for a dedicated Signaling Server SIP gateway trunk with special patches to handle individual carrier inter-operating issues.

SIP Trunk Bridge architecture

Figure 2 "Communication Server SIP Trunk Bridge components" (page 16) shows the Communication Server 1000 SIP Trunk Bridge architecture.

Figure 2
Communication Server SIP Trunk Bridge components



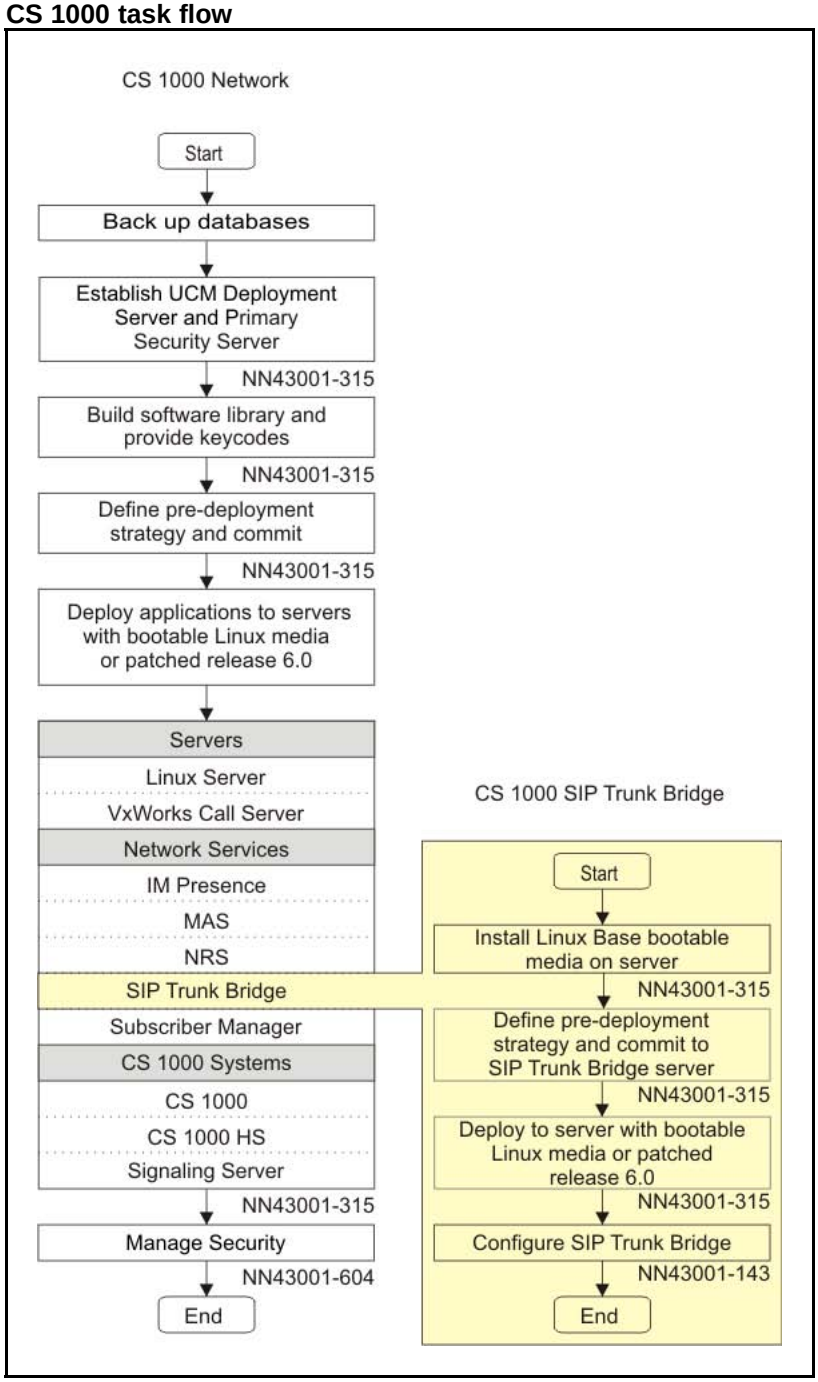
- SIP BBUA: This is a back-to-back user agent for SIP signaling. It deals with the service requests, including connect, disconnect, authentication, and authorization.
- Media Relay: This component manages media flow through the bridge.
- Bridge Management: SIP Trunk Bridge is configured using the Bridge Manager.
- UCM: The Bridge Manager is launched using the Unified Communication Manager (UCM).

  For more information see Procedure 1 “Logging on to UCM” (page 39) and “Navigating to SIP Trunk Bridge Manager from UCM” (page 40).
- CS 1000 base: The Linux base customized for Communication Server.
- Linux: The application to be run and deployed on the Linux server.

Communication Server 1000 task flow

This section provides a high-level task flow for the installation or upgrade of a Communication Server 1000 system. The task flow indicates a recommended sequence of events to perform when you configure a system and provides the technical document number that contains the detailed procedures required for the task.

Figure 3
CS 1000 task flow



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

SIP Trunk Bridge features

SIP Trunk Bridge supports the following features:

ITSP interop

SIP Trunk Bridge mediates signals and media to and from ITSPs. For more information, see "Deployment models" (page 24).

Mobile X

SIP Trunk Bridge detects the mid-call digits on an IP call for mid-call features using the Mobile X feature. To trigger this feature on the Call Server, the incremental feature intercepts the RFC2833 digits and sends an INFO message to the Communication Server with the RFC2833 dialed digits.

NAT traversal

In a typical SIP Trunk Bridge deployment, SIP Trunk Bridge is connected to an enterprise LAN. The enterprise LAN typically has a firewall and Network Address Translator (NAT) that translates global addresses to private (non-routable) addresses.

The SIP Trunk Bridge service is implemented as a Back To Back User Agent (B2BUA) that enables NAT traversal and connectivity to an Internet Telephony Service Provider (ITSP). It anchors media and provides rewriting of the SIP or SDP headers so that packets can pass through the firewall or NAT. This is routed from an ITSP to the SIP Trunk Bridge server through a NAT and vice versa.

SIP Trunk Bridge supports both dynamic NAT and static NAT. It re-writes SIP or SDP headers in the call setup signaling as needed by the ITSP. It also keeps NAT bindings alive using periodic outbound signaling if needed (for example use empty packets for RTP keep alive and CR-LF sequences for SIP keep alive).

Backup and restore

SIP Trunk Bridge supports configuration backup and restore.

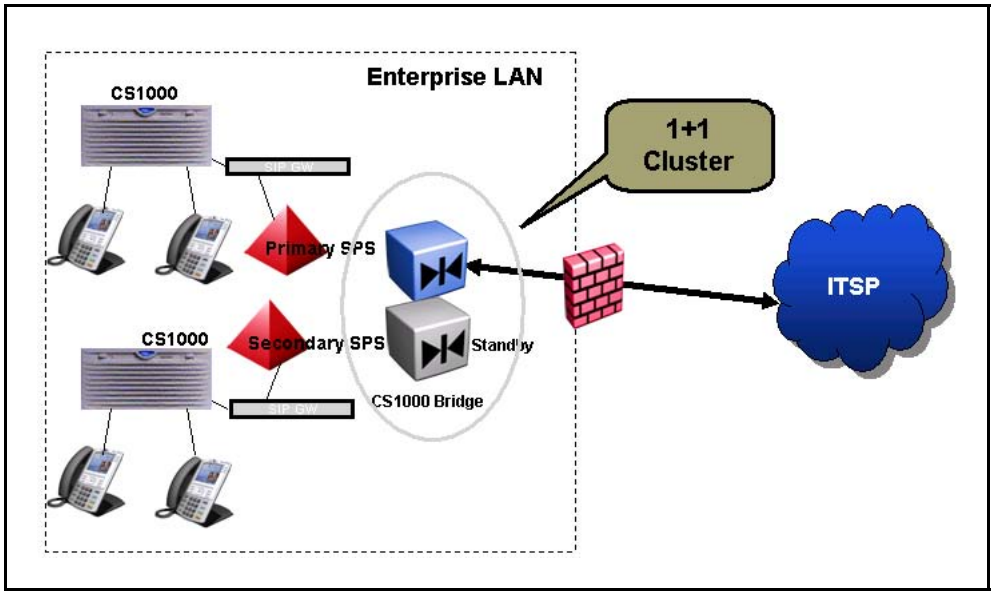
For more information about deployment parameters, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Redundancy

Communication Server 1000 SIP Trunk Bridge supports redundancy. Before deploying the SIP Trunk Bridge, configure the redundancy in Deployment Manager. This model supports one Active plus one Standby server. The Standby server assumes the IP address of the failed server. Inbound traffic terminates on one IP address. The SIP Proxy Server (SPS) may route the traffic distribution to alternative servers for outbound calls.

Virtual IP is issued for communication with SIP Trunk Bridge. If the primary server goes down, secondary server takes over the Virtual IP and continues the service. When primary server is up again, it takes the Virtual IP and continues the service. This time the secondary server becomes the standby server and goes to standby mode. The data configured on the primary is synchronized with the secondary. For the larger setups, you can deploy the multiple SIP trunk Bridge cluster.

Figure 4
1+1 High Availability Cluster



Planning and engineering

This chapter contains the following topics:

SIP Trunk Bridge platforms and capacity

The following are the supported platforms and their capacities:

Table 1
SIP Trunk Bridge Platforms and Capacity

Platform	Capacity
COTS2	2.5 GHZ Quad-Core Xeon\4 GB DDR2.
CPDC	1.8 GHz low power AMD Dual Core\2 GB DDR2 (expandable to 4 GB), single 80 GB disk, USB installation.

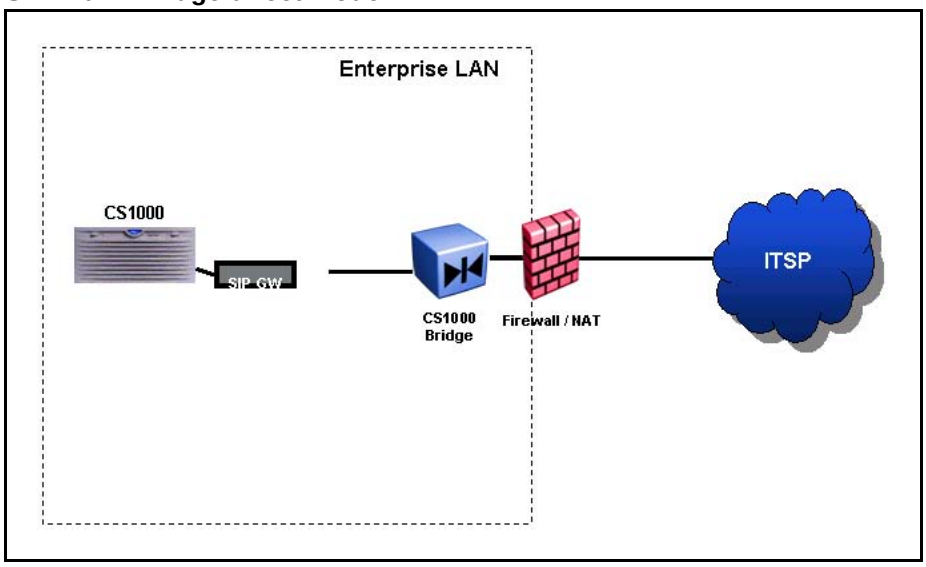
Deployment models

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

Direct model

Figure 5 "SIP Trunk Bridge direct model" (page 24) illustrates the direct model for SIP Trunk Bridge.

Figure 5
SIP Trunk Bridge direct model



In direct mode, SIP Signaling Gateway directly points to the bridge without the SPS or any other SIP component. The SIP Trunk Bridge is in between Communication Server 1000 and the ITSP. In this mode, following parameters must be selected or configured in the Bridge Manager in CS1000 Account section:

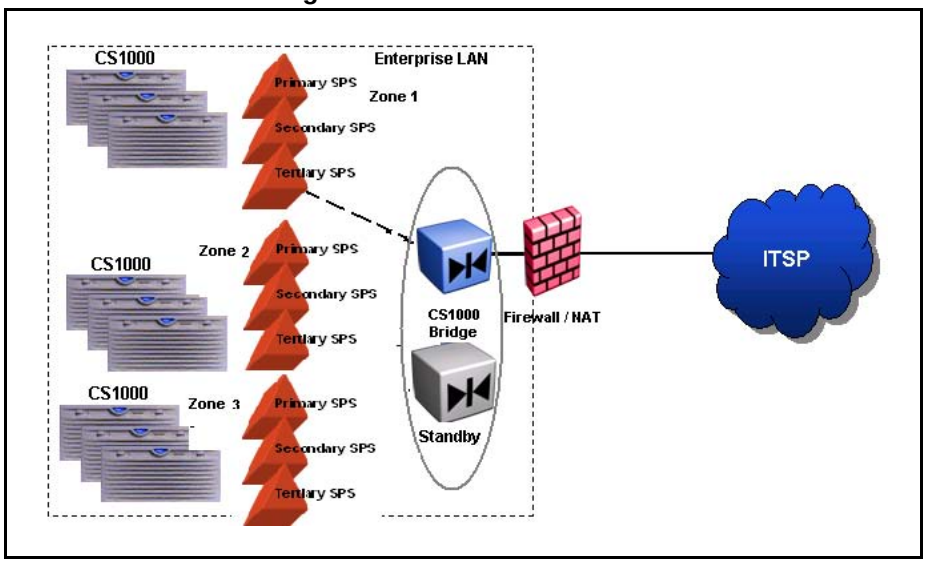
- Mode: Direct
- CS 1000 signaling gateway node IP address

For information about configuration of these parameters, see “CS1000 Account” (page 50).

SPS Model

Figure 6 "CS 1000 SIP Trunk Bridge SPS model" (page 25) illustrates the SPS model for SIP Trunk Bridge.

Figure 6
CS 1000 SIP Trunk Bridge SPS model



In the SPS model, the SPS directs traffic through the SIP Trunk Bridge as an endpoint and then the Bridge directs traffic to the ITSP. In this mode, following parameters must be selected or configured in the Bridge Manager in CS1000 Account section:

- Mode: SPS
- Primary SPS IP address
- Secondary SPS IP address
- Tertiary SPS IP address

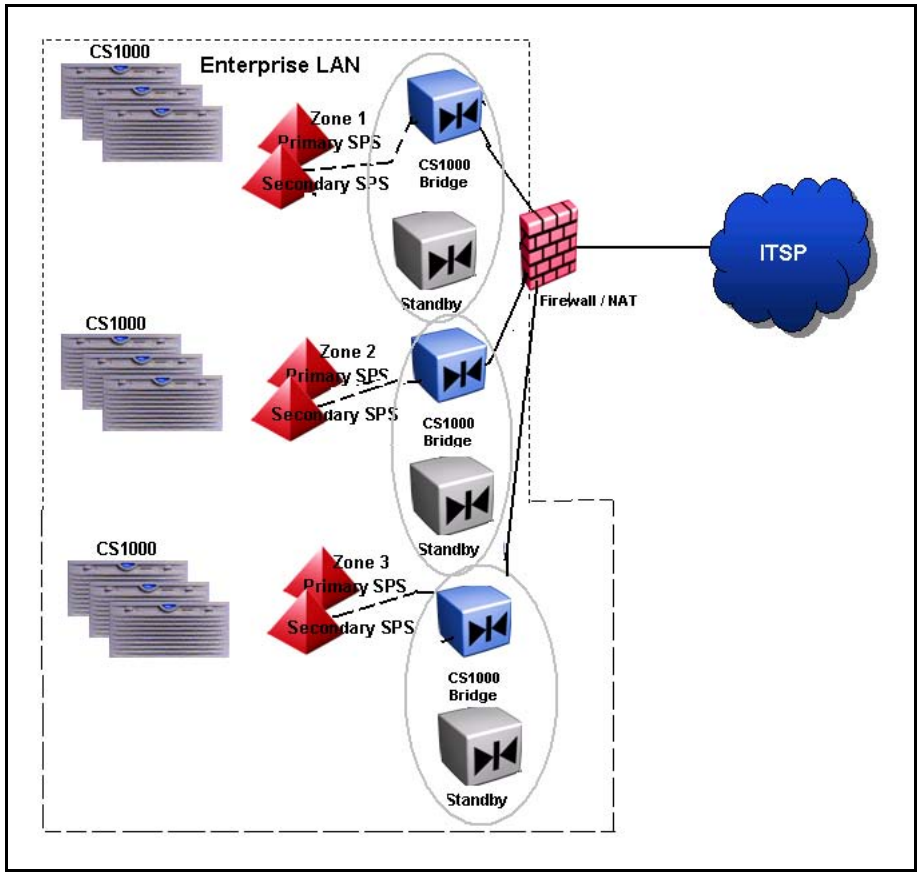
For information about configuration of these parameters, see “CS1000 Account” (page 50).

For multi zone SPS deployment model, if SPS responses with 300 or 302, then Bridge tries to connect to the address provided in the 300 or 302 redirection responses of that SPS.

Multiple cluster deployment

Figure 7 "Multiple cluster deployment" (page 26) illustrates the deployment model for multiple Bridge cluster.

Figure 7
Multiple cluster deployment



For large setup, you can deploy the multiple SIP Trunk Bridge clusters. In larger setups, you can have as many clusters as you want. That is, there is no limit to the number of clusters. The preceding figure shows the setup having three clusters.

Each SIP Trunk Bridge can be configured in direct or SPS mode.

For more information about direct and SPS model, see “Direct model” (page 24) and “SPS Model” (page 25).

LAN deployment behind firewall or NAT

The deployment behind firewall or NAT for SIP Trunk Bridge can be done either in direct mode or SPS mode as shown in the figures Figure 8 "LAN deployment behind firewall or NAT - SPS" (page 27) and Figure 9 "LAN deployment behind firewall or NAT - Direct" (page 27) respectively

Figure 8
LAN deployment behind firewall or NAT - SPS

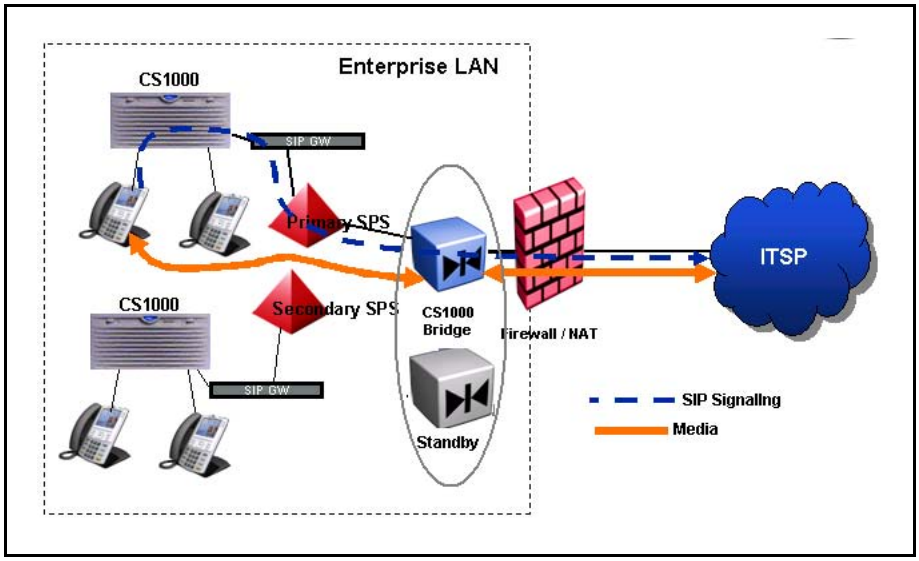
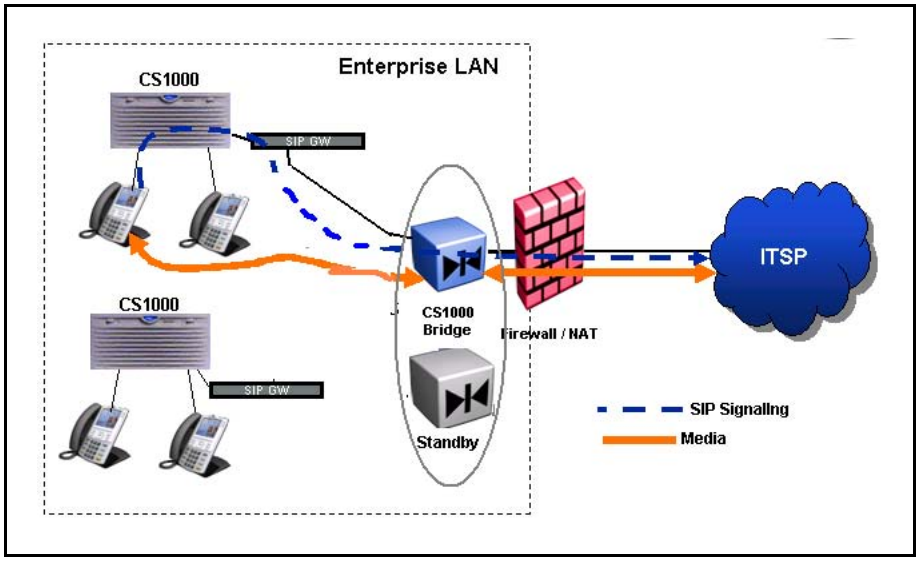


Figure 9
LAN deployment behind firewall or NAT - Direct



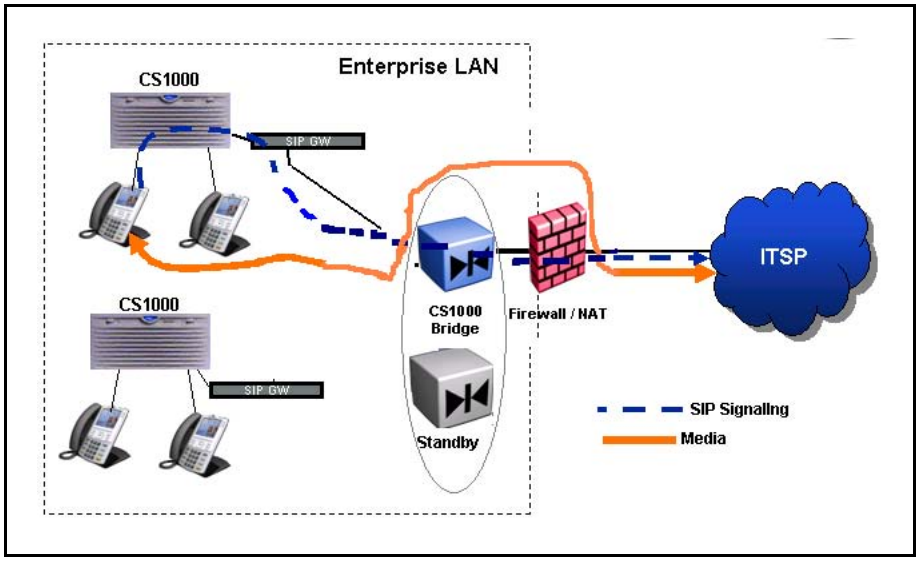
SIP Trunk is deployed in the private network and the ITSP is on public network, therefore, if VPN is not configured, SIP Trunk Bridge has to be behind NAT. In this model, SIP Trunk Bridge relays the media.

For more information about NAT configuration, see “NAT” (page 44).

LAN deployment without NAT

Figure 10 "LAN deployment without NAT" (page 28)illustrates the LAN deployment without NAT.

Figure 10
LAN deployment without NAT

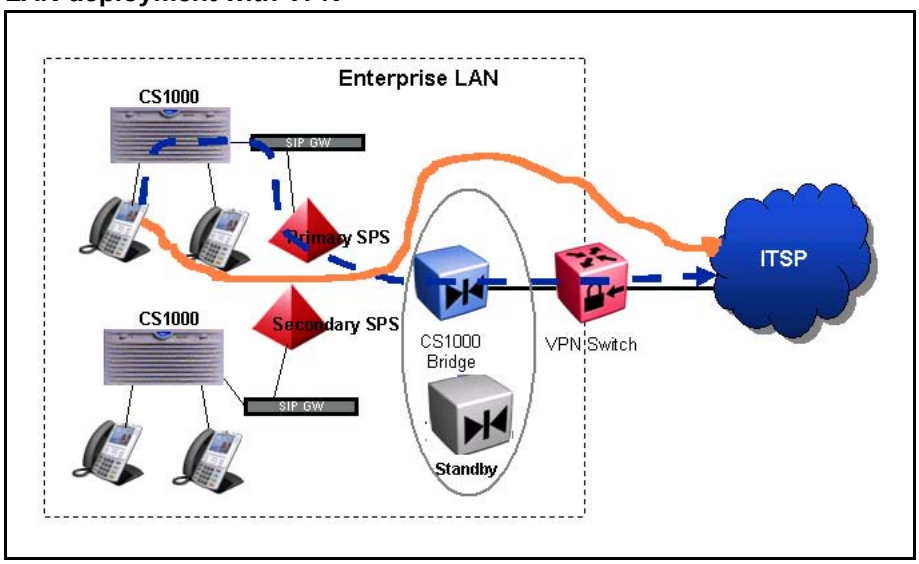


In this model, media flows directly to the ITSP from the CS 1000 and not relayed through the SIP Trunk Bridge or firewall. But the SIP Signaling is relayed through the SIP Trunk Bridge.

LAN deployment with VPN

Figure 11 "LAN deployment with VPN" (page 28) illustrates the LAN deployment with VPN for SIP Trunk Bridge.

Figure 11
LAN deployment with VPN



In this model, the SIP Trunk Bridge tunnels through the VPN Switch. You do not need to configure the NAT parameters, as the VPN is connected in between the SIP Trunk Bridge and the ITSP.

ATTENTION
If you want the media to relay through the Bridge, you need to enable the NAT and configure the public IP address as same as the virtual IP address of the Bridge. For information on the configuration, see Procedure 3 “Editing NAT properties” (page 44)

RFC compliance

The SIP Trunk Bridge complies with the following Request for Comments (RFC):

- RFC3261 Session Initial Protocol
- RFC3264 Offer/Answer Model with SDP
- RFC3311 UPDATE
- RFC3262 PRACK
- RFC3515 REFER
- RFC2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals. If NAT is not configured, media flow is end to end and Bridge cannot collect mid call digits.
- RFC4567 Key Management Extensions for SDP and RTSP
- RFC4568 Session Description Protocol (SDP) Security Descriptions for Media Streams (SDesc)

Operating parameters

The SIP Trunk Bridge has the following operating parameters:

- In Release 7.0, the SIP Trunk Bridge cannot co-reside with any other applications. It is a stand-alone component and cannot co-reside with UNIStim LTPS, NRS, or Gateway applications such as SIP Gateway or H.323 Gateway.
- In direct model, only one Communication Server can be connected with Bridge.
- In SPS model, more than one Communication Server can be used. NRS or SPS manages Communication Server routing.
- Release 7.0 supports a single SIP Trunk Bridge for a single ITSP. For multiple ITSPs, you will require multiple SIP Trunk Bridges.
- SIP Trunk Bridge cannot be co-located with the Primary UCM security domain server. The Deployment Manager manages and enforces these restrictions.
- You must do the deployment again, if you want to change:

— from redundant mode to non-redundant mode or vice versa,

— the virtual IP, primary IP, or secondary IP

To redo the deployment, delete the Bridge view from Deployment Manager, un-deploy the Bridge application and then recreate the Bridge view and deploy the Bridge application. After the deployment, configure the parameters on the Bridge Manager again.

- You must configure all the Bridge parameters through Bridge Manager before running the sipxsetup.

  For information about configuration of parameters, see Procedure 2 “Editing General Properties” (page 43), Procedure 3 “Editing NAT properties” (page 44), Procedure 4 “Editing ITSP Account” (page 46), and Procedure 5 “Editing CS1000 Account” (page 50).

  For information about post configuration steps, see “Running the sipxecs setup” (page 53).

- If you want to upgrade the SIP Trunk Bridge, you must upgrade the Communication Server 1000 system to the same release as that of SIP Trunk Bridge.

- The SIP port in the General Properties section is different than the Public SIP port in the NAT section. For information on the SIP port in General properties section, see step 1 in Procedure 2 “Editing General Properties” (page 43). For information on the Public SIP port in NAT, see step 5 in Procedure 3 “Editing NAT properties” (page 44).

Limitations

Following are the limitations of the SIP Trunk Bridge:

- SIP Trunk Bridge does not support media transcoding.
- In Release 7.0, SIP Trunk Bridge does not support IPv6 format.
- Changes to any parameter using Bridge Manager requires restarting of the services.

  For information about how to restart the services, see “Troubleshooting” (page 57).

- Host name of the server hosting Bridge should not contain any capitalized name. In Release 7.0, FQDN (hostname+domain) with capitalized letters is not supported.

Installation

Use Deployment Manager to install and deploy Communication Server 1000 (CS 1000) SIP Trunk Bridge.

To install and deploy the software to the target primary and secondary SIP Trunk Bridge servers, you must configure the deployment parameters in the Deployment Manager GUI. The deployment parameters includes:

- Cluster name
- Cluster ID
- Virtual IP address
- Cluster mode
- Primary server
- Secondary server

You can deploy the Communication Server 1000 SIP Trunk Bridge as:

- Non-redundant single server (1 server mode)
- Redundant two server (1+1 server mode)

This single or two-server configuration is a cluster.

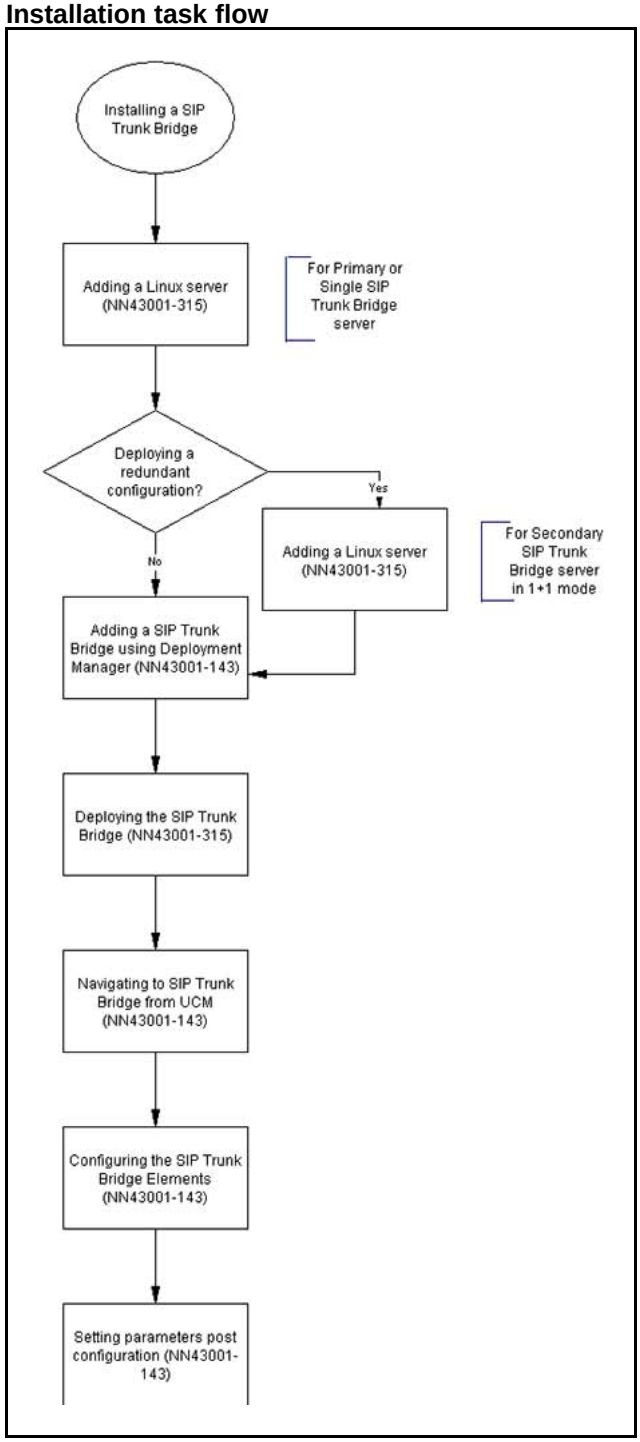
Communication Server and the ITSP point to the virtual IP address in redundant and non-redundant modes. The virtual IP address has to be different from the primary and secondary IP addresses. All these IP addresses must be on same subnet.

For more information about server configuration and configuration of deployment parameters and SIP Trunk Bridge deployment, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

Installation task flow

This section provides a high-level task flow for the installation of a SIP Trunk Bridge. 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 12
Installation task flow



Upgrades

To upgrade the SIP Trunk Bridge, follow these steps:

Step	Action
1	Take a back up of the configuration data.
2	Upgrade the SIP Trunk Bridge.
3	Restore the data.

--End--

For more information about backup and restoring the data and SIP Trunk Bridge upgrade, see *Linux Platform Base and Applications Installation and Commissioning* (NN43001-315).

After the upgrade, run the sipxces setup.

Patch management

You must run the sipxecs-setup on the servers that have SIP Trunk Bridge applications as a **root** user after applying the SIP Trunk Bridge patch *nortel-cs1000-sipbridge-X.XX.XX-XX.i386.XXX*. This special instruction should be followed when applying SIP Trunk Bridge patch to Linux server.

For more information about Nortel Linux patching see, *Patching Fundamentals* (NN43001-407).

ATTENTION
It takes a few moments for the services to be up after you run the sipxecs setup.

Operations

This chapter contains the following topics:

Logging on to Unified Communications Management

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

Procedure 1
Logging on to UCM

Step	Action
1	Open the Web browser.
2	Enter one of the following in the Address bar. • UCM framework IP address—After you enter the UCM framework IP address, a Web page appears stating that you must access UCM 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**.

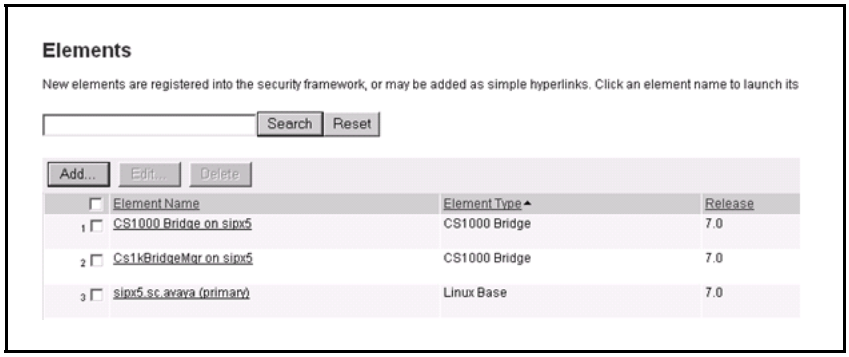
The default navigation Web page for UCM appears.

--End--

Navigating to SIP Trunk Bridge Manager from UCM

Step	Action
1	Login to the UCM web page. Bridge Manager appears as an element in the UCM table as shown in Figure 13 "UCM table" (page 40).

Figure 13
UCM table



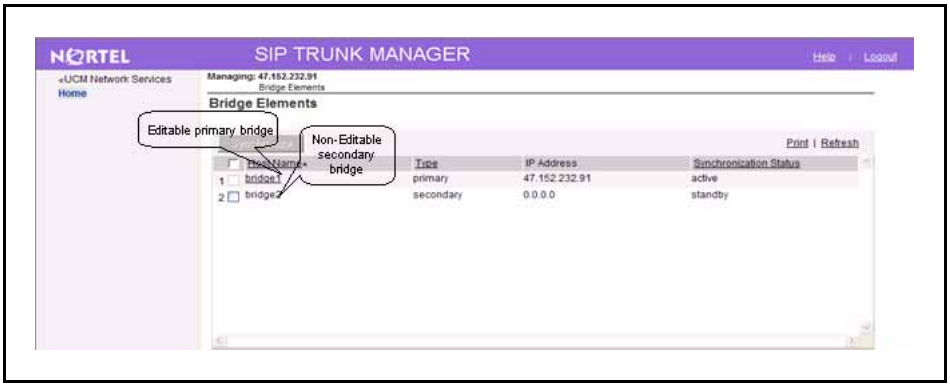
2	Click on the respective element link to navigate to the Bridge Manager.

--End--

SIP Trunk Bridge Elements

Bridge Manager is available for both primary and secondary bridges. The bridge elements in a particular cluster are listed in the Figure 14 "Bridge Element Home page" (page 41). The master configuration is maintained in the primary server. Therefore, you can configure the parameters only from the primary server. You can only view the configuration from secondary server and cannot modify it.

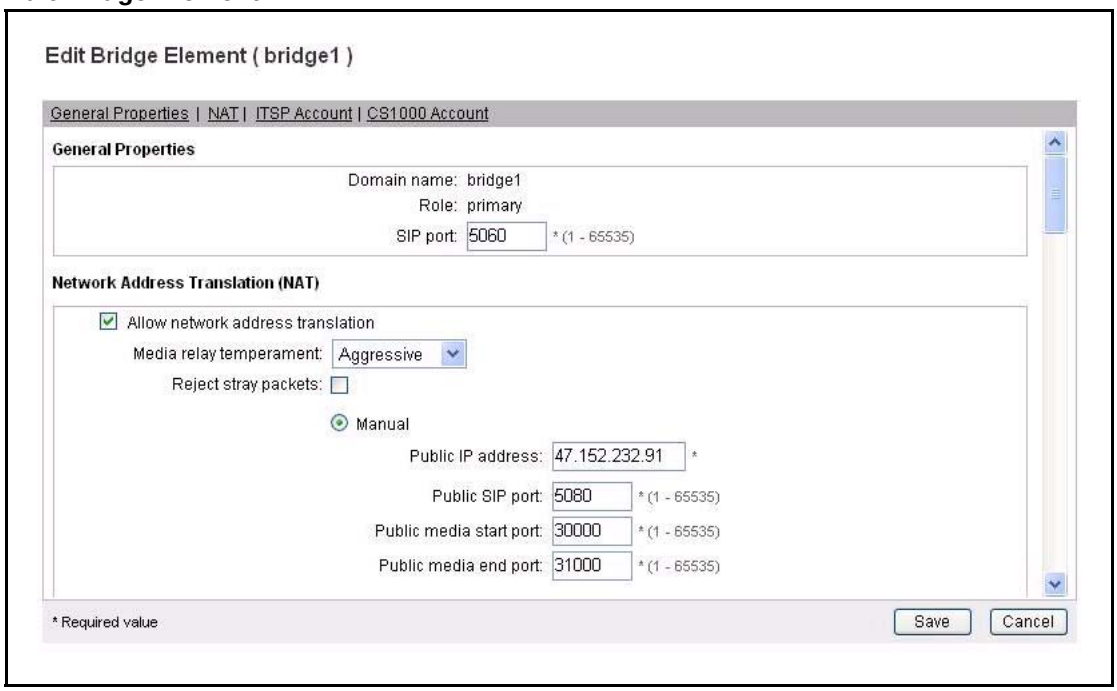
Figure 14
Bridge Element Home page



Configuring SIP Trunk Bridge Elements

You can configure the Bridge parameters in the Figure 15 "Edit Bridge Element" (page 41) web page. To launch this web page click on the Bridge Element in Figure 14 "Bridge Element Home page" (page 41).

Figure 15
Edit Bridge Element



This web page has the following four sections:

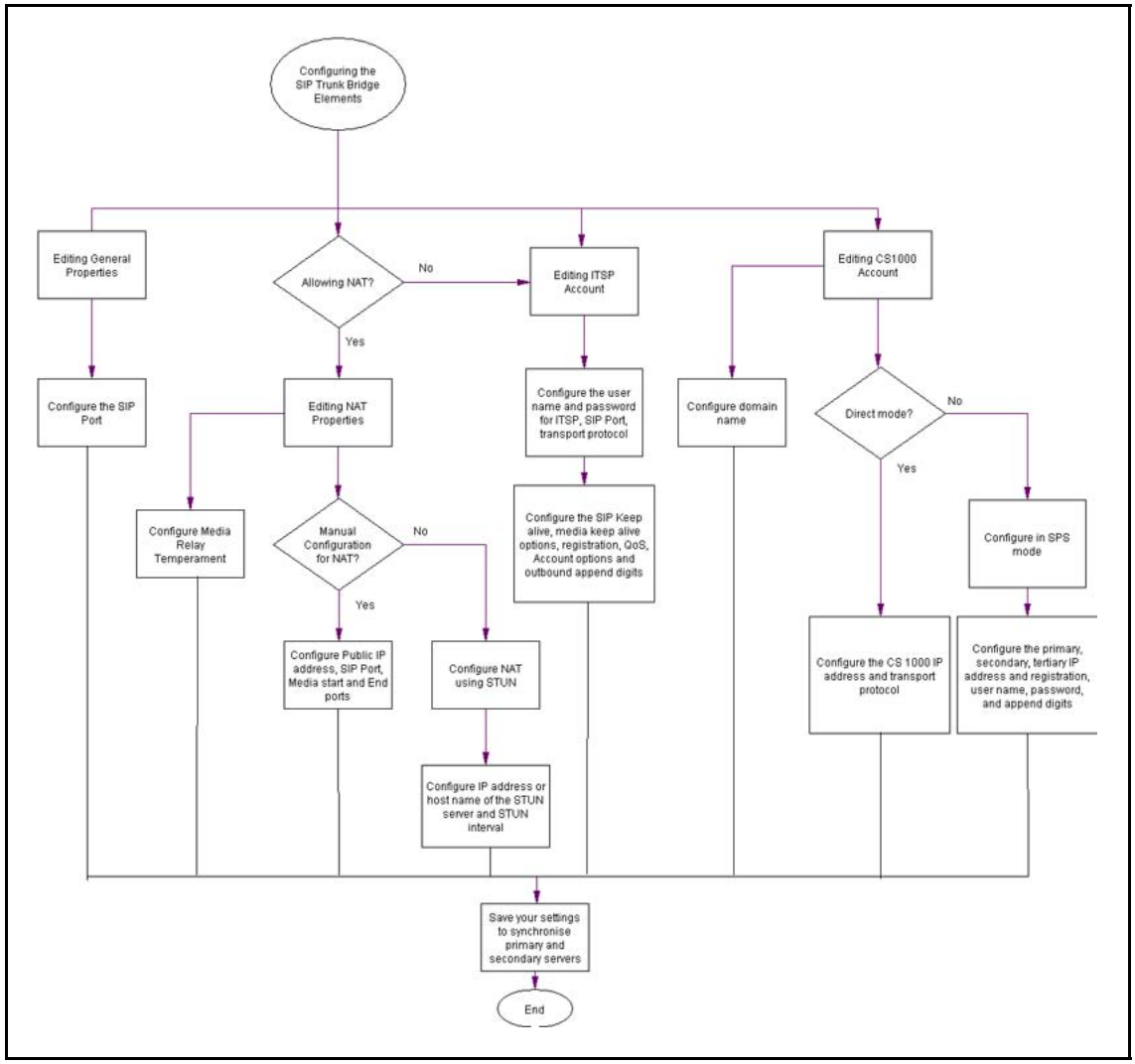
- “General properties” (page 43)
- “NAT” (page 44)
- “ITSP Account” (page 46)
- “CS1000 Account” (page 50)

ATTENTION
A user, logged in with network administrator privilege can configure the Bridge parameters in the primary server. However, these parameters can only be viewed in secondary server and all fields will be greyed out.

Bridge Configuration task flow

This section provides a high-level task flow for the configuration of SIP Trunk Bridge using Bridge Manager. The task flow indicates the recommended sequence of events to follow when configuring a system.

Figure 16
Configuring the SIP Trunk Bridge Elements



General properties

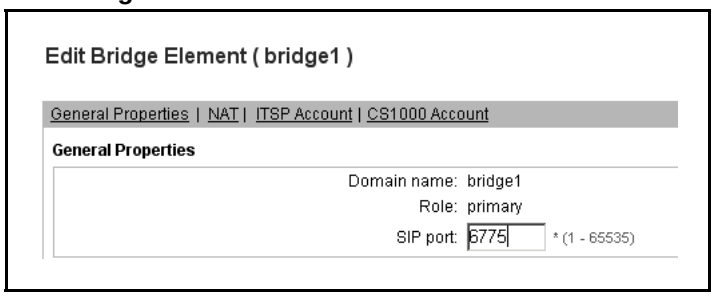
Follow these steps to configure General Properties.

Procedure 2
Editing General Properties

Step	Action
1	Under General Properties section in Figure 17 "Edit Bridge Element - General" (page 44), enter the **SIP port**. Use a numerical value in the range 1 to 65535. This is a mandatory field. SIP Trunk Bridge receives SIP messages from Communication

Server or SPS on this port. This should be same as the one in the CS 1000 system.

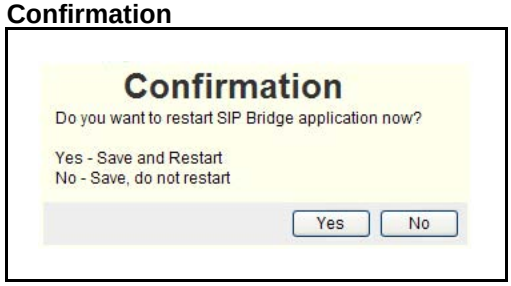
Figure 17
Edit Bridge Element - General



2 Click **Save**.

3 When you click **Save**, a **Confirmation** dialog appears as shown in Figure 18 "Confirmation" (page 44). Click **Yes**, if you want to restart the SIP Trunk Bridge application.

Figure 18
Confirmation



--End--

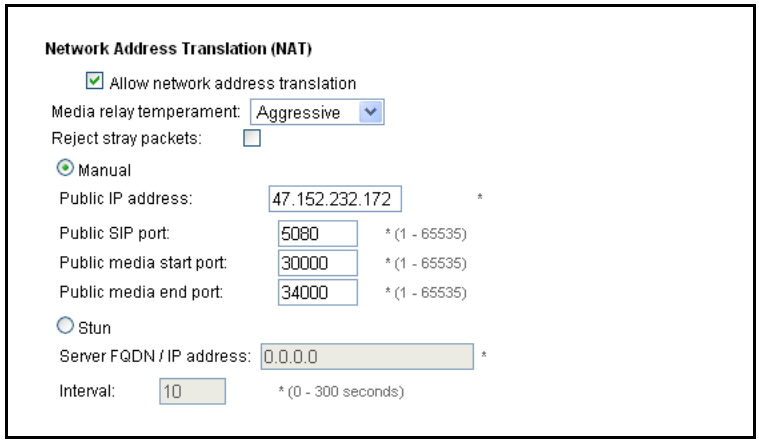
NAT

Follow these steps to configure the NAT properties.

Procedure 3
Editing NAT properties

Step	Action
1	Click **NAT** in **Edit Bridge Element** page. The Figure 19 "Edit Bridge Element - NAT" (page 45) page appears.

Figure 19
Edit Bridge Element - NAT



2 Select the **Allow network address translation** check box to enable NAT configuration.

When the check box is enabled, you can edit NAT properties.

3 Select the **Media relay temperament** from the drop-down list. The options are **Aggressive** and **Conservative**.

In **Aggressive** option, the NAT traversal feature insists on using a media relay between two endpoints that appear to be behind the same NAT. In **Conservative** option, the NAT traversal feature will be conservative in its use of media relays and refrain from using one between two endpoints that appear to be behind the same NAT.

ATTENTION
Release 7.0 supports only Aggressive option. Conservative option is not supported in this release.

4 Select the **Reject stray packets** option to determine whether or not media relay should reject the stray packets. RTP packets received by the bridge on the port allocated for the call (not from far end) are discarded or forwarded to the peer far end.

5 Select the **Manual** option if you want to configure in manual mode. When you select this option, you need to enter the following data:

ATTENTION
Only IPv4 format is supported in Release 7.0 and IPv6 format is not supported. Therefore, you must enter the addresses in the IPv4 format only.

- Public IP address
- Public SIP port in the range 1 - 65535
  SIP Trunk Bridge receives SIP messages from ITSP on this port.

Note 1: This port is used irrespective of the NAT configuration.

Note 2: If you want to change this port when NAT is not being used, you need to do the following:

a. ***Select the Allow network address translation check box.***

b. ***Modify the Public SIP port.***

c. ***Click Save.***

d. ***Clear the Allow network address translation check box***

e. ***Click Save again.***

- Public media start and end ports in the range 1 - 65535

  For each media session four ports are required. For example, if there are 100 parallel sessions, the range should be 4000 (30000 to 34000).

6 Select the **Stun** option if you want to configure in stun mode. In Simple Traversal UDP in NAT (STUN) mode, the server allows the NAT clients to setup the phone calls to a VOIP provider outside the local network. When you select this option, you need to enter the following data:

- Server FQDN or IP Address in IPv4 format.

  ATTENTION
  Spaces are not allowed.

- Interval in the range 0 to 300 seconds.

7 Click **Save**.

8 When you click **Save**, a **Confirmation** dialog appears as shown in Figure 18 "Confirmation" (page 44). Click **Yes**, if you want to restart the SIP Trunk Bridge application.

--End--

ITSP Account

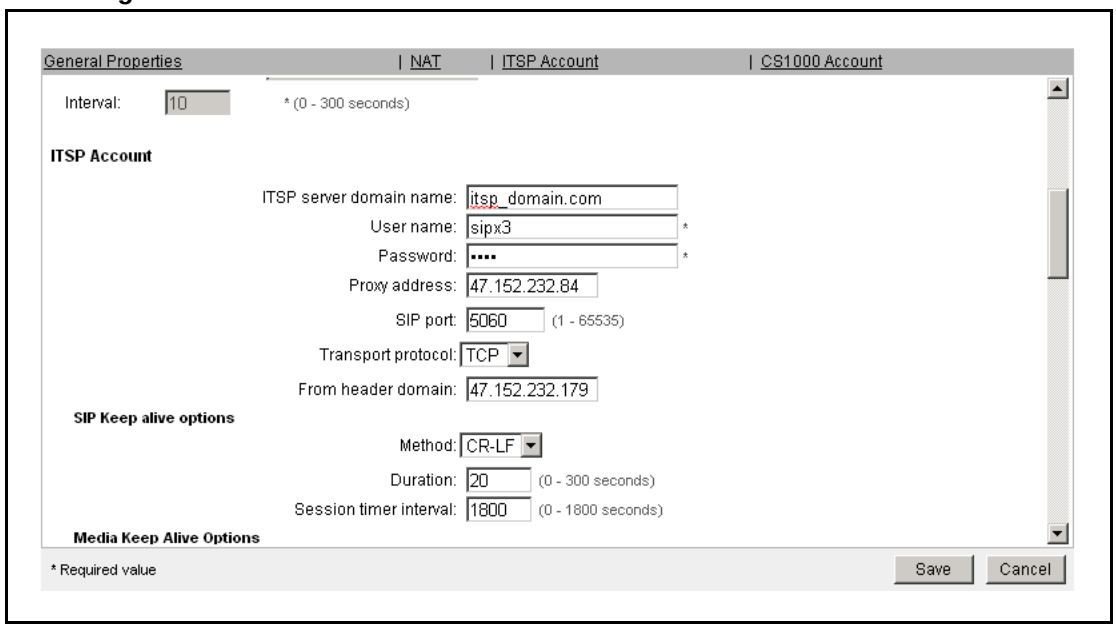
Follow these steps to configure the ITSP Account.

Procedure 4
Editing ITSP Account

Step	Action
1	Click **ITSP** in **Edit Bridge Element** page.

The Figure 20 "Edit Bridge Element - ITSP Account" (page 47) page appears.

Figure 20
Edit Bridge Element - ITSP Account



2 Enter the ITSP server domain name.

Specify the SIP domain name coming from the ITSP.

3 Enter the **User name** for the ITSP.

You can enter a maximum of 64 characters. Special characters like #,%,<,>,' are not allowed. This is a mandatory field.

4 Enter the Password for the ITSP user name.

You can enter a maximum of 64 characters. Special characters like #,%,<,>,' are not allowed. This is a mandatory field.

5 Enter the **SIP port** in the range 1 - 65535.

This is the SIP listening port of the ITSP. This port can be same or different than the public SIP port in NAT section.

6 Select the **Transport protocol** from the drop-down list.

TCP and UDP are the options available.

7 Enter the **From header domain** in IPv4 format.

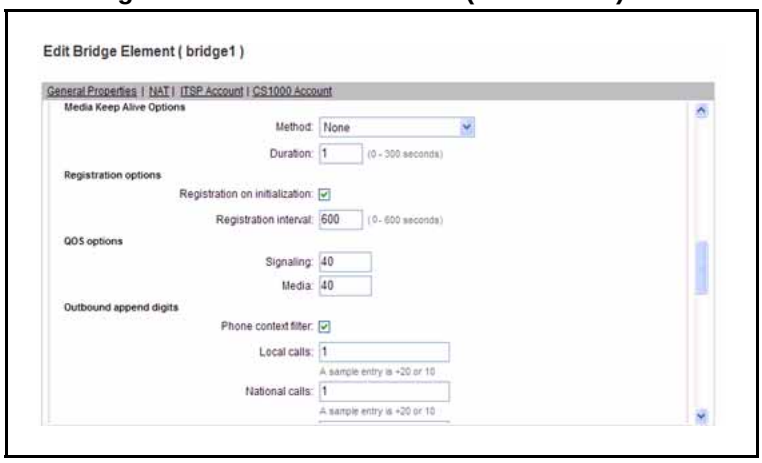
The From header sent to the Communication Server 1000 is will change to SIP:<DN>@<IP address>.

Where DN is the directory number and IP address is the From Header Domain in IPv4 format.

8 Under **SIP Keep alive options** enter the following:

- Method - CR-LF or None- Defines the mechanism to use for SIP keepalive. Sends empty SIP messages if CR-LF method is used for keep alive mechanism. If None is selected, then there will be no keep alive mechanism.
- Duration - 0 to 300 seconds
- Session time - interval in the range 0 to 1800 seconds.

Figure 21
Edit Bridge Element - ITSP Account (continued1)



9 Under **Media Keep Alive Options** enter the following:

- Method -None, Use empty packet, Relay last sent packet, User dummy RTP payload
- Duration - 0 to 300 seconds

10 Under the **Registration options**, enter the following:

- Select **Registration on initialization** option if you want to register the Bridge as a dynamic endpoint with ITSP.
- Enter the **Registration interval** in the range 0 to 600 seconds.

11 Under **QOS** options, enter the **Signaling** and **Media** options.

ATTENTION
This option is not supported for Release 7.0. Therefore, a place holder is placed for future releases.

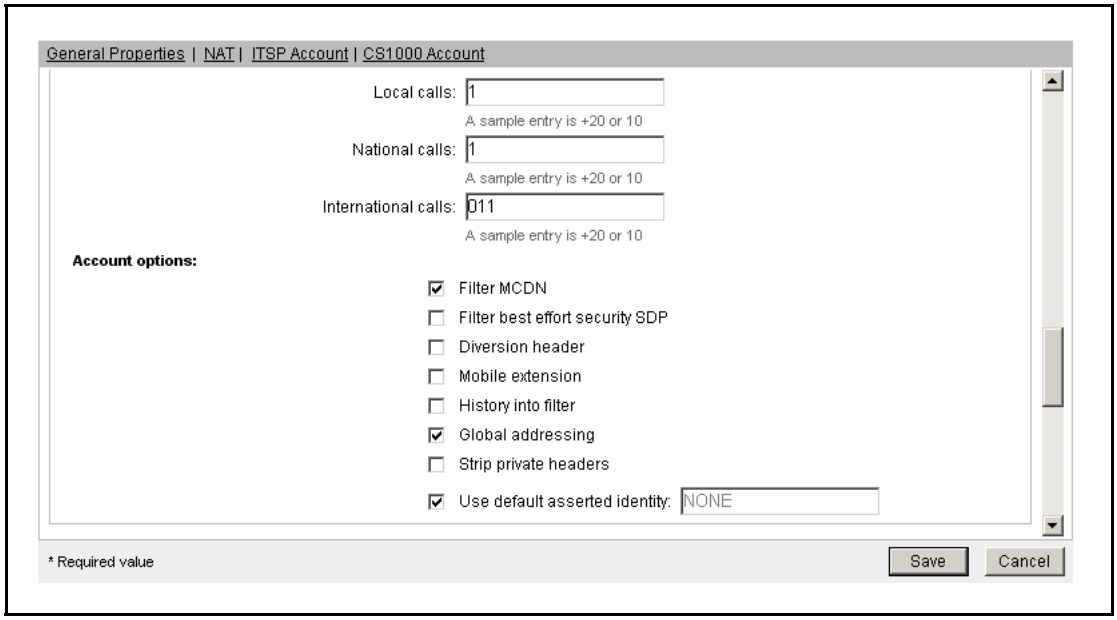
12 Under **Outbound append digits** options, enter the following:

- Select the **Phone Context Filter** option if you want to remove the phone context parameter received from CS 1000 before sending it to ITSP in the URI of SIP INVITE message.

This filters the phone context received from Communication Server 1000 while sending to ITSP.

- Enter the prefix digits for **local**, **national**, or **international** calls in the format X or +X, where X is a numerical value upto ten digits.

Figure 22
Edit Bridge Element - ITSP Account (continued2)



13 Select the required **Account options**.

Following are the ITSP account options:

- Filter MCDN - If you select this option, MIME content received from CS 1000 is removed before sending to ITSP.
- Filter best effort security SDP - If you select this option, when a user receives an offer from CS 1000 with best effort security, the user filters the security part and sends a regular SDP to ISTP side.

  ATTENTION
  This option is not supported for Release 7.0. Therefore, a place holder is placed for future releases.

- Diversion header - If you select this option, diversion header is added to the hair pinned call to ITSP.
- Mobile extension - Select this option if you want to enable MobileX feature on SIP Trunk Bridge. Media is relayed through bridge. Mid call RFC2833 digits are collected and sends SIP INFO message with collected digits.

ATTENTION
This option is only applicable in LAN deployment with NAT models.

- History info filter – This option is used if you want to filter the captured information occurred during a particular call. For stripping this field, use strip private header feature and for using it to generate diversion header, use diversion feature.

ATTENTION
This option is not supported for Release 7.0. Therefore, a place holder is placed for future releases.

- Global addressing - This option is used along with NAT configurations. When you select this option, the NAT Public IP is used for SIP Signaling and media (SDP). Else the virtual IP is used
- Strip private headers- When you select this option, it strips sensitive headers such as Subject, Call-Info, Organization, User-Agent, Reply-To, and In-Reply-To. Display Name is stripped where ever it appears.
- Use default asserted identity- When you select this option, the default asserted identity is used. That is, INVITE to ITSP will have PAI (p-asserted identity) as "P-Asserted-Identity: <sip: user@itsp_domain.com>". Otherwise, you need to enter a username@domain to override the default. That is, the INVITE to ITSP will have P-Asserted-Identity: "<sip: test@mydomain.com>"

14 Click **Save**.

15 When you click **Save**, a **Confirmation** dialog appears as shown in Figure 18 "Confirmation" (page 44). Click **Yes**, if you want to restart the SIP Trunk Bridge application.

--End--

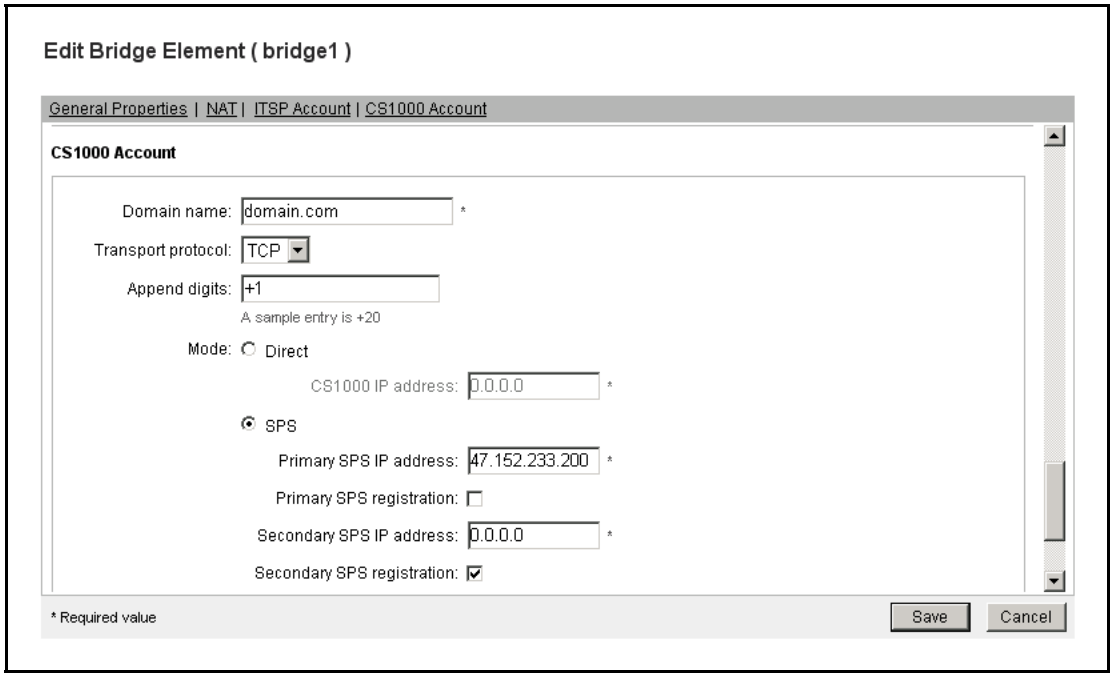
CS1000 Account

Follow these steps to configure the CS1000 Account.

Procedure 5
Editing CS1000 Account

Step	Action
1	Click **CS1000 Account** in **Edit Bridge Element** page. The Figure 23 "Edit Bridge Element - CS1000 Account" (page 51) page appears.

Figure 23
Edit Bridge Element - CS1000 Account



2 Enter the domain name. The domain name could be the domain of CS 1000 in direct mode or domain name of SPS in SPS mode.

Direct mode: This domain name matches with the name in **CS1000 IP Network -> Node -> Gateway SIPGw -> SIP domain name**.

SPS mode: This domain name matches with the name in **CS1000 Network Element -> SPS -> Service Domain**.

You can enter a maximum of 64 characters. Special characters like #,%,<> ,' are not allowed. This is a mandatory field.

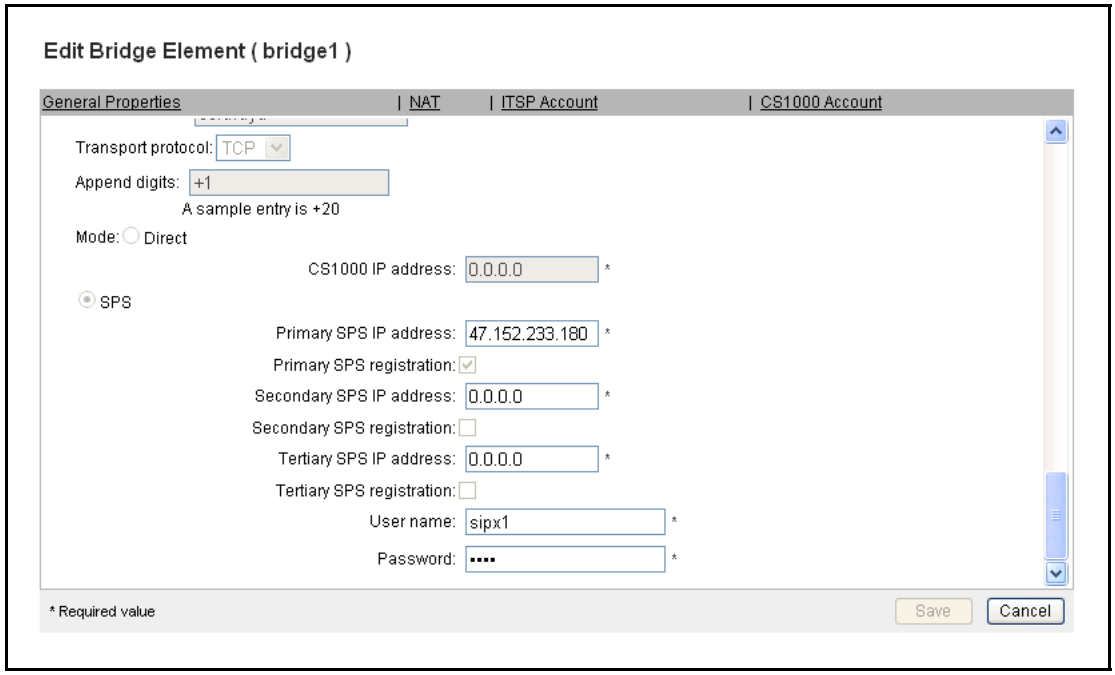
3 Select the TCP or UDP protocol.

The CS 1000 SPS and SIP Gateway must have the same transport protocol enabled.

4 Enter the digits to be prefixed to the inbound call from ITSP in the +X format.

5 If you are selecting the **Direct** mode, enter the CS 1000 signaling gateway node IP address.

Figure 24
Edit Bridge Element - CS1000 Account (continued)



6 If you are selecting the **SPS** deployment mode, you must configure the following.

- Enter the **Primary SPS IP address**.
- Select the **Primary SPS registration** option, if you want to register the Bridge as a dynamic endpoint with SPS.
- Enter the **Secondary SPS IP address**.
- Select the **Secondary SPS registration** option, if you want to register the Bridge as a dynamic endpoint with SPS.
- Enter the **Tertiary SPS IP address**.
- Select the **Tertiary SPS registration** option, if you want to register the Bridge as a dynamic endpoint with SPS.
- Enter the **User name**. The user name is used to register and authenticate with SPS. You can enter a maximum of 64 characters. Special characters like #,%,<,>,' are not allowed.

  Note: User name should match with the endpoint name in SPS.

- Enter the **Password**.

ATTENTION
Select the registration check boxes if you want to register the bridge.

7 Click **Save**.

8 When you click **Save**, a **Confirmation** dialog appears as shown in Figure 18 "Confirmation" (page 44). Click **Yes**, if you want to restart the SIP Trunk Bridge application.

--End--

Synchronization

The synchronization status column shows the synchronization status of the servers in the Bridge Elements page.

If the synchronization fails, you can manually synchronize it by clicking on **Synchronize** button in Bridge Elements page.

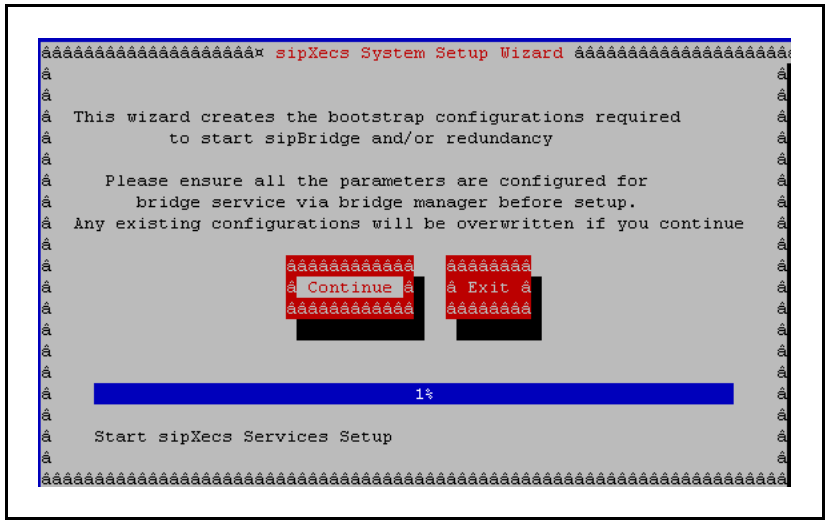
Running the sipxecs setup

Once you have configured the parameters in the General, NAT, ITSP, and CS1000 Account sections as shown in the preceding sections, you need to run the sipxecs-setup and start all the services as shown in the following procedure.

Procedure 6
Running sipxecs setup

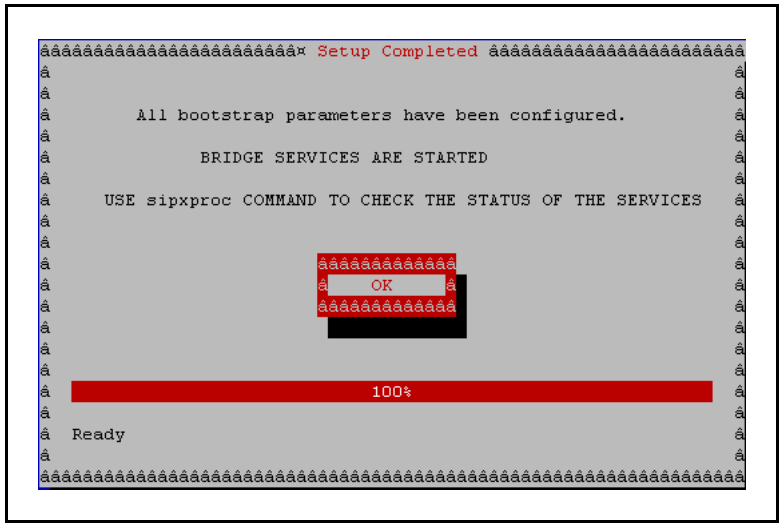
Step	Action

1 Log in to the server (ssh) as root user and run the sipxecs-setup.



2 Click **Continue** to proceed (if all the Bridge parameters are satisfied). If you want to change the Bridge parameters you need to exit from the set up. Press the **Exit** key to exit.

For information on configuring Bridge parameters, see “Configuring SIP Trunk Bridge Elements” (page 41).



3 Select **OK** and press the **Enter** key.

4 Run **`sipxproc`** command to know the status of the services.

The sample output of the status of the services is shown in "Process status command" (page 57).

Note: It takes a few moments for the services to come up.

--End--

If the 1+1 server is deployed, you will need to run the sipxecs setup on the secondary server also. Follow the procedure Procedure 6 "Running sipxecs setup" (page 53) to run the setup on secondary server.

Maintenance

This chapter describes maintenance for the SIP Trunk Bridge.

Impact of power cycle on SIP Trunk Bridge

After you power cycle the system, all applications are re-initialized, including SIP Trunk Bridge. All data stored in memory is lost.

Impact on a SIP Trunk Bridge call

Table 2 "Call impact" (page 55) describes call activity after the system is power cycled.

Table 2
Call impact

Call type	Description
Simple, active calls	• If the media is an end-to-end call, the speech path is maintained for the duration of the call. • If the media is through bridge (Media relay), speech path will be dropped. • New calls are processed after system is up.
Transient calls	Transient calls are calls that are in signaling set-up stage. Transient calls are dropped when the server restarts.
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.

Troubleshooting

The following commands are available for troubleshooting the SIP Trunk Bridge:

Process status command

Login as **root** and run the command **sipxproc**. This command shows the status of the processes.

Syntax: **sipxproc**

A Sample output of this command is as follows:

On Primary Bridge server

```
Redundancy Status

-----------------

Server:  PRIMARY VIP status:  UP so in PRIMARY mode

Process Status

-----------------

{"SipXbridge"=>"Running", "SipXrelay"=>"Running"}
```

On Secondary Bridge server

```
Redundancy Status

-----------------

Server:  SECONDARY VIP status:  DOWN so in SECONDARY mode

Process Status

-----------------

All process in standby
```

SIP Trunk services - start, stop, check status, and restart command

To start, stop, check status, or restart the SIP Trunk Bridge services, login as **root** and run the command **/sbin/service sipxecs {start|stop|status|restart}**.

Sample outputs of these services are shown in the following sections.

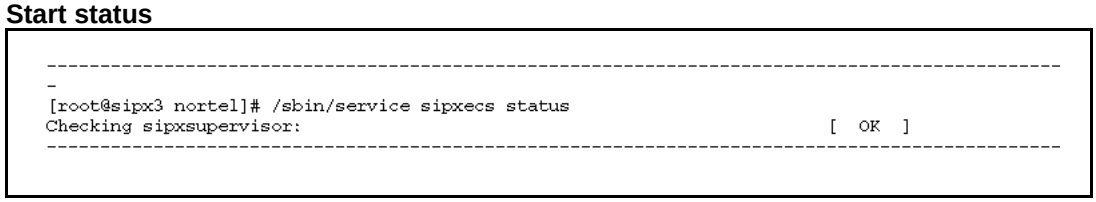
Sample output for start

A sample output of the start service and its status is as shown in Figure 25 "Start service" (page 58) and Figure 26 "Start status" (page 59) respectively.

Figure 25
Start service

```
-------------------------------------------------------------------------------------------
[root@sipx3 nortel]# /sbin/service sipxecs start
Checking bootstrap setup:                                  [  OK  ]
Checking TLS/SSL configuration:                            [  OK  ]
Checking Per-process file descriptor limits:               [  OK  ]
Checking rpm configuration file updates:                   [  OK  ]
Checking SELinux is not enforcing:                         [  OK  ]
Checking hostname is fully qualified:                      [  OK  ]
Checking localhost address configured:                     [  OK  ]
Checking localhost name is not shared:                     [FAILED]
Checking /tmp directory has correct permissions:           [  OK  ]
sipXpbx:
sipXpbx: sipXpbx configuration problems found:
sipXpbx:
sipXpbx: Check localhost name is not shared
sipXpbx: The 127.0.0.1 address should map to only the names
sipXpbx:'localhost.localdomain' and 'localhost'.
sipXpbx:
sipXpbx: Any other name for that address may cause routing or authentication errors.
sipXpbx:
sipXpbx: Remove the following names from the 127.0.0.1 line in /etc/hosts:
sipXpbx:
sipXpbx: secondaryDNSIP
sipXpbx: tertiaryDNSIP
sipXpbx: primaryDNSIP
sipXpbx:
Starting sipXpbx:
                                                                          [  OK  ]
                                                                          [  OK  ]
Starting sipxsupervisor:                                                  [  OK  ]
-------------------------------------------------------------------------------------------
```

Figure 26
Start status



Sample output for stop

A sample output of the stop service and its status is as shown in Figure 27 "Stop service" (page 59) and Figure 28 "Stop status" (page 59) respectively.

Figure 27
Stop service

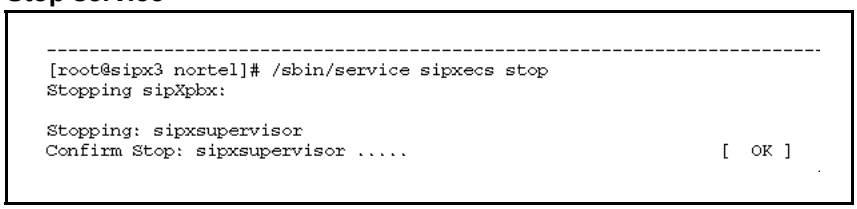
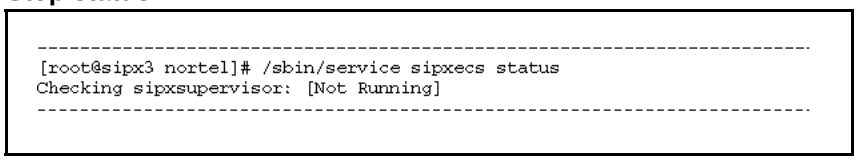


Figure 28
Stop status



Sample output for restart

A sample output of the restart service and its status is as shown in Figure 29 "Restart" (page 60) and Figure 30 "Restart status" (page 60) respectively.

Figure 29
Restart

```
--------------------------------------------------------------------------------
[root@sipx3 nortel]# /sbin/service sipxecs restart
Stopping sipXpbx:

Stopping: sipxsupervisor
Confirm Stop: sipxsupervisor .....                         [  OK  ]
Checking bootstrap setup:                                  [  OK  ]
Checking TLS/SSL configuration:                            [  OK  ]
Checking Per-process file descriptor limits:               [  OK  ]
Checking rpm configuration file updates:                   [  OK  ]
Checking SELinux is not enforcing:                         [  OK  ]
Checking hostname is fully qualified:                      [  OK  ]
Checking localhost address configured:                     [  OK  ]
Checking localhost name is not shared:                     [FAILED]
Checking /tmp directory has correct permissions:           [  OK  ]
sipXpbx:
sipXpbx: sipXpbx configuration problems found:
sipXpbx:
sipXpbx: Check localhost name is not shared
sipXpbx: The 127.0.0.1 address should map to only the names
sipXpbx:'localhost.localdomain' and 'localhost'.
sipXpbx:
sipXpbx: Any other name for that address may cause routing or authentication errors.
sipXpbx:
sipXpbx: Remove the following names from the 127.0.0.1 line in /etc/hosts:
sipXpbx:
sipXpbx: secondaryDNSIP
sipXpbx: tertiaryDNSIP
sipXpbx: primaryDNSIP
sipXpbx:
Starting sipXpbx:                                                    [  OK  ]
                                                                     [  OK  ]
Starting sipxsupervisor:                                             [  OK  ]
--------------------------------------------------------------------------------
```

Figure 30
Restart status

```
--------------------------------------------------------------------------------
[root@sipx3 nortel]# /sbin/service sipxecs status
Checking sipxsupervisor:                                             [  OK  ]
```

Log settings commands

Run the following commands as root user for setting the log levels of SIP Trunk Bridge for debugging purpose.

- “Set-bridge-log-level [option]” (page 60)
- “Set-relay-log-level [option]” (page 61)

Set-bridge-log-level [option]

This command sets the log level for the bridge component.

Syntax: **`set-bridge-log-level [option]`**

`option` can be one of the following:

- `0:OFF`
- `1:DEBUG`

- `2:INFO`
- `3:WARNING`
- `4:ERROR`
- `5:TRACE`

For example, to enable INFO logs, run the command `set-bridge-log-level 2`

Set-relay-log-level [option]

This command sets the log level for the relay component.

Syntax: **`set-relay-log-level[option]`**

`option` can be one of the following:

- `0 : OFF`
- `1 : DEBUG`
- `2 : INFO`
- `3: WARNING`
- `4: ERROR`
- `5 : TRACE`

For example, to enable INFO logs run the command `set-relay-log-level 2`

Finding log files

Go to the directory **/var/log/sipxpbx/** to find the log files.

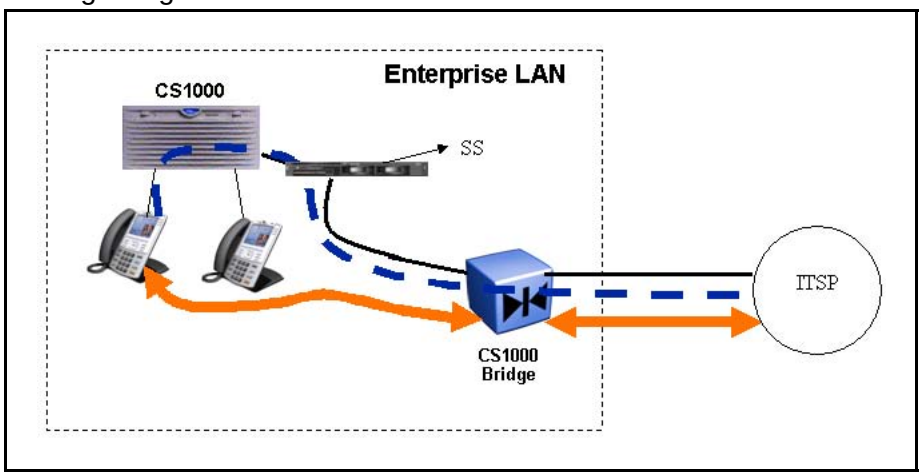
Appendix
Connecting Bridge to the LAN

Following are the ways in which you can connect Bridge to the LAN:

- Connecting the Bridge directly to the Signaling Server of CS 1000)
- Connecting Bridge to SPS (SIP Proxy Server) or NRS (Network Routing Server)

Connecting the Bridge directly to the Signaling Server

Consider the following scenario in which the Bridge is directly connected to the Signaling Server.



In this case, consider the following IP addresses for the signaling server:

- Node IP : 47.152.233.167
- TLAN IP : 47.152.233.166
- ELAN IP : 47.152.232.196

In this case, consider the following IP addresses for the Bridge:

- Virtual IP : 47.152.232.88
- TLAN IP : 47.152.232.201
- Public IP address configured in Bridge : 47.152.232.96

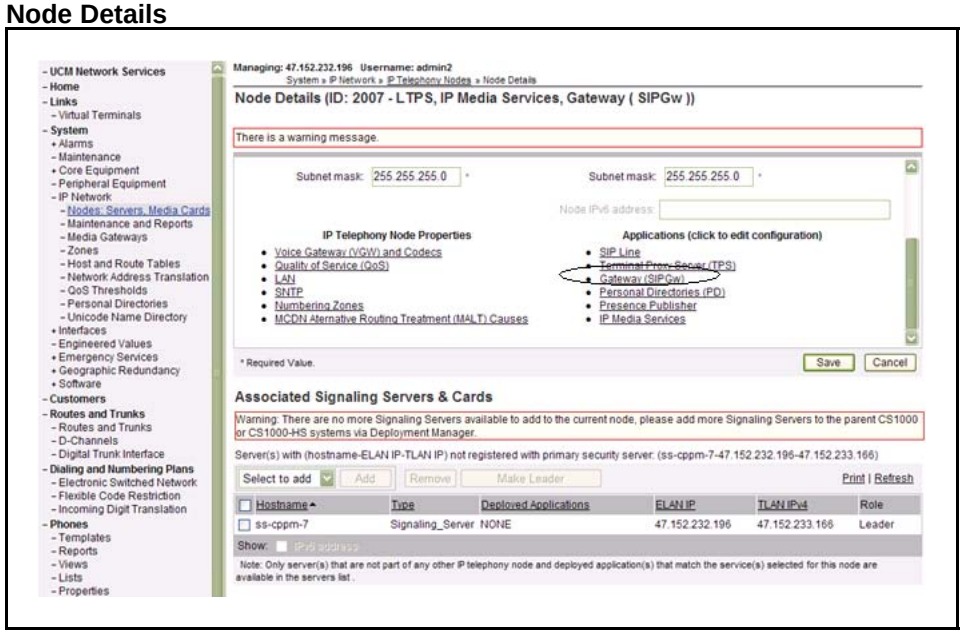
You are required to do the configurations both on the Signaling Server side as well as on the Bridge side. These configurations are explained in the following sections:

Signaling Server side configurations

If you are connecting Bridge directly to the signaling server, you have to configure the Bridge IP address in Virtual Trunk Gateway details page. Follow these steps for Signaling Server side configurations:

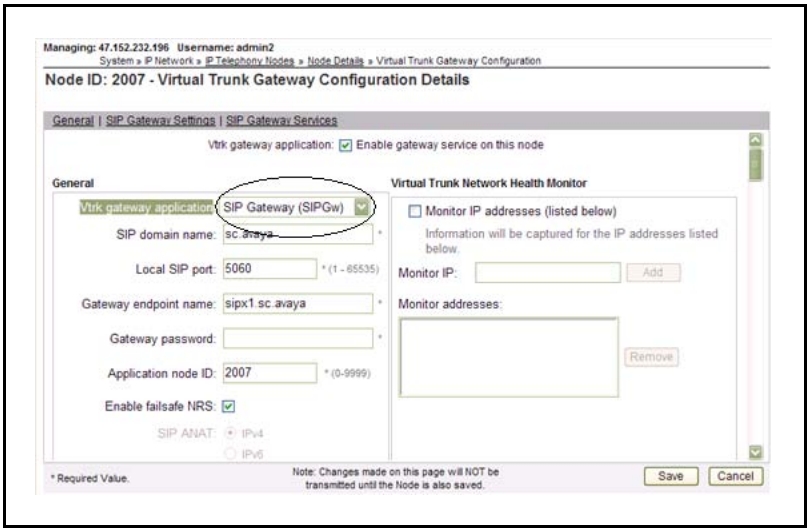
Step	Action
1	Login to the Signaling Server Element Manager.
2	Click on the **Nodes: Servers, Media Cards** under the **IP Network** in the navigation tree. **Node Details** page appears.

Figure 31
Node Details



3	Click on the link **Gateway(SIPGw)** . **Virtual Trunk Gateway Configuration Details** page appears.

Figure 32
Virtual Trunk Gateway Configuration Details - General



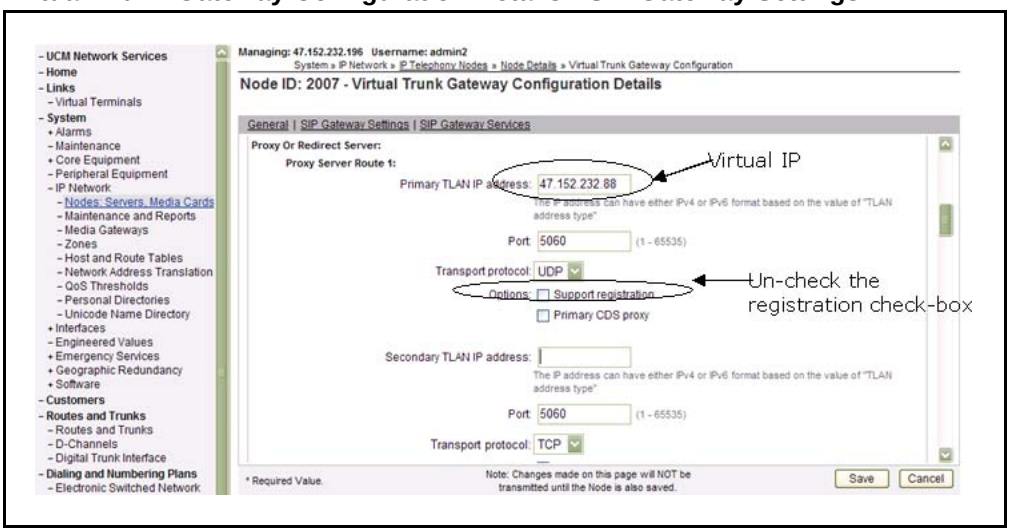
4 Under General section, configure the SIP Gateway.

ATTENTION
Disable to TLS security, as it is not supported in this release.

5 Click on the **SIP Gateway Settings** link.

SIP Gateway Settings page appears.

Figure 33
Virtual Trunk Gateway Configuration Details - SIP Gateway Settings



6 Enter the Primary TLAN IP address. Specify the Virtual IP address of the SIP Trunk Bridge in this field.

7 Select the transport protocol as UDP and give the port number 5060 for SIP signaling in this case.

8 Clear the check box **Support registration** as CS 1000 does not accept the registration.

9 Click **Save** and exit.

--End--

Bridge side configurations

Follow these steps for Bridge side configurations:

Step	Action

1 Login to the Bridge Manager.

Edit Bridge Element page appears.

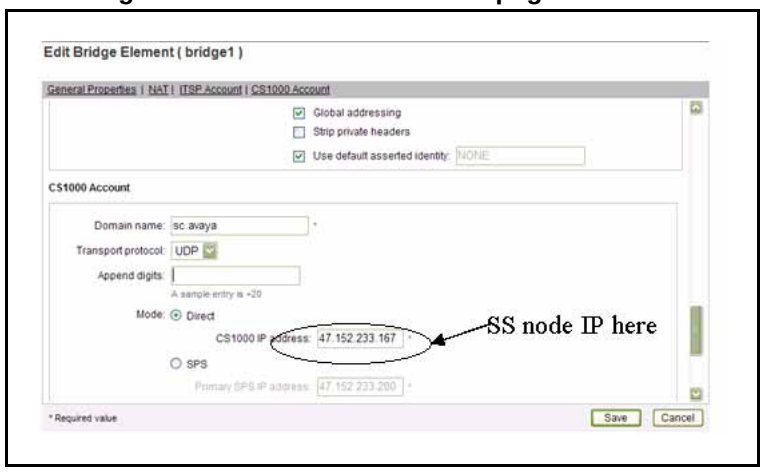
Figure 34
General Properties page

2 Under General section, enter the port number for SIP signaling with the LAN side.

This should be same as the one configured in Signaling Server, 5060 in this case.

3 Under CS1000 Account section, select **Direct** mode and enter the CS1000 signaling server node IP address.

Figure 35
Edit Bridge Element- CS1000 Account page



4 Select the transport protocol.

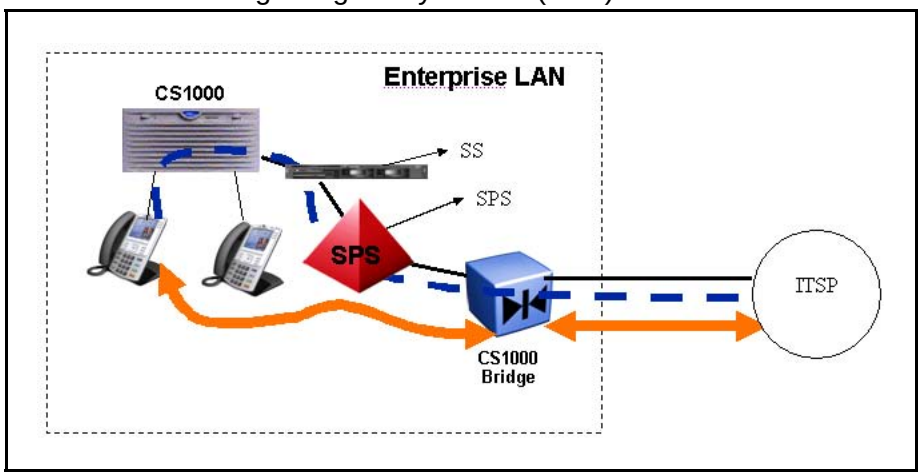
This should be same as the one selected for Signaling Server side, UDP in this case.

5 Click **Save** and exit.

--End--

Connecting Bridge to Signaling Proxy Server or Network Routing Server

Consider the following scenario in which the Bridge is connected to the Signaling Proxy Server (SPS).



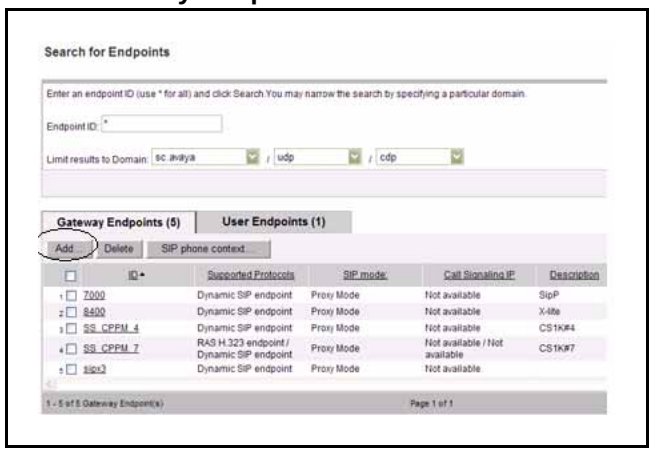
In this case, consider the SPS IP address (TLAN) as 47.152.233.180.

SPS side configuration

Follow these steps to connect the Bridge to the SPS:

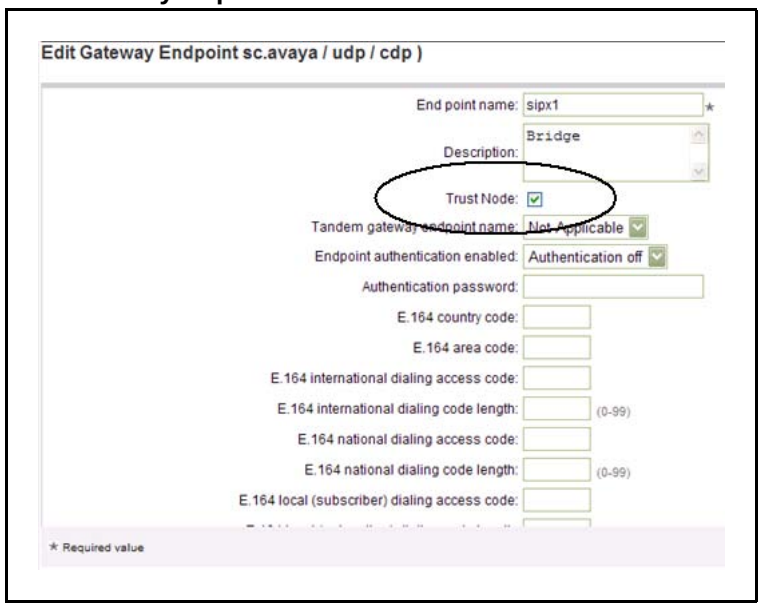
Step	Action
1	After the Domain is configured (sc.avaya in this case), you need to add a Gateway endpoint under that domain.

Figure 36
Add - Gateway Endpoint



2 Click **Add**.

Figure 37
Edit Gateway Enpoint

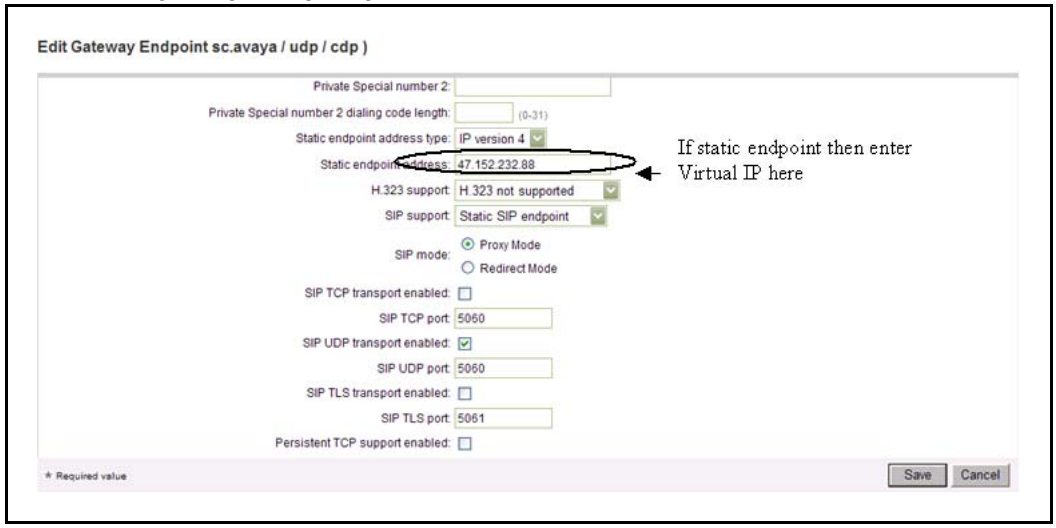


3 Enter the end point name and make it as trust node by checking the option **Trust Node**.

4 Select either Authentication on or Authentication off option in **Endpoint Authentication enabled** drop-down list.

Bridge supports both ’on’ and ’off’ options.

Figure 38
Edit Gateway endpoint (cont)



5 Enter the Virtual IP address of the Bridge in **Static endpoint address** if the SIP support field is configured as Static SIP Endpoint.

In the SIP Support field, you can configure Bridge as a Static SIP Endpoint or a Dynamic End point.

6 Select proxy mode as SIP mode.

7 Select the transport protocol and enter the port number for SIP signaling.

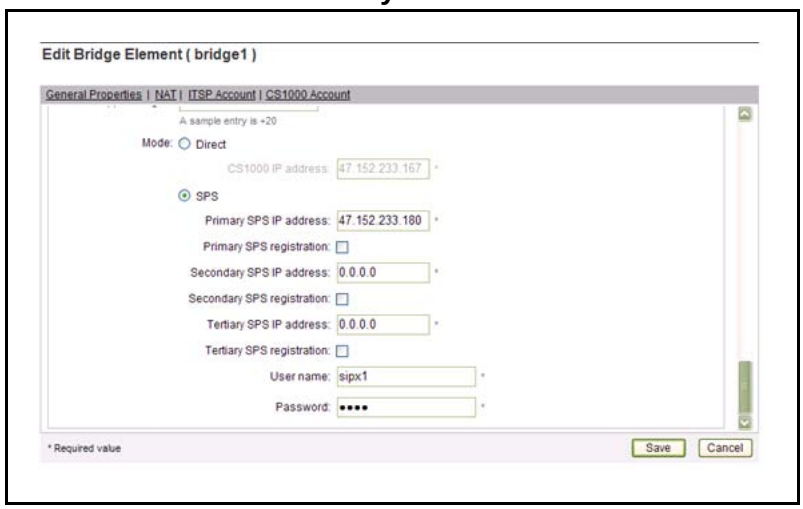
8 Click **Save** and exit.

--End--

Bridge side configuration

Follow these steps for Bridge side configurations:

Step	Action
1	Login to the Bridge Manager.
2	Under General section, enter the port number for SIP signaling with the LAN side.
3	Select the transport protocol which should be same as the one configured in SPS. UDP in this case.
4	Under CS1000 Account section, select SPS mode and enter the IP address of SPS in **Primary SPS IP address** field.



5 If you have configured the Bridge as a Static Endpoint, do not check the **Primary SPS registration** check box and similarly if it is configured as a Dynamic endpoint in SPS, then select this registration check box.

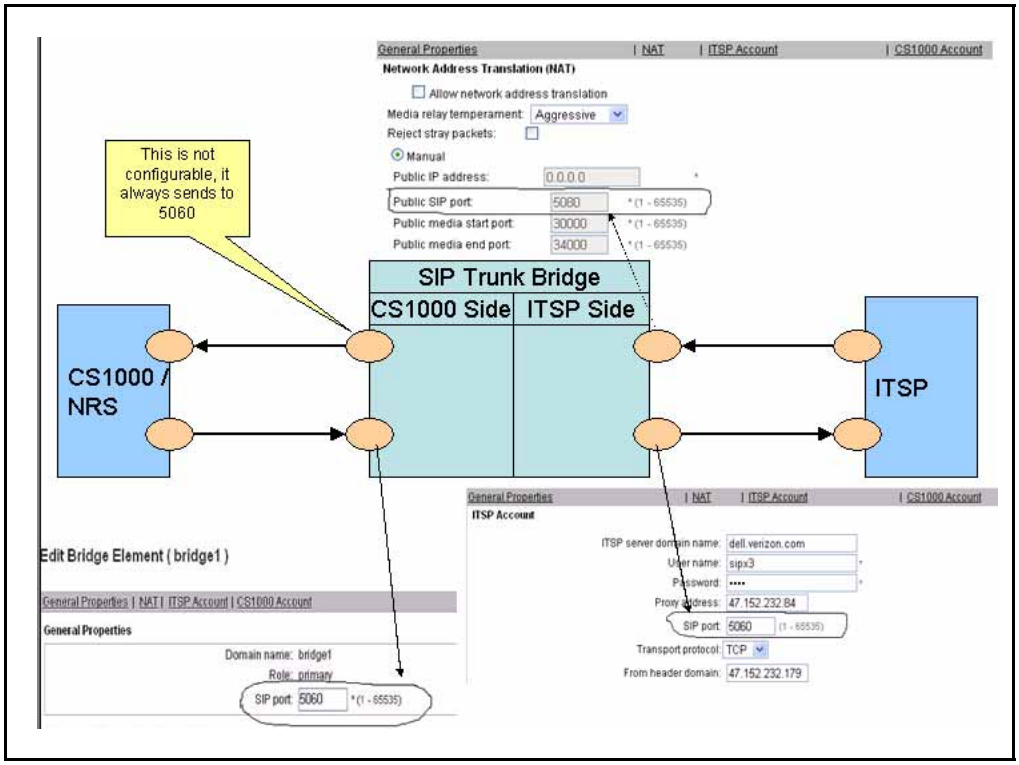
6 If there are redundant SPS servers, then configure the Secondary and Tertiary SPS IP addresses and check the respective registration check boxes appropriately.

7 Click **Save** and exit.

--End--

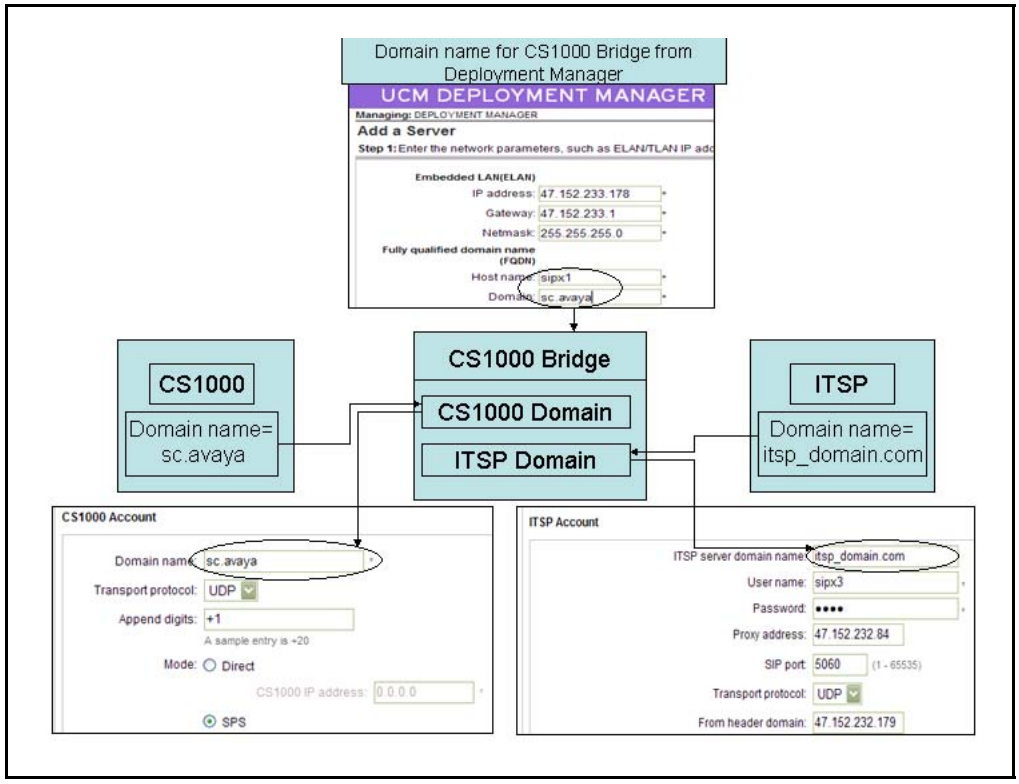
Appendix
SIP port configuration on Bridge

The following figure shows the SIP port configurations of NAT, General properties, and ITSP Account sections:



Appendix
SIP domain configuration on Bridge

The following figure shows the SIP domain configurations for CS1000 properties and ITSP Account sections:



Nortel Communication Server 1000

SIP Trunk Bridge Fundamentals

Release: 7.0
Publication: NN43001-143
Document revision: 01.02
Document release date: 15 June 2010