Carrier VoIP

Session Server Trunks Configuration Management

NN10338-511

Document status: Standard
Document version: 04.03
Document date: 20 October 2006

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

Contents

New in this Release

The following sections detail what's new in *Session Server Trunks Configuration Management* for (I)SN09U.

- Features
- "Other changes" (page 6)

Features

Session Server Trunks (SST) introduces the following new features in configuration management for this release.

Support for SIP DID Trunks on Session Server (A00011533)

This feature provides Carrier Voice over IP networks with additional IETF compliance and interoperability with the session initiation protocol (SIP) and SIP for telephones (SIP-T) standards. The enhancements improve interworking between CS 2000 switches and with other third-party SIP servers.

Support for SIP direct inward dialing (DID) trunk types on SST provides the following improvements:

- Preserves existing SIP-T functionality provided by virtual router distribution node (VRDN) in CS 2000
- Provides enhanced ANSI ISUP parameter mapping to SIP to support SIP interfacing to remote CS 2000 and third party SIP servers.
- Supports the mobile telephone exchange (MTX) DID trunk type on the Session Server
- The Session Timer extension (RFC4028) enables SIP servers and endpoints to know if an endpoint is no longer in a session, such as in case of a crash, and to limit the duration of a session. An endpoint that has the Session Timer extension activated sends periodic keep-alive messages to notify that it is active or to extend the duration of the session.

  SIP protocol RFC 4028 Session Timers defines two new headers—Session-Expires and Min-SE and a new response code of 422. The Session-Expires header conveys the lifetime of the session,

the Min-SE header conveys the minimum value for the Session Timer, and the 422 response code indicates that the Session Timer duration is too small. The Session-Expires/session timer range you can provision using the SST GUI is between 5-30 minutes.

For more information, refer to "Configuring Remote SIP Servers" (page 26).

SST - Mapping of prefix digits to an incoming DPT trunk group

This feature allows the CS2K-SST to process SIP to TDM calls with multiple trunk groups on the core from signaling on a single SIPLink. This functionality allows the SST application to interpret the leading digits (digits prefixed on the called DN) and, based on these digits, select an incoming DPT trunk group in the CS 2000. These digits are mapped to a SIPLink in the SST, and therefore a trunk group in the CS 2000, in the same manner as the mapping of a x-nortel-profile header.

Other changes

The "MCS interoperability" (page 21) section has been revised.

CAUTION

When SST CPU utilization exceeds 80 per cent (over 800,000 busy hour call attempts), entering the GUI may impact call processing. To check CPU utilization from the command line, enter the following:

```
mtccli qrycputl
```

If you are already in the GUI, CPU utilization displays as a percentage in the System Status pages. From the Platform Manager, click System Status.

The "Configuring SIP Gateway application parameters" (page 46) section has been updated to include the following configurable parameters; numAuditMsgsPerCycle and auditTimeInterval.

Configuration management strategy

This document provides Session Server Trunks (SST) configuration management procedures including for CS 2000 networks. The document does not provide installation and commissioning of the SST platform or its applications. For initial network installation of an SST, consult the appropriate Installation Methods document (IM) available from Nortel.

General configuration limitations and restrictions

Neither of the two graphical user interfaces (GUIs), CS 2000 Session Server Manager or the CS 2000 NCGL Platform Manager, support being accessed over a connection made with network address translation. Only SPFS web proxied connections are supported. For more information about these configuration limitations, consult your site network engineering guidelines and site network administrator.

When changing mapping tables using either GUI, allow the operation to complete before performing other actions.

Tools and utilities

Reprovisioning or changing of the SST existing settings is performed using a number of interfaces depending on the activity required. The interface needed is called out at the beginning of the applicable procedure. The following interfaces are used in accomplishing the tasks.

- CS 2000 Session Server Manager, a client web browser application
- CS 2000 NCGL Platform Manager, a client web browser application
- NCGL command line interface (CLI)

Client web browser requirements

For provisioning and maintaining the SST the following client web browsers are supported.

Supported web clients on a Windows 2000, XP, or 2003-based PC:

- Internet Explorer 6.0 SP1 and above
- Netscape 6.2.3+ and 7.1+

Supported web clients on a Solaris 2.8 and 2.9-based Sun workstation:

- Netscape 6.2.3
- Mozilla 1.4+

The following browsers are NOT supported by Session Server:

- Any browser running on a Linux operating system
- Any browser running an OS under VMware
- Any browser running under Solaris operating system on a PC
- Any browser running on Macintosh hardware

Accessing SST user interfaces

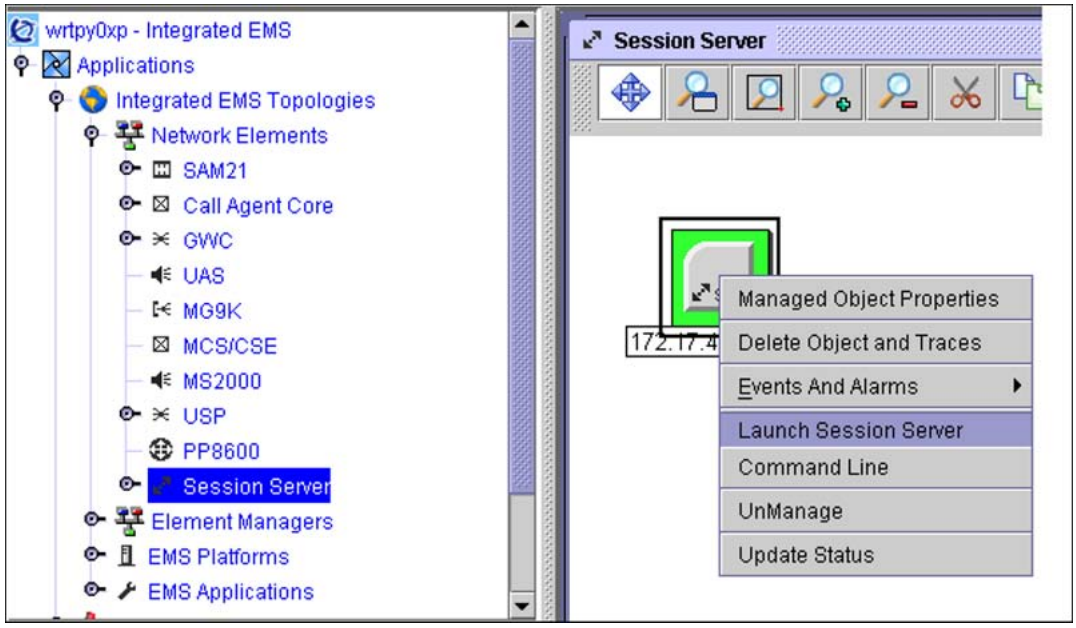
The SST can be configured to be accessed from the Integrated Element Manager System (IEMS) between the customer operation LAN and the CS 2000 CS LAN. It can also be configured without the IEMS because the SST functions as its own element manager. This means that provisioning takes place on the node itself.

Personnel use a web-based interface to perform the provisioning and maintenance activities. The web-based interface consists of a web server, running on both SST units, that provides web pages for performing OAM&P activities.

There are three primary methods for accessing user interfaces:

- Selecting and right-clicking on the active unit from the IEMS expanded Network Elements view, as shown below.

Accessing Session Server GUIs or CLI from the IEMS



For more information, refer to procedure "Access the CS 2000 SST from the IEMS," found in the *Session Server Trunks Security and Administration* (NN10346-611). For information about using the IEMS service, refer to the *IEMS Overview* (NN10329-111).

- Graphical user interfaces to the SST can be accessed from a remote system known to the proxy server (running on CS 2000 Management Tools server) on the CS LAN.
- The CLI interface can be accessed through a secure shell (SSH) connection from a remote client to a unit by way of SSH/telnet access through the SPFS server.

  The CLI can also be accessed using a console connected to the rear of the unit. In some cases, this connection is wired to a terminal box. See "Attaching a VGA monitor and keyboard console" (page 25) for more information about using this method.

Limitations and restrictions

For all methods of GUI access, first-party cookies (cookies that only get sent back to the originating server) must be enabled on the client system web browser to enable logging in to the SST. Third-party cookies (cookies that can be read by servers other than the originating server) can be disabled.

Web browsers can only connect over secure HTTP (https). For security reasons, non-secure access (http) is not supported.

Pop-Up blocking should be either disabled or restricted to only allow pop-ups from the same server. If you must use Pop-Up blocking software, add the SPFS server's hostname or IP address to the software's "no block" list. Please consult technical support or local IS services for more information on browser configuration policies and restrictions.

SST configuration

The following high-level activities are included in this document:

- SST NCGL Platform commissioning
- SST SIP Gateway Application software installation
- SST SIP Gateway Application provisioning

Configuring multiple SST nodes in the call server network

One or more SST nodes are installed in either the SAMF or Call Control Frame (CCF) or Call Server Frame (CSF). On the SAMF, up to two SST nodes, up to four hardware units, are mounted at the top of the frame, starting below the BIP power distribution unit. On the CCF, an SST node, made up of two hardware units, is usually mounted below the STORM SAM-XTS units. On the CSF, up to six HP servers can be used for SST.

Each unit is labeled for identification to distinguish it from other devices in the network frame. Most often, the naming identification should be similar to the hostname of the unit made during commissioning. For more information about physically locating SST nodes in the SAMF, CCF and CSF, refer to the *Session Server Trunks Basics* (NN10333-111).

Overview of CS 2000 XA-Core and Compact Call Agent table provisioning

There are several important tables that are provisioned on the CS 2000 XA-Core or the CS 2000 Compact to enable processing of SIP calls by the SST. These include:

- Table SERVRINV stores provisioned data for gateway controllers (GWC) including SIP-T and VRDN GWCs used by the SST.
- Table SERVSINV contains the names of the server subtending nodes and their associated gateways. The subtending nodes are the Audio Controller and the SIP-T Dynamic Packet Trunks (DPTs).
- Table TRKGRP contains customer defined data associated with each trunk group that exists in the switch. This applies to SIP-T DPT trunk groups.
- Table TRKOPTS provides a mechanism to identify and store network protocol data for DPTs. Because SST uses DPT trunks, SIP trunk CLLIs in table TRKOPTS require DPT datafill.
- Table SIPLINK is where the association is made between a trunk group and a SIP LINKNAME.
- Table DPTRKMEM dynamically provisions DPT trunks for the IP network. For SST, table DPTRKMEM provides a means to associate trunk group CLLIs with ranges of external trunk names (EXTRKNM).

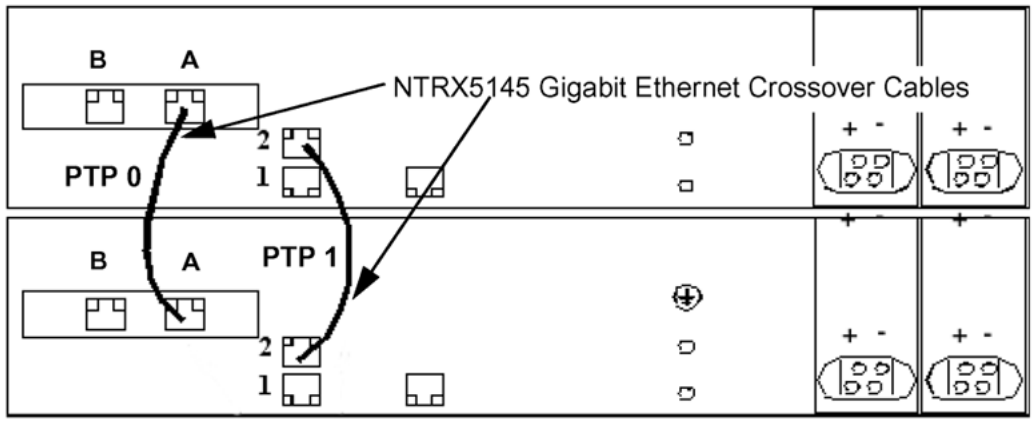
For more information about provisioning these tables, refer to the CS 2000 Configuration Management NTP applicable to your solution.

Connecting SST Ethernet ports to the CS LAN

Each of a unit's two gigabit Ethernet interfaces (shown as link 0 and link 1) are directed to the CS 2000 LAN switch that routes call traffic and signaling on the customer's private central office network. In addition, two Ethernet interfaces, acting as Point To Point (PTP) links, connect unit 0 to unit 1.

The following figure shows a rear view of a Session Sever unit chassis and the location of the Ethernet connections.

Ethernet ports and cable connections for SST units



Notes about ethernet ports:

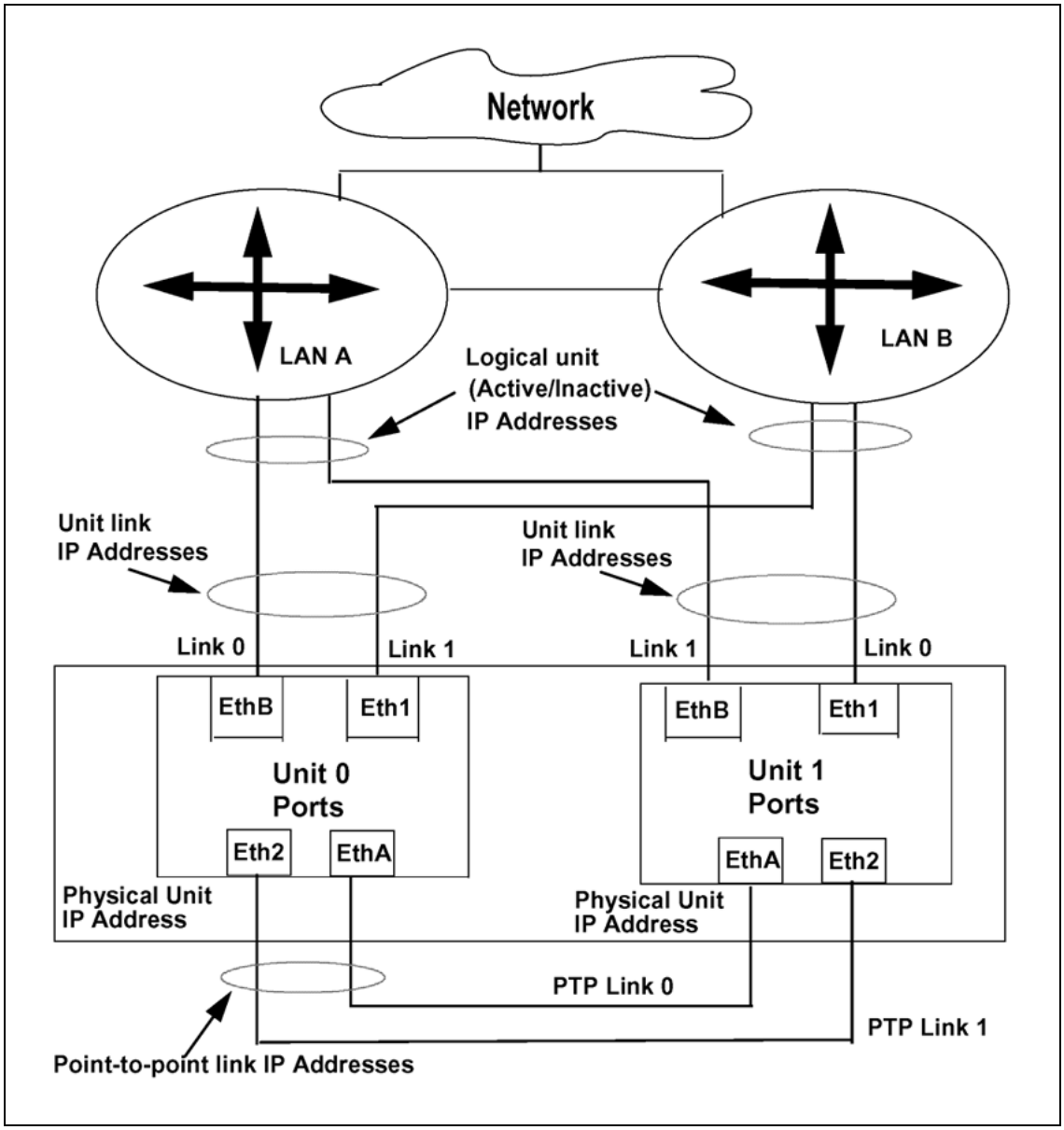
Ports 1 and B (both sets) go to CS LAN Switch

Ports 2 (PTP1) and A (PTP0), on both units, are used for point-to-point connections between Session Server - Trunks units

Mapping IP addresses and links to physical Ethernet ports

The following figure shows the port and link configuration for both units. Port ethB of each unit is connected directly to a CS LAN switch, while port eth1 is connected to the redundant CS LAN switch. Ports ethA and eth2, found on each unit, are cross-connected to the mate ports on the mate units. This configuration is used to support full network redundancy between both units and between the units and the network.

Physical map of Ethernet links and ports to IP addresses



Understanding SST node IP addressing

All the physical Ethernet ports on each unit are assigned an IP address. Together both units use a block of eight consecutive IP addresses all on the same subnet as the CS LAN. Address usage is assigned as follows:

- Four IP addresses, one for each physical Ethernet port
- Four IP addresses, an active and inactive logical address per unit
- Two internal IP addresses, one for each end of the point-to-point connections

The unit 0 and unit 1 IP physical addresses are specified during the commissioning process. Consideration of requirements at the customer site and the IP solution Network Engineering Guidelines are used. The rest of the IP addresses are calculated by the system based on the unit 0 physical IP address. Note the last octet of the active IP address must be divisible by 8.

Sample IP addressing scheme for an SST node

Session Server IP addresses	Example unit IP address scheme	Datafilled or generated by:	Description
Active unit	172.16.16.72	system	Logical unit
	Note: The active node's last set of digits must be the highest address and must be divisible by 8.		
Inactive unit	172.16.16.71	system	Logical unit
Unit 0	172.16.16.67	user	Physical unit 0
Unit 0, Link 0	172.16.16.65	system	Physical unit link
Unit 0, Link 1	172.16.16.66	system	Physical unit link
Unit 1	172.16.16.70	user	Physical unit 1
Unit 1, Link 0	172.16.16.68	system	Physical unit link
Unit 1, Link 1	172.16.16.69	system	Physical unit link
Local PTP link 0	192.168.1.1	system	Local point to point link
	Note: The IP addresses 192.168.1.1 and 192.168.1.2 are generated by the system and assigned to the local and mate unit Point to Point (PTP) links. To avoid conflict, do not assign the same IP address to the mate PTP link on the mate unit.		
Mate PTP link 1	192.168.1.2	system	Mate point to point link

Managing Session Server GUI access using IEMS

The IEMS must be configured to enable access to the SST user interfaces. Refer to the following procedures.

Procedure
"Adding a Session Server," refer to *IEMS Configuration Management* (NN10330-511)
"Modifying NCGL platform provisioning" (page 202)

Adding DPT trunk group connections handled by SST

Adding new SIP trunk groups to a local Call Server network involves configuration activities on a range of network elements.

New DPT (SIP) trunk datafill must be added to table SIPLINK on the CS 2000, and the DPT entry RTS'd from the DPTTRM map level of the CS 2000 to facilitate the link names being transferred from table SIPLINK. See "Troubleshooting SIP-T trunk group link status on the Core" in the *Session Server Trunks Fault Management* (NN10332-911), for details about bringing new DPT (SIP) trunks into service, monitoring their status, and troubleshooting service issues.

In addition to the normal commissioning and provisioning required to add a new DPT GWC, the IP address of the GWC(s) must be added to the list of GWCs associated with the SST node while the SST node is in service. Additional DPT GWCs required to handle increased call volume, can be introduced without any impact to call processing. The in-service addition of trunk groups and DPT GWCs made available to the SST node can be accomplished because the SST node uses a simple, round-robin scheme to distribute incoming calls across all in-service DPT GWCs. Consult the CS 2000 Configuration Management document for your solution for information and end-to-end instructions for adding new DPT trunk groups for your network.

ATTENTION

In a multiple SST configuration, all DPT GWCs in use for SST calls need to be provisioned on all SST nodes carrying SIP calls on the CS 2000. The shared GWCs report the state of inservice where the link status of the last GWC to report is enforced. Provisioning all the DPT GWCs on all SST nodes is necessary to ensure correct reporting of the SST associated trunk states.

Use the following procedures to add new trunk groups to your network:

Procedure

Refer to and complete procedure *Provisioning SIP-T DPTs in an office with a Session Server*, found in the CS 2000 Configuration Management NTP applicable to your solution

"Adding and managing telephony profiles" (page 68)

"Configuring Remote SIP Servers" (page 26)

"Adding and managing Access Link Maps" (page 73)

Modifying SIP (DPT) trunk group connections handled by SST

Use the following procedures to modify the number of trunk groups that can process calls on the SST:

Procedure
"Modifying DPT trunk group connections supported by the SIP Gateway application" (page 173)

Increasing the number of calls allowed through SST

Whenever you are adding new trunk groups or increasing the number of SIP calls that can be managed by your network you must adjust the SST provisioning.

Use the following procedures to increase the number of simultaneous calls that can be handled by the SST:

Procedure
"Modifying SST maximum DPT call limits" (page 174)

Enabling optional access control lists (ACLs) for remote SIP servers

In certain central office environments it may be desirable to restrict which far-end nodes or servers are allowed to initiate call processing with the SIP Gateway application on the SST node. The ability to create these restrictions exists in the form of an Access Control List (ACL).

Enabling Access Control List (ACL) will mitigate the risk of potential Denial of Service attacks. Please ensure to add only trusted and authenticated IP addresses to the ACL.

The following conditions and restrictions apply to the ACL:

- ACL functionality is optional and can be enabled/disabled by users. By default ACL is disabled. ACL is enabled and disabled using the system configuration menu of SIP Gateway application.
- If ACL is disabled, all incoming SIP messages are accepted.
- Because remote SIP servers are automatically included in the ACL list for screening, remote SIP server IP addresses are not required to be provisioned again in the ACL list.
- With ACL enabled, SIP messages only from the list of servers provisioned in ACL list or listed in Remote SIP Server IP list are accepted.
- All remote servers and gateways that can connect to the SST SIP Gateway application must be datafilled in ACL if it is enabled. For example, if the remote server is a VRDN, it is not sufficient to simply

datafill the VRDN IP address, all SIP-T GWCs must also be included in the ACL, because SIP-T GWCs send SIP messages directly to the SST.

- If ACL is enabled while both the ACL list and Remote Server IP address list are empty, all incoming messages are dropped. Before enabling ACL, ensure that you have properly provisioned the Remote SIP server and/or the ACL list.
- Access control list datafill may be added using the Add IP Range link in the *Access Control List* folder.
- When adding an IP address range to the ACL, the range of IP addresses to allow is calculated based on a combination of the IP address and network mask entered.

Use the following procedures to setup and manage the access control list:

Procedure
"Configuring SIP Gateway application parameters" (page 46)
"Configuring Remote SIP Servers" (page 26)
"Adding and managing SIP server IP address access control lists" (page 58)
"Adding and managing SIP-T GWCs" (page 62)

Creating and modifying NCGL filesystems

Use the following procedures to manage filesystems in the NCGL operating system:

Procedure
"Starting filesystem monitoring" (page 210)
"Stopping filesystem monitoring" (page 213)
"Modifying filesystem monitoring thresholds" (page 215)
"Removing a filesystem" (page 225)
"Increasing filesystem size" (page 217)
"Creating a filesystem" (page 220)

Performing SST platform re-commissioning

Use the following procedures to re-commission the platform and NCGL operating system and to reconfigure the system BIOS settings:

Procedure
"Modifying NCGL platform provisioning" (page 202)
"Reprovisioning the NCGL platform software" (page 192)

Procedure
"Reconfiguring the SST BIOS" (page 188)
"Adding an SST node to the SPFS server web proxy" (page 176)

Reinstalling SIP Gateway Application software

For detailed information about reinstalling the SIP Gateway application as part of an upgrade activity, refer to the *Nortel Carrier Voice over IP Upgrade and Patches* (NN10440-450).

Managing the SIP Gateway Application call processing

Use the following procedures to manage call processing activity handled by the SIP Gateway Application running on the active SST unit:

Procedure
"Locking the SIP Gateway application" (page 161)
"Unlocking the SIP Gateway application" (page 164)
"Suspending the SIP Gateway application" (page 167)
"Unsuspending the SIP Gateway application" (page 170)

Reconfiguring the SIP Gateway application software

Execute the following steps in the order presented, to reconfigure the SIP Gateway Application software on a unit:

ATTENTION

When possible, only perform service affecting procedures on the inactive unit after confirming that the active unit is alarm free. Failure to do so may affect call processing on the active unit.

Step	Procedure
1	"Configuring SIP Gateway application parameters" (page 46)
2	"Configuring Remote SIP Servers" (page 26)
3	"Adding and managing SIP server IP address access control lists" (page 58)
4	"Adding and managing SIP-T GWCs" (page 62)
5	"Adding and managing telephony profiles" (page 68)
6	"Adding and managing NOAs, NPIs, and Phone Context maps" (page 78)
7	"Adding and managing Access Link Maps" (page 73)
8	"Adding and managing SIP base protocols" (page 89)
9	"Adding and managing ISUP to SIP mapping" (page 94)

Step	Procedure
10	"Adding and managing SIP to ISUP mapping" (page 104)
11	"Adding and managing SIP Redirection mapping" (page 112)
12	"Adding and managing ISUP variant mappings" (page 119)

Monitoring the SST platform and SIP Gateway application

Use the following procedures to monitor call processing activity handled by the SIP Gateway application and to monitor the status of resources and the activity of either the active or standby unit:

Procedure
"Viewing the operational status of the SIP Gateway application" (page 141)
"Viewing the operational status of the NCGL platform" (page 146)

Enabling T.38 Annex D for SIP

This feature provides T.38 Annex D interworking support for SIP with a Nortel Media Gateway 7480/15000 using H.248 signaling on the local side. For this feature to work, the Gateway Controller must have T.38 enabled in the network codec profile provisioning, the H.248 Media Gateway 7480/15000 must support T.38, and field T.38 AnnexD Supported must be set to Yes on the Remote SIP Server web page. If these conditions are met, then a switchover from G.729 or G.711 to T.38 is performed upon fax detection.

The switchover is performed by sending a re-invite message with the new codec. If the offer is accepted, the call switches to T.38 after the re-invite sequence completes. In the event that the switchover is rejected at either end, an attempt is made to preserve the call by switching to G.711.

A second part of this feature offers the ability to prevent automatic upspeed of G.729 to G.711 by the Media Gateway 7480/15000, which is the default Media Gateway 7480/15000 behavior to perform upon fax detection. When configuring or reconfiguring the Media Gateway 7480/15000 on the Remote SIP Server web page, field Re-Invite for Voice Band Data must be set to Yes to provide this functionality. If set to Yes, the Media Gateway 7480/15000 will not automatically upspeed to G.711, but send a re-invite request instead. The negotiated result of the re-invite request depends on the codec of the original call, and the status of the two fields just described:

- Re-Invite for Voice Band Data enabled, T.38 disabled

  If the voice codec is G.729, then the Media Gateway 7480/15000 will re-invite to G.711 upon fax detection. If the voice codec is G.711 no re-invite request is sent.

- Re-Invite for Voice Band Data enabled, T.38 enabled

If the voice codec is G.729 or G.711 and fax tones (V.21/CNG) are detected, a re-invite request to T.38 is sent. If the voice codec is G.729 and fax tones other than V.21/CNG are detected, a re-invite to G.711 is sent, and the SST continues to scan for fax tones. If V.21/CNG tones are detected, a re-invite to T.38 is sent.

Set fields T.38 AnnexD Supported and Re-Invite for Voice Band Data accordingly for new and existing remote SIP servers:

Procedure
"Configuring Remote SIP Servers" (page 26)

CWR activation/deactivation for trunk type

To enable CRW for a desired trunk type, set the CWR_ON_TRUNK option in table ISERVOPT to Y. To disable CRW for a desired trunk type, set the CWR_ON_TRUNK option in table ISERVOPT to N. The CWR_ON_TRUNK option contains the following trunk types.

- ETSI_ISUP
- IBN7
- R2

All the trunk groups that belong to a trunk type (listed above) support CWR when the trunk type is set to Y in table ISERVOPT.

CWR deactivation for individual trunk group

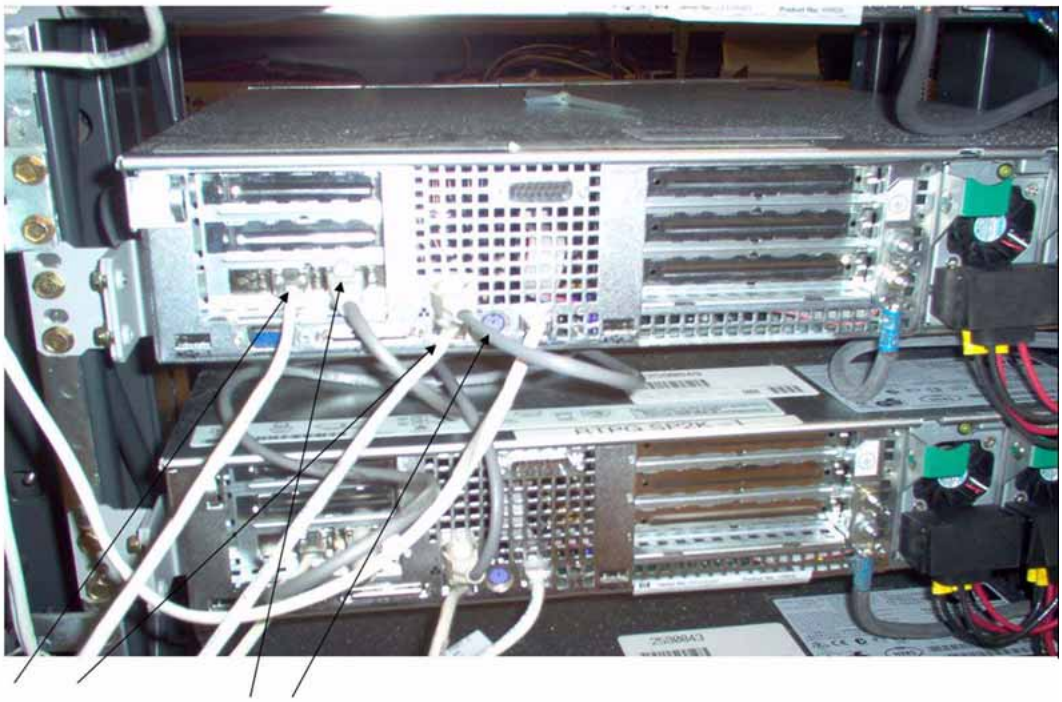
Option CWR_OFF in table TRKOPTS provides the ability to disable CWR for a specific trunk group without disabling the whole trunk type. Option CWR_OFF is independent of the CWR_ON_TRUNK in table ISERVOPT. Therefore, if CWR_OFF is assigned to a trunk group in table TRKOPTS, CWR is disabled for that trunk group even though CWR_ON_TRUNK is enabled in table ISERVOPT.

If the CWR_OFF option is removed from a trunk group in table TRKOPTS, the setting in option CWR_ON_TRUNK in table ISERVOPT is considered again for CWR over trunk ability.

There is no explicit relationship or dependency between the settings in table TRKOPTS and ISERVOPT. It is possible to assign the CWR_OFF option to a trunk group even if the trunk type of that trunk group is disabled in option CWR_ON_TRUNK.

Checking Ethernet cabling at the rear of the units

Each unit may be configured with two 1000Mbs/100Mbs/10Mbs interfaces directed to the LAN switch, as represented by link 0 and link 1. Configuration depends on the IP router configuration. In addition, two interfaces connect unit 0 to unit 1, as shown as the Point To Point (PTP) link.



MCS interoperability

SST POR feature 2787 Out of band SIP Refer Signaling Between MCS 5200 and CS 2000 provides improved Converged Desktop 2 interaction.

Use this feature to enable out-of-band REFER for click-to-dial on SST.

Navigation

- For brief feature highlights, refer to Out-of-Band REFER
- For procedures, refer to Configuring MCS interoperability

Out-of-band REFER

Feature description

The SST uses a non-call associated signalling (NCAS) link for out-of-band REFER messaging to provide the following improvements to the MCS 5200 click-to-dial feature:

- correctly removes click-to-dial call originator from the terminating call model (TCM) on the CS 2000.
- recognizes originating call manager (OCM) services and feature interactions. These interactions include denied originations, PIC, LPIC, and other translation-related services.
- avoids unnecessary TCM interactions such as call forwarding on the originator of click to dial.
- resolves an error in OCM, updating incoming call memory (ICM).
- resolves problems with ringback, tones, busy signal, and treatments not heard by the originator. A click-to-dial call has two distinct trunk-to-line calls with their media tied to the MCS 5200.
- correctly captures billing for incoming terminating calls.

Limitations and restrictions

Following restrictions and limitations apply to this feature:

- Session Server Lines are not supported.
- Messages can be lost during various maintenance actions such as restarts and swacts. These actions could cause the Call Log on the MCS 5200 not to be updated correctly.
- International calls are not supported by this activity due to a limitation in the number of CDN digits that can be sent to the CS 2000. Subscribers cannot dial international calls from click-to-dial.

Individual procedures

CAUTION
You must execute most procedures in the rest of this document as part of a higher level activity. Refer to "Configuration management strategy" (page 7).

Attaching a VT-100 console monitor to the RJ-45 serial port

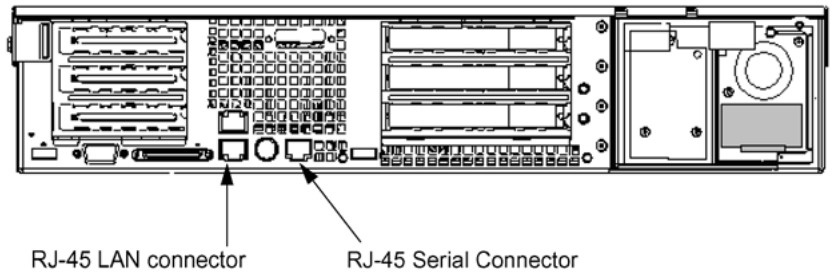
Use the following procedure to attach a VT-100 monitor (or emulator) or input to a serial box to the rear of the chassis for use as a console monitor using an RJ-45 serial connector (Nortel PEC NTRX5178). This may be required to isolate faults or to assist in commissioning activities.

CAUTION
Remove the RJ45 serial cable from the unit once this procedure is complete. Failure to remove the cable may cause future software upgrades to fail.

Use this procedure when the operating system is not fully configured.

Procedure steps

Step	Action
1	At the rear of the chassis, attach the VT-100+ terminal to the serial port using the diagram shown below.



2	Ensure that the SST RJ-45 Serial cable is connected to the serial port on the rear of the unit and not the RJ-45 LAN connector. It should be connected to a VT-100 capable console device such as a PC or laptop running a VT-100 terminal communications session into the RJ-45.

—End—

Attaching a VGA monitor and keyboard console

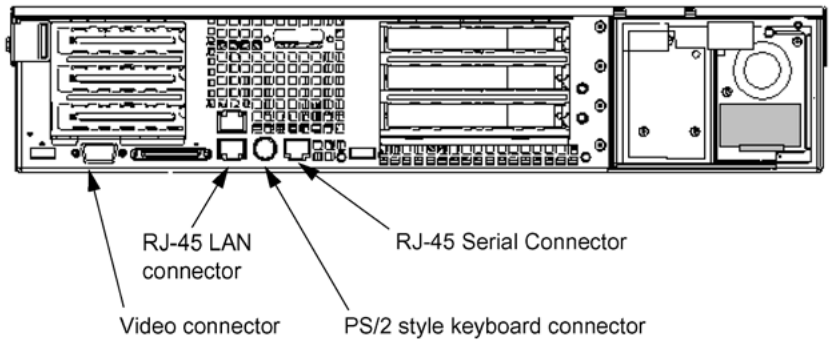
Use the following procedure to attach a VGA monitor and PS/2 style keyboard into the rear of an SST chassis for use as a console monitor.

ATTENTION

You cannot use this method to fully commission an SST unit. Instead, use method "Attaching a VT-100 console monitor to the RJ-45 serial port" (page 24).

Procedure steps

Step	Action
1	Plug in a PS/2 style keyboard and VGA monitor into the rear of the SST chassis using the diagram shown below. Optionally use a dongle (Y cable) to connect both keyboard and mouse to the same PS/2 mouse/keyboard port.



—End—

Configuring Remote SIP Servers

Purpose of this procedure

Use the following procedure to add, list details for, and delete data entries for remote SIP Servers in the SIP Gateway application database.

The SST communicates with a remote SIP server or any remote SIP device, such as other CS 2000 Communication Servers or a Multimedia Communication Server (MCS), using the session initiation protocol. SST awareness of these remote SIP servers is provisioned using this procedure.

Limitations and restrictions

New SIP servers can have a maximum name length of 64 characters.

If you are adding a new SIP server associated with a new trunk group, first see "Adding DPT trunk group connections handled by SST" (page 13) to ensure that all prerequisite activities have been completed.

When you modify GWC IP addresses, you cannot reuse IP addresses.

When you modify a Session Server IP address datafill for existing remote SIP servers, you cannot reuse remote server names and IP addresses.

For sites that enable optional access control lists (ACL), because remote SIP servers are automatically included in the ACL list for screening, it is not necessary to reprovision remote SIP server IP addresses in the ACL list.

SIP and SIP-T interface

None of the new SIP headers and parameters, except History-Info, associated with the SIP and SIP-T interface are part of any SIP RFC or draft. Therefore, the enhanced SIP mapping for SIP and SIP-T interface only works with two Nortel CS 2000s or PMSCs. The new SIP headers and parameters are included in Recommended and default Remote SIP Server provisioning parameters.

Simultaneous SIP and SIP-T interface to a remote server is not supported.

Also, the SIP and SIP-T interface supports only ANSI ISUP. SIP interface for international ISUP variants, such as Brazil ISUP, is not supported.

Prerequisites

You must complete this procedure before procedure "Adding and managing Access Link Maps" (page 73).

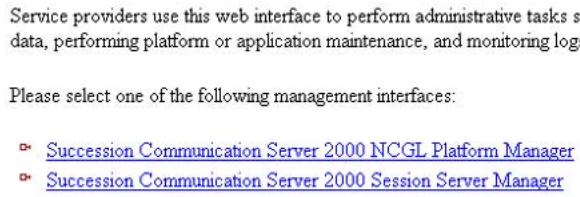
Review section "Recommended provisioning information for various configurations" (page 40) for details regarding completing datafill activities applicable to your configuration and Carrier VoIP software release.

Action

Step	Action

At the CS 2000 Session Server Launch Point or IEMS client

1 Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



2 Select **Provisioning > Application > SIP Gateway > Remote SIP Server** from the left side menu.

3 Use the following table to determine your next step:

If	Do
adding a Remote SIP Server	step 4
modifying an existing Remote SIP Server	step 9
deleting a Remote SIP Server	step 14

4 Click **Add Server**.

The Add a SIP Server page opens in the right side frame.

5 Click **Add Opt IP Address** to add optional IP addresses. Repeat this step to add up to a maximum of 90 IP addresses.

6 Datafill each field using "Recommended or default Remote SIP Server provisioning parameters" (page 31). Default and recommended values are indicated in this table where appropriate. Also, review section "Recommended provisioning information for various configurations" (page 40) for details regarding completing datafill activities applicable to your configuration and Carrier VoIP software release.

The following is a minimum list of fields that must be datafilled for the SIP Gateway Application to work properly with a remote SIP server. For unlisted fields, assume defaults are used:

- Server Name (up to 128 alphanumeric characters, with hyphens, underscores and periods allowed)
- Server Type
- IP Address (Use the default Port number and Protocol values; do not use 0.0.0.0)

  In a loop-around configuration, the IP Address field for the Remote SIP server representing the SST node should be datafilled with the active IP address of the SST node itself. This IP address was assigned during the initial commissioning.
- NOA/NPI to Phone Context Map
- Out of Band DTMF Payload (select a DTMF payload from the drop-down menu)
- ISUP to SIP Cause Map (select from drop-down menu)
- SIP to ISUP Cause Map (select from drop-down menu)

- SIP Redirection Map (select from drop-down menu)
- ISUP Variant to SIP Version Map (select from drop-down menu)

Custom mapping does not need to be defined for the SIP Gateway application to function. DEFAULTS can be used.

7 When you have verified that the information is correct, click the **Add** button. If you are uncertain about the validity of all data, click the **Abort Operation** button to cancel the operation.

8 Click **OK** to confirm aborting the addition.

9 Use the following table to determine your next step:

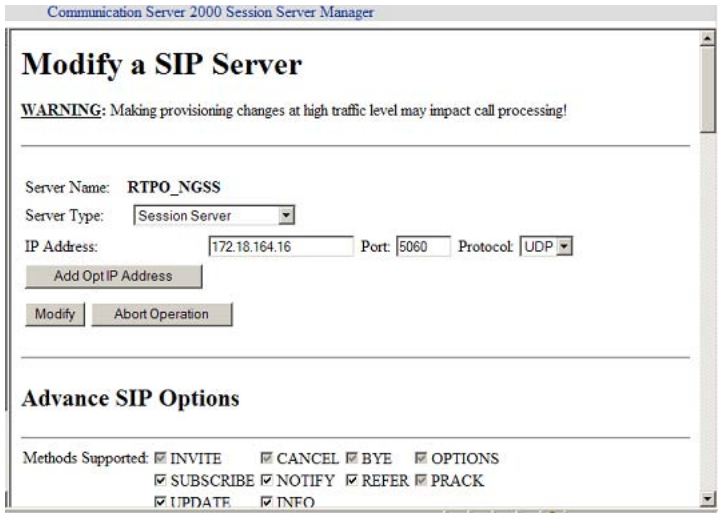
If	Do
you want to add more Remote SIP Servers	return to step 4
you want to view or modify the provisioning parameters for the new Remote SIP Server you added to the database	continue with step 9
you want to delete an existing Remote SIP Server	skip to step 14

10 Click **List Servers**.

The List Remote SIP Servers page opens in the right side frame.

11 Click **Details** for a Remote SIP Server to review provisioning details.

The Modify a SIP Server page opens in the right frame.



12 See "Recommended or default Remote SIP Server provisioning parameters" (page 31) to assist with parameters.

13 Click the **Modify** button (found by scrolling to the bottom of the page) when done, then the **OK** button to confirm the changes.

ATTENTION

Enabling TLS requires that the server name is less than or equal to 64 characters. If their server name is longer than 64 characters, you will receive an error message and you must cancel enabling TLS. To enable TLS on a SIP Server that was upgraded from SN07, you must first completely delete the server, then add it into the database again. However, before deleting any SIP server, take a snapshot of the web page showing the server's settings or record the datafill and settings for the server. The SIP application database will not remember the data when you add the server back in.

Ensure that any SIP servers for which you want to modify datafill are not in use processing calls. If you attempt to modify SIP server datafill for a server that is processing calls, the request may be denied by the system.

14 Return to step 3 if you want to make other changes to other Remote SIP Servers. Otherwise you have completed this procedure.

15 To delete a remote SIP server, click **List Servers**. Otherwise skip to step 17.

The List Remote SIP Servers page opens in the right side frame.

16 Click the **Delete** link next to the SIP server to remove.

Ensure that any servers that you want to delete are not in use. If you attempt to delete a server that is in use, the request is denied by the system.

The system responses:

```
Do you really wish to delete the SIP server
<servername>?
```

17 Click **OK** to confirm the deletion.

18 Return to step 3 if you want to make other changes to other Remote SIP Servers. Otherwise, you have completed this procedure.

—End—

Recommended or default Remote SIP Server provisioning parameters

Use the following table to assist you with datafilling the remote SIP server fields with the correct values. In addition, for certain configurations and compatibility issues, See the following tables:

- "Recommended provisioning information for various configurations" (page 40)

Field	Description	Default Value or Range	Recommended Value
Modify a SIP Server			
Server Name	Character string name for the remote SIP server, up to 128 alphanumeric characters, with hyphens, underscores and periods allowed.	N/A	Use DNS naming conventions when naming your server.
Server Type	Indicates the role and capabilities of the remote SIP server.	N/A	See "Recommended provisioning information for various configurations" (page 40)

Field	Description	Default Value or Range	Recommended Value
IP Address, Port, and Protocol	An IP address for the Remote SIP Server in the following format: 192.168.12.101 At least one IP address must be entered. If used for loop-around calls, the IP address for the active SST node should be entered.	Default Port address is 5060 for UDP or TCP, and 5061 for TLS. Default Protocol is UDP. Other options include TCP and TLS.	See "Recommended provisioning information for various configurations" (page 40).
Optional (Opt) IP Addresses, Ports, and Protocols	Up to 6 additional IP addresses, ports and protocols are supported for each remote SIP server.	Default Port address is 5060 Default Protocol is UDP. Other options include TCP and TLS.	See "Recommended provisioning information for various configurations" (page 40).
Advanced SIP Options			
Methods Supported	Contains the following options: • INVITE • CANCEL • BYE • OPTIONS • SUBSCRIBE • NOTIFY • REFER • PRACK • UPDATE • INFO	INVITE, CANCEL, BYE, OPTIONS, PRACK	See "Recommended provisioning information for various configurations" (page 40).
SIP Headers Supported	Click appropriate advanced SIP options headers supported by remote server: • Content-Disposition • Remote-Party-ID • P-Asserted-ID • Privacy • Reason • Replaces • Referred-By	All False; check a box to make the header true (supported)	See "Recommended provisioning information for various configurations" (page 40).

Field	Description	Default Value or Range	Recommended Value
	• Diversion • History Info • Generic Digits • Charge Number • Resource-Priority		
URI Parameters Supported	The following Uniform Resource Indicator (URI) parameters are supported:	CIC, RN, NPDI, and Phone-Context	See "Recommended provisioning information for various configurations" (page 40).
• CIC	Circuit Identification Code (CIC) carries circuit information from SIP to ISUP and vice-versa.		
• RN	Redirect Number (RN) used in LNP scenarios		
• NPDI	Number Portability Dip Indicator (NPDI) indicates that LNP Dip has been done and prevents lookups in legacy PSTN databases		
• Phone-Context	Phone-Context indicates the geographic context of phone number such as number plan area, for example North America, or local calling area		
• OLI	Originating Line Information (OLI) provides information about the nature of the line, such as toll call from a pay phone or hotel.		
• CIP	Carrier Identification Parameter (CIP) provides an identification code which identifies the transporting network. CPC is provided in setup data supplied by the calling party or by subscription.		
• JIP	Jurisdiction Information Parameter (JIP) indicates the switch that originates the call and may be used to determine calling charges		

Field	Description	Default Value or Range	Recommended Value
• Carrier Selection	Carrier Selection forwards information that identifies whether the calling user presubscribed to the transit network or dialled input. Also, if the caller presubscribed, Carrier Selection flags if they dialled the carrier identification code.		
• NOC	Nature of Connection (NOC) information forwarded to identify satellite indicator, continuity check indicator, and echo control device indicator.		
• CPC	Calling Party Category (CPC) identifies various classes of calling party, such as parties that opt out of call display. Also distinguishes between types of callers, allowing for different treatment of emergency callers such as police or 911 over general callers.		
Non-Standard MIME Type	Contains the following parameters: • User-to-User Interface (UUI) • Location XML	 unselected unselected	See "Recommended provisioning information for various configurations" (page 40)
SIP Header Format	Supports the following form of SIP headers: • Compact • Long	Compact	Use the default
Use OPTIONS for Heartbeat	Indicates if SIP Options method is used to determine accessibility of the SIP server.	No	See "Recommended provisioning information for various configurations" (page 40)

Field	Description	Default Value or Range	Recommended Value
Telephony Profile Support	An indication of whether or not the SST sends the x-nortel-profile header or the Trunk Group ID Prefix to this remote SIP Server.	Yes Datafill with "No" when the Remote SIP Server does not support receiving the x-nortel-profile header or Trunk Group ID Prefix in the SIP message.	Use the default
Accepts Early SDP	Determines if Early Session Description Protocol is allowed	Yes	See "Recommended provisioning information for various configurations" (page 40).
Accept Invite Without SDP	Indicates whether to accept an Invite without SDP and proceed with the call or reject the call and return a *488 Not Accepted Here* error response	Yes	Use the default
Enforce CODEC -Compatibility	Indicates whether support for other codecs is provided. If Yes, then at least one of the codec fields must be set to yes in the Config Data web page. See the procedure "Configuring SIP Gateway application parameters" (page 46).	No	See "Recommended provisioning information for various configurations" (page 40).
Accepts Encapsulated ISUP	Indicates whether to perform ISUP encapsulation or not. For call overlap to be supported, this value must be set to Y and the Accepts Early SDP value must be set to N.	Yes	See "Recommended provisioning information for various configurations" (page 40).
Conn Mode Allowed	Use the default unless otherwise specified	No	No
OCN Allowed	Use the default unless otherwise specified	No	No
T.38AnnexD Supported	Indicates if the remote SIP server supports switching the codec to T.38 upon fax detection. See "Enabling T.38 Annex D for SIP" (page 18).	No	No

Field	Description	Default Value or Range	Recommended Value
Re-Invite for Voice Band Data	Related to field T.38 AnnexD Supported, forces the remote SIP server to send a re-invite message before changing voice codec. See "Enabling T.38 Annex D for SIP" (page 18).	No	No
Enhanced Media Cut Through (EMCT)		Yes	See"Recommended provisioning information for various configurations" (page 40)
Auto-Subscribe	This field enables full RFC 3842 compliancy by allowing the SIP Gateway application to send and receive the subscribe header for the Message Waiting application.	No	See "Recommended provisioning information for various configurations" (page 40).
E.164 Format Allowed	Indicates if E.164 format is supported. To derive ETSI ISUP messages utilizing SIP instead of SIP-T, value must be set to No. ***Note:*** If this field is set to 'Y', the **Country Code Supported** must be set to 'Y' and a valid **Country Code** datafilled in the provided field.	No	See "Recommended provisioning information for various configurations" (page 40).
Validate Request URI	Checks for a valid IP address or hostname in the Request URI in the INVITE message before allowing the call to complete when enabled	No	See "Recommended provisioning information for various configurations" (page 40)
Country Code	Indicates what Country Code to use. Datafill a three-digit Country Code if E.164 Format Allowed is set to Yes.	NULL	See "Recommended provisioning information for various configurations" (page 40)

Field	Description	Default Value or Range	Recommended Value
Long Call Audit Mechanism	Long call audit provisioning If the SIP Info audit method is specified, the Session Server Manager sends a SIP INFO message to the SIP server destination at regular intervals. If no response is received on two successive audit attempts or if an error response is received, the call is taken down.	INFO. Other options are NONE, Re-invite with SDP, and Session Timer If the Long Call Audit Mechanism value is set to Session Timer then a valid value for Session Timer must be datafilled.	INFO
	Note: If the remote SIP server does not support the SIP INFO message for this purpose, the SIP server must be configured to use the SIP re-invite method for auditing. If this approach is selected, a SIP Invite is sent at regular intervals for a call once it is answered. Again, successive failures or no response results in the call being taken down. If the call is not answered after multiple audit intervals, the call is taken down.		
Session Timer Value	Used to track and apply limits to the duration of a session.	Default is 20 minutes. The range is 5-30 minutes	Use the default
	To enable Session Timer on remote SIP servers, set the following options: • On the SST GUI, go to SIP Gateway > Config Data and change supportedExtensionList from “100rel” to “100rel, timer”. This change requires restarting CallP. See the procedures "Configuring SIP Gateway application parameters" (page 46) and "Invoking a maintenance SWACT of the SST platform" in *Session Server Trunks Security and Administration* (NN10346-611) • Set the Long Call Audit Mechanism value to Session Timer and set the timer value between 5 and 30 minutes.		
Out of Band DTMF Payload	Indicates the Out of Band DTMF payload monitor/detection mechanism to use. Select from the drop down menu: • application/dtmf-relay • application/telephone-event • application/vnd.nortelnetworks.digits • Not Applicable	application/telephone-event	See "Recommended provisioning information for various configurations" (page 40). Set to vnd.nortelnetworks.digits if the remote SIP server is not RFC 2833 compliant.
Agent Representation	Indicates the agent supported; ISUP, PRI, or Line		

Field	Description	Default Value or Range	Recommended Value
Unknown header	Indicates the string to use when Presentation indication is Unknown	NULL	Use the default unless otherwise specified
Anonymous header	Indicates the string to use when Presentation indication is restricted	NULL	Use the default unless otherwise specified
Server Identifier	Only for MCS 3.0 use CS 2000_NGSS/8.0 else use NONE	None	Use the default unless otherwise specified
SIP PSTN Interworking Options			
ISUP to SIP Cause Map	Contains the name of the mapping table for ISUP Release Cause to SIP response code	DEFAULT	Select a preferred map from the list or use DEFAULT
SIP to ISUP Cause Map	Contains the name of the mapping table for SIP Response code to ISUP Release Cause	DEFAULT	Select a preferred map from the list or use DEFAULT
SIP Redirection Map	Contains the name of the mapping table for redirection mapping	DEFAULT	Select a preferred map from the list or use DEFAULT
ISUP Variant to SIP Ver Map	Contains the name of the mapping table for ISUP Variant to SIP Version Mapping.	DEFAULT	Select a preferred map from the list or use DEFAULT
NOA/NPI to Phone Context Map	Only selectable if URI parameter Phone-Context is selected. Contains the name of the mapping table for NOA/NPI to Phone Context Mapping.	DEFAULT	Select a preferred map from the list or use NULL
SIP Cause Precedence Priority	A list of precedence rules and their respective priority; 1=highest and 3=lowest. • Encapsulated Msg • Retry after reason • Cause Code Map	 First Second Third	See "Recommended provisioning information for various configurations" (page 40).
APN Information	Action Point Number for Private Numbering Plan-type calls • Representation • Prefix • Phone Context		

Field	Description	Default Value or Range	Recommended Value
BCI Data	Backward Call Indicator (BCI) options: • Interworking Indication • ISUP / BICC Indicator • ISDN Access Indicator	 Interworking Not Encountered ISUP Not Used All the Way Terminating Access is Not ISDN	See "Recommended provisioning information for various configurations" (page 40)
FCI Data	Forward Call Indicator (FCI) Data options: • Domestic/International Call Indication • Interworking Indicator • ISDN User Part Indicator • ISUP Preference Indicator • ISDN Access Indicator	 Treat as International Call Interworking Encountered ISUP Used All the Way ISUP/BICC Not Required Originating Access is Not ISDN	See "Recommended provisioning information for various configurations" (page 40)
Digit Prefix Used	Use the default unless otherwise specified	No	No
Prefix Digit for International	Use the default unless otherwise specified	Default is for field to be blank	Use the default unless otherwise specified
Trunk Group ID Prefix	Enables identification of the incoming trunk group mapping using prefix digits. When this parameter is set to a value between 1 and 7, the trunk group prefix is used as a Nortel Profile name in the Access Link Map. The value of the Trunk Group ID Prefix defines the maximum character length of the numeric trunk group prefix. ***Note:*** The x-nortel-profile header must not be present for this feature to function.	Default is 0 (disabled) and range is 1 to 7 (allowing for trunk group prefix range of 1 to 9999999	Use the default unless otherwise specified

Field	Description	Default Value or Range	Recommended Value
Hop-Counter Factor	Sets the typical number of HOPS to account for when adjusting for call latency. A Hop-Counter Factor is used to derive the Hop-Counter value. As specified in the Q1912 Standard, Table 11/Q19125, the Hop-Counter value = the Integer part of (Max-Forwards value / Hop-Counter Factor), where the factor is constructed according to the following principles: - Hop-Counter value for a given message should never increase and should decrease by at least 1 with each successive visit to an interworking unit regardless of intervening interworking, and similarly for Max-Forwards in the SIP domain. - The initial and successively mapped values of Hop-Counter should be large enough to accommodate the maximum number of hops that might be expected of a validly routed call.	Default is 7 and range is 1 to 10.	Use the default
National Circuit Code		Default is 8 and range is 8 to 15	

Recommended provisioning information for various configurations

The remote SIP server configuration page allows the craftsperson to provision a number of fields on a per-customer basis. The different configurations documented include:

- SST to MCS
- SST to VRDN
- SST to SST
- SIP-based voice mail server

The following table lists provisioning information for the above configurations when using the "Recommended or default Remote SIP Server provisioning parameters" (page 31). Use the table to provision your SST.

Field	SST to MCS	SST to VRDN	SST to SST	SIP-based voice mail server
Modify a SIP Server				
Server Type	Session Server	VRDN	Session Server	Message Server
IP Address	x.x.x.x	x.x.x.x	x.x.x.x	x.x.x.x
Port	5060	5060	15060 or 5061	5060
	The port can be configured to a number of the customer's choosing, but ensure that the port number used is consistent across the communicating nodes. The default protocol port for TCP and UDP is 5060. The default protocol port for TLS is 5061.			
Protocol	UDP	5060	UDP, TCP or TLS	UDP or TCP
Optional IP (1-6)	none	none	none	none
Advanced SIP Options				
Methods Supported	INVITE, CANCEL, BYE, OPTIONS, PRACK	INVITE, CANCEL, BYE, OPTIONS, SUBSCRIBE, NOTIFY, PRACK, INFO	INVITE, CANCEL , BYE, OPTIONS, SUBSCRIBE, NOTIFY, PRACK, INFO, UPDATE, REFER	INVITE, CANCEL, BYE, OPTIONS, PRACK, INFO, SUBSCRIBE, NOTIFY
	Note: Either all the nodes in a SIP call should support UPDATE, or none of them should. Otherwise, undesired behavior may occur.			
SIP Headers supported	Remote-Party -ID, P-Assert ed-ID,Privacy, Diversion, Cont ent-Disposition, Reason	Content-Dispo sition, one of Remote-Party-ID or P-Asserted-ID, Privacy, Diversion	all	
URI Parameters Supported	None	CIC	all	
Non-standard MIME type	None		all	
SIP Header format	Compact	Compact or Long	Compact or Long	Compact or Long
Use OPTIONS for Heartbeat	Yes	Yes	Yes	
Telephony Profile Support	Yes	Yes	Yes Or No	

Field	SST to MCS	SST to VRDN	SST to SST	SIP-based voice mail server
Long Call Audit Mechanism	INFO	Yes	NONE	
Accepts Early SDP	No	Yes	Yes Or No	
	Setting Enhanced Media Cut Through field to 'Y' will nullify the field Accepts Early SDP. If Overlap mode is enabled in core table TRKSGRP, field OVLAP, then Accepts Early SDP should be set to 'N' and ensure that Accepts Encapsulated ISUP is set to 'Y'.			
Accept Invite without SDP	Yes	Yes	Yes	
E.164 Format Allowed	Yes	No	Yes	
	Setting this field to 'Y' requires datafilling the Country Code Supported field to '1'.			
Validate Request URI	No			
Enforce CODE C-Compatibility	No	No	Yes Or No	
	Setting this field to 'Y' requires selection of at least one applicable codec in the 'Config Date' section.			
T.38AnnexD Supported	No	No	Yes Or No	No
Accepts Encapsulated ISUP	No	Yes	Yes Or No	
	Setting this field to "N" requires setting the Accepts Early SDP field to "N" Setting both these fields to "N" indicates support for Sip (without ISUP payload) in an SST-to-SST configuration.			
Conn Mode Allowed	Yes	Yes	No	
OCN Allowed	No	Yes	No	
Re-Invite for Voice Band Data	No	No	No	No
Enhanced Media Cut Through (EMCT)	Yes	No	Yes	Yes

Field	SST to MCS	SST to VRDN	SST to SST	SIP-based voice mail server
Auto-Subscribe	No	No	No	Yes
Retain Contact Info	No			
Country Code	1			
	Country Code must be set to '1' if the 'E.164 Allowed' field is set to 'Y'.			
Digit Prefix Used	Use the default unless otherwise specified	No	No	
Prefix Digit for International	Use the default unless otherwise specified	Use the default unless otherwise specified	Use the default unless otherwise specified	
Session Timer Value	20			
Out of Band DTMF Payload	vnd.nortelnetworks.digits	telephone-event	telephone-event	
Unknown Header	Any String	Any String	Any String	
Anonymous Header	Any String	Any String	Any String	
ServerIdentifier	Only for MCS 3.0 use CS 2000_NGSS/8.0 else use NONE			
SIP PSTN Interworking Options				
ISUP to SIP Cause Map	Default	Default	Default	Default
	You can add a custom ISUP - SIP cause map by clicking on the "ISUP and SIP Mappings" tab and adding a new mapping under the "ISUP to SIP Map".			
SIP to ISUP Cause Map	Default	Default	Default	Default
	You can add a custom SIP - ISUP cause map by clicking on the "SIP and ISUP Mappings" tab and adding a new mapping under the "SIP to ISUP Map".			
SIP Redirection Map	Default	Default	Default	Default
	You can add a custom SIP Redirection Map by clicking on the "ISUP and SIP Mappings" tab and a new mapping under the "SIP Redirection."			

Field	SST to MCS	SST to VRDN	SST to SST	SIP-based voice mail server
ISUP Variant to SIP Version Map	Default	Default When interworking with VRDN, add an entry with base/version of gr394/gr394 for any external protocol (such as Q764, NULL, NULL, gr394, gr394).	Default	Default
	ISUP Variant to SIP Version Map maps the ISUP Protocol/Version/Variant to the SIP base and Version fields. See table "Protocols, versions, and variants used for VRDN communication" (page 129) for different protocol variants that are required for communicating with VRDN configurations. For all other configurations, base/version entries are configurable.			
NOA/NPI to Phone Context Map	Default	Default	Default	Default
	For incoming SIP calls the Nature Of Address/Numbering Plan Identifier-to-Phone-Context Mapping table is used to determine the NOA/NPI values to be used in the ISUP message. Similarly, for outgoing calls, this table is used to determine the phone-context parameter to be added to Request-URI. The button "Phone-Context" (under URI-Parameters) must be turned "ON" for this functionality to take effect.			
SIP Cause Precedence Priority	Default (OR) Encap: Third Retry: Second CauseCode: First	Default	Any	
Backward Call Indicator (BCI) Data	(I) networking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN	(I) networking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN	(I) networking Encountered (K) ISUP Not used All the Way (M) Terminating Access is not ISDN	

Field	SST to MCS	SST to VRDN	SST to SST	SIP-based voice mail server
Forward Call Indicator (FCI) Data	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access is not ISDN	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access is not ISDN	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access is not ISDN	
Hop-Count Factor	2	7	7	
	For SST to MCS, Hop-Count Factor should be configured based on the MCS configuration. Please check the MCS's Initial Maximum Hop Value, and then set the HOP-Counter field based on the MCS configuration. See the *Nortel Session Manager Fundamentals* (NN10029-111), for assistance with determining the Hop Count value set on the MCS.			
Trunk Group ID Prefix	Default	Default	Default	

Configuring SIP Gateway application parameters

Purpose of this procedure

Use the following procedure to change provisioning parameters for an existing SIP Gateway application.

Limitations and restrictions

If the SIP Gateway application is in-service when the following listed values are changed, the application must be taken out of service (suspended) and brought back to an in-service state (unsuspended).

- generalLingerTimer
- inviteLingerTimer
- localTCPport
- localUDPport
- maxCallLegs
- maxSIPMsgSize
- maxSubscrIPtion
- provisionalTimer
- retransmissionT1
- retransmissionT2
- retransmissionT4
- retryCount
- subAutoRefresh
- supportedExtensionList

When upgrading from VRDN to SST, the mgcHostName must match the HOST_MGCNAME parameter in table OFCENG in the CS 2000. Once the upgrade is complete, the IP address of the remote SST (or MGCINV if VRDN is used) should be changed to the newly provisioned SST IP address.

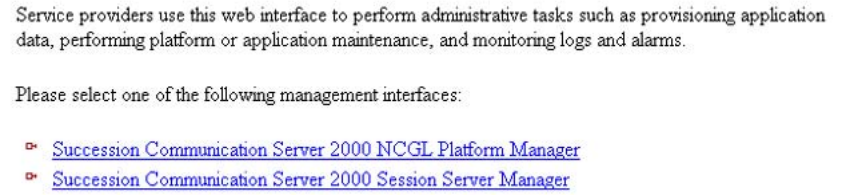
Prerequisites

There are no prerequisites for performing this procedure.

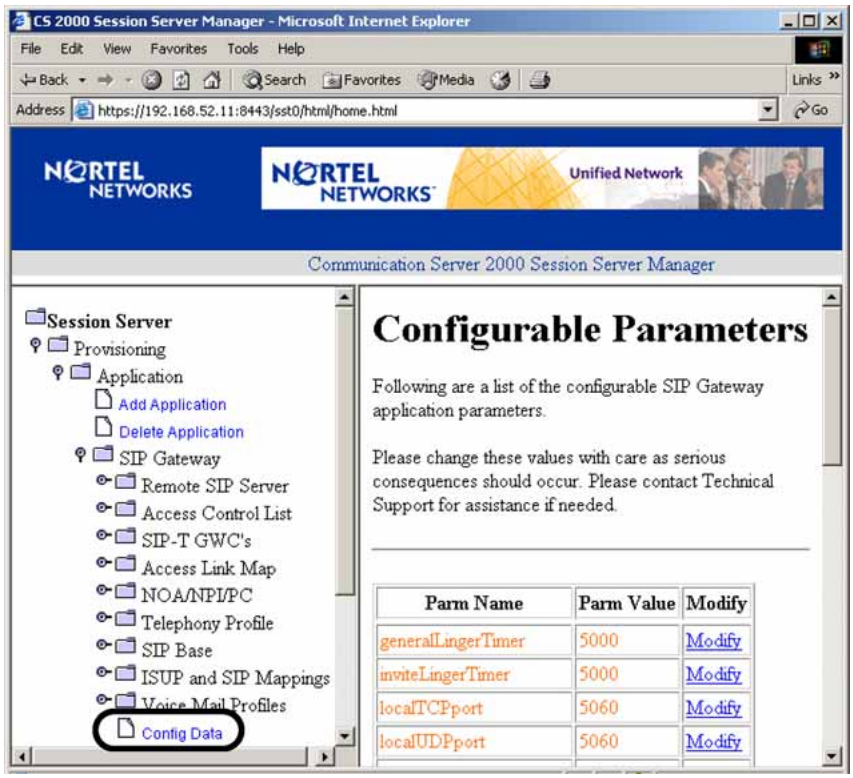
Action

Step	Action
	At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.

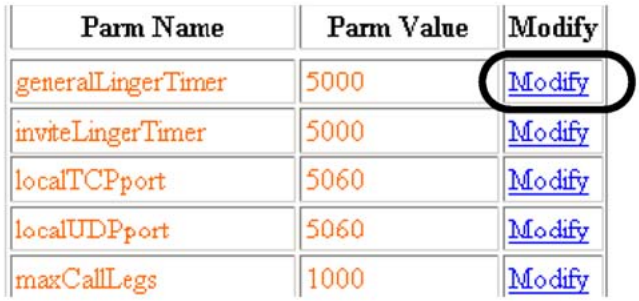


2 At the Session Server folder, click the **Provisioning > Application > SIP Gateway > Config Data**.



The Configurable Parameters page opens in the right side frame.

3 Click the **Modify** link to the right of the Parm Value to change.



Parm Name	Parm Value	Modify
generalLingerTimer	5000	Modify
inviteLingerTimer	5000	Modify
localTCPport	5060	Modify
localUDPport	5060	Modify
maxCallLegs	1000	Modify

The Configuration Data page opens in the right side frame.

4 Type a new value in the field and click **Change**. Refer to "Additional Information" (page 48) for a reference to the valid range and type of values for each parm value.

ATTENTION

Changes to fields shown in orange in the GUI take effect only after call processing is restarted, in which case Nortel recommends that you restart CallP by executing a double WARM SWACT. This process ensures that active calls stay connected, while alerting calls are dropped. Refer to the next step in this procedure.

Changes to fields shown in green in the GUI take effect immediately after the change is applied.

5 If applicable, perform a double WARM SWACT to force any new parameter values to take effect. That is, twice in succession repeat the procedure "Invoking a maintenance SWACT of the SST platform" in *Session Server Trunks Security and Administration* (NN10346-611).

—End—

Additional Information

Use the following table to assist you in modifying the Configuration Data table using the recommended values and ranges:

Enforcement of all field values and ranges is handled by the database.

For all Boolean (Y/N) fields, the case (upper or lower) for the variable is preserved as entered.

Parameter Name	Description	Recommended Value and Range
numAuditTimeInterval	This parameter controls the time interval between execution of SST callp audits.	Range = 180 to 18000 Default = 390 Recommended = 390
expeditedAuditThreshold	This parameter provides a percentage threshold used to determine when the expedited audit is triggered. The SST call audit enters expedite mode when the number of audit failures within an audit cycle exceeds the threshold percentage of audited calls.*ThresholdCount=(ExpeditedAuditThreshold)/100*(number of calls audited in the previous cycle)*	Range = 1 to 100 Default = 390 Recommended = 10
generalLingerTimer	After the SST sends a final response, it cannot be sure that the client gateway device has received the response message. The SST should be able to retransmit the response upon receiving retransmissions of the request for <generalLingerTimer value> milliseconds.	Range = 0 to 60000 Default = 5000 (milliseconds)
inviteLingerTimer	After sending an ACK for an INVITE final response, a SIP Gateway client device cannot be sure that the SST has received the ACK message. The client should be able to retransmit the ACK upon receiving retransmissions of the final response for <inviteLingerTimer value> milliseconds.	Range = 0 to 60000 Default = 5000 (milliseconds)
localTCPport	The local TCP port on which the SIP Stack listens. localTCPport can be configured for SST-to-SST calls.	Range = 1024 to 65534 Default = 5060
localUDPport	The local UDP port on which the SIP Stack listens. localUDPport can be configured for SST-to-SST calls.	Range = 1024 to 65534 Default = 5060
maxCallLegs	The maximum number of call-legs the SIP Stack allocates and expects to handle simultaneously. ***Note:*** This value must match the sum of the usage limit values found in both SOC CS2B0008 and SOC CS2B0009 call types.	Range = 0 to 50000 Default = 1000

Parameter Name	Description	Recommended Value and Range
maxSIPMsgSize	Indicates the maximum size (in bytes) that the SIP message header can be. If interworking with a Nortel MCS system, set this value to 2048.	Range = 500 to 4000 Default = 1536 Recommended = 2048
numGCPAuditMsgsPerCycle	Controls the maximum number of audit related GCP messages sent to the DPT GWCs within one audit cycle. Setting this value too low results in the possibility of not detecting stuck resources in a timely manner due to an insufficient number of calls being audited in a cycle.	Range = 10 to 500 Default = 250 Recommended = 250
numSIPAuditMsgsPerCycle	Controls the maximum number of audit related SIP messages sent SIP endpoints within one audit cycle. Setting this value too low results in the possibility of not detecting stuck SIP sessions in a timely manner due to an insufficient number of calls being audited in a cycle.	Range = 10 to 500 Default = 250 Recommended = 250
maxSubscrIPtions	The number of subscrIPtions the SIP Stack allocates. You should set this value to the maximum number of subscrIPtions that you expect the SIP Stack to handle simultaneously. The default (0) means that subscrIPtions are not supported. ***Note:*** This value must match the value in field maxCallLegs.	Range = 0 to 100 000 Default = 1000
provisionalTimer	When a client gateway device receives a provisional response, it continues to retransmit the request, but with an interval of <provisionalTimer value> milliseconds. If you set the provisional timer to zero (0), no timer is set.	Range = 0 to 540000 Default = 180000 (milliseconds)
retransmissionT1(timer)	T1 determines several timers as defined in RFC3261. For example, When an unreliable transport protocol is used, a 'Client Invite' transaction retransmits requests at an interval that starts at T1 milliseconds and doubles after every retransmission. A 'Client General' transaction also retransmits requests at an interval that starts at T1 and doubles until it reaches T2.	Range = 0 to 60000 Default = 2000 (milliseconds)

Parameter Name	Description	Recommended Value and Range
retransmissionT2(timer)	T2 Determines the maximum retransmission interval as defined in RFC 3261. For example, when an unreliable transport protocol is used, general requests are retransmitted at an interval which starts at T1 and doubles until it reaches T2. If a provisional response is received, retransmissions continue but at an interval of T2.	Range = 0 to 60000 Default = 4000 (milliseconds)
retransmissionT4(timer)	T4 represents the amount of time the network takes to clear messages between client gateway device and SST transactions as defined in RFC 3261. For example, when working with an unreliable transport protocol, T4 determines the time that a client call agent or client manager (example: the Centrex IP Client Manger) waits after receiving an ACK message and before terminating the transaction.	Range = 0 to 60000 Default = 5000 (milliseconds)
retryCount	Used for SIP Gateway application configuration.	Range = 0 to 7 Default = 6
subsRetryTmr	Determines the interval between attempts to send a SUBSCRIBE message to voice mail remote SIP servers. 0 indicates not to retry.	Range = 0 to 50 000 Default = 6000 (milliseconds)
codecG726Allowed	These 4 audio codecs are for use with the Enforce CODEC-Compatibility field on the Remote SIP server page. At least one of these codecs must be set to Y if Enforce CODEC- Compatibility field is set to Y. Refer to procedure "Configuring Remote SIP Servers" (page 26).	Default = N
codecG729Allowed		Default = N
codecPCMUAllowed		Default = N
codecPCMAAllowed		Default = N
	Note 1: codecG726Allowed must be set if 'codec-enforcement' is turned on for the server.	
	Note 2: codecG729Allowed must be set if 'codec-enforcement' is turned on for the server.	
	Note 3: codecPCMUAllowed must be set if 'codec-enforcement' is turned on for the server.	
	Note 4: codecPCMAAllowed This must be set if 'codec-enforcement' is turned on for the server.	

Parameter Name	Description	Recommended Value and Range
enableAccessControlList	Enables the capability to configure a valid range of IP addresses and netmasks that SIP servers may use to contact the SST SIP Gateway Application. Refer to procedure "Adding and managing SIP server IP address access control lists" (page 58). If this value is set to "Yes", ensure ALL the IP addresses the SST communicates with are listed in the Access Control List as shown in procedure "Adding and managing SIP server IP address access control lists" (page 58). IP addresses that are datafilled in Remote Server Page area automatically are part of the list. For example, when communicating using the VRDN implementation, ensure the IP addresses of all the communicating SIP-T GWCs are listed, otherwise, call processing does not work.	Default = N
mgcHostName	**CAUTION** Using special characters other than the '-' and '.' for mgcHostName and HOST_MGCNAME may cause conflicts with third-party vendor equipment that strictly adheres to the RFC recommendation. mgcHostName is the FQDN (fully-qualified domain name) network name of the SST node. mgc_hostname can be up to 64 alphanumeric characters. This value must exactly match the value in core table host_mgcname and must also match the common name used when creating self-signed or CA-signed security certificates. Refer to *Session Server Trunks Security and Administration* (NN10346-611) for procedures on generating security certificates.When upgrading from VRDN to SST, the mgcHostName must match the HOST_MGCNAME parameter in table OFCENG in the CS 2000. Once the upgrade is complete, the IP address of the remote SST (or MGCINV if VRDN is used) should be changed to the newly provisioned SST IP address.	Default = null

Parameter Name	Description	Recommended Value and Range
subsAutoRefresh	Specifies whether to send a refresh SUBSCRIBE request when the subscrIPtion is going to be expired. Using the default value (N for No) specifies that the refreshing request is not sent automatically.	Default = N
supportedExtensionList	The list of supported option-tags, separated by commas, which are supported by the SIP Stack. The list is added to a Supported header for outgoing messages. The default value (null) adds an empty list.	Default = 100rel, replaces

Configuring an NCAS link

Purpose of this procedure

Use this procedure to add or modify a Non Call Associated Signaling (NCAS) link between the SST and the CS 2000 or CS 2000 - Compact.

Limitations and restrictions

The digit manipulation in Table MSGRTE is designed to work on the route info for the messages. For the SCTP selector, the route info has no meaning. Therefore, the digit manipulation in Table MSGRTE should not be used with the SCTP selector.

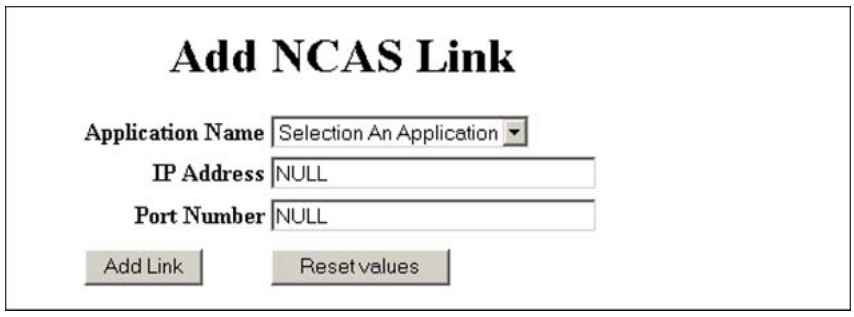
Prerequisites

Before performing this procedure:

- enter provisioning in tables NETNAMES, IPAPPL, and MSGRTE, record the port number identified in IPAPPL
- enable Software Optionality Code (SOC) MDC00078
- determine the IP address of the CS 2000 CMHOST 0 or CMHOST 1, or, for CS 2000 Compact, the activeirm IP address

Action

Step	Action
	At the CS 2000 Session Server Manager
1	Select **Provisioning > Application > NCAS Link > Add NCAS Link** from the left side menu. To modify and existing NCAS link, select **List NCAS Links** from the left side menu, and then the Modify URL in the right side frame for the link to modify. *The Add NCAS Link web page opens in the right side frame.*



2 Enter the provisioning data, refer to the following table:

Field	Description	Value
Application Name	This field controls is the link is used for message waiting indicator control, or if the link is used for out of band refer to interoperate with MCS 5200 Session Manager.	Message Waiting if used for voice mail. Out Of Band Refer if used for MCS 5200 interoperability.
IP Address	The IP address of the host at the other end of the NCAS link.	Enter the IP address of the CS 2000 HIOP or CS 2000 - Compact activeirm.
Port Number	Port number on the remote host.	Enter the port number identified in table IPAPPL. This value must be between 4900 and 4981.

3 Click **Add Link**.

The page refreshes and reports that the link was added successfully.

The link can be viewed by selecting List NCAS Links from the left side menu. Maintenance on the link is performed by selecting **Maintenance > Application > NCAS Link** *from the left side menu.*

—End—

Additional information

When the NCAS links are listed, the state of each link is reported. Status is one of:

- Stopped -- The link is not connected and no communication exists.
- TryingToConnect -- The link is not connected, but attempts are in progress. This state occurs under the following conditions:
  - — link is provisioned in the SIP Gateway application, but not datafilled in table IPAPPL in the CS 2000
  - — maintenance activity is in progress on the CS 2000
  - — the communication route has trouble such that no data can be transferred between the SIP Gateway application and CS 2000
- Connected -- The link is connected and communication exists.

Configuring a voice mail profile

Purpose of this procedure

This procedure is used when configuring the SIP Gateway application to support SIP network message waiting service (NMS) based on RFC 3842. When this procedure is complete, a range of directory numbers (DN) are associated with a remote SIP server for NMS. This procedure must be performed for all remote SIP servers that the CS 2000 will provide MWI status to.

Limitations and restrictions

There are no limitations or restrictions.

Prerequisites

Perform the following procedures before beginning this procedure:

- Ensure that tables NETNAMES, IPAPPL, and MSGRTE are provisioned on the CS 2000 or CS 2000 - Compact.
- "Configuring an NCAS link" (page 54) and ensure the link is in the Connected state.
- Know the range of DNs served by the remote SIP server.

Action

Step	Action

At the CS 2000 Session Server Manager

1 Select **Provisioning > Application > SIP Gateway > Voice Mail Profiles > Add VM Profile** from the left side menu.

To List the existing profiles, click List VM Profiles. To modify a profile, list it, delete it, and add it with the new parameters.

The Add Voice Mail Profile web page opens in the right side frame.

2 Refer to the following table for provisioning information:

Field	Description	Value
Remote SIP Server	The identity of the remote SIP server.	Pull down menu listing of remote SIP servers.

Field	Description	Value
Starting DN	Ten digit directory number indicating the beginning of the range.	
Ending DN	Ten digit directory number indicating the end of the range.	

3 Click **Add**.

The page refreshes and the entry is added to the list of Voice Mail Profiles.

When the SST node receives a MWI message from the CS 2000 over an NCAS link, the SST parses the message for the DN and then generates a SIP message to the remote SIP server that serves the appropriate DN range.

—End—

Adding and managing SIP server IP address access control lists

Purpose of this procedure

Use the following optional procedure to create an access control list (ACL) and configure a valid range of IP addresses and netmasks that SIP servers may use to contact the SIP Gateway Application.

Enabling Access Control List (ACL) will mitigate the risk of potential Denial of Service attacks. Please ensure to add only trusted and authenticated IP addresses to the ACL.

Limitations and restrictions

IP restriction for SIP server addresses is an optional parameter and can be turned off and on using the Configuration Data menu.

The SIP Gateway application supports multiple ranges in the access control list, allowing multiple IP address ranges.

SIP server IP addresses are added to the access control list automatically, regardless of whether they show up in the GUI immediately after being added.

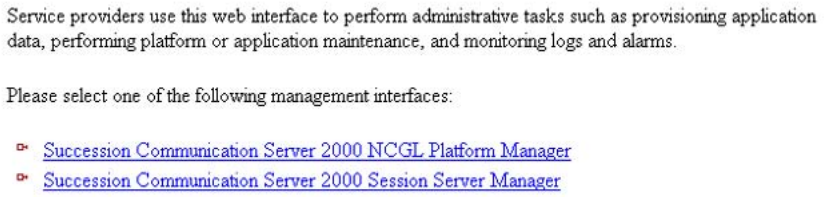
Remote servers that are provisioned in the database cannot be listed using "List IP Ranges" link. Once the IP ranges are displayed, you can choose to delete a particular IP range.

Prerequisites

IP restriction for SIP server addresses is an optional parameter and must be turned off and on using the Configuration Data menu. Refer to procedure "Configuring SIP Gateway application parameters" (page 46).

Action

Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.

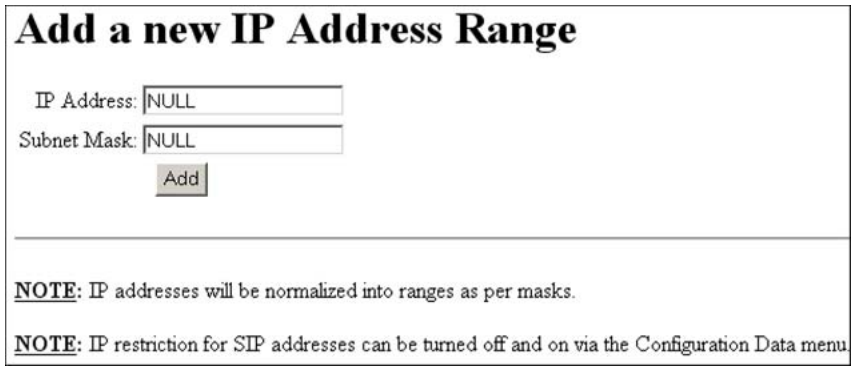


2 Select **Session Server > Provisioning > SIP Gateway > Access Control List** from the left side menu.

3 Use the following table to determine your next step:

If	Do
you are adding an IP address range to the Access Control List	step 4
you are viewing a list of existing IP address ranges in the Access Control Lists currently in the database	step 8
you are deleting an IP address range from the Access Control List	step 14
you are finished with this procedure	step 13

4 Click **Add IP Range** in the left side menu.



5 Datafill the IP address range and subnet values

- IP Address -- for example, 10.0.8.0
- Subnet Mask -- for example, 255.255.255.0

The range of IP addresses to allow is calculated based on a combination of the IP address and network mask entered. If conjugating with a VRDN GWC on another switch, ensure that the IP addresses for SIP-T GWCs on the other switch are entered here.

ATTENTION

IP addresses are normalized into ranges as per the subnet masks.

While an IP address can be entered more than once, an IP address/subnet mask combination cannot be entered into the system more than once.

6 When you have verified that the information is correct, click the **Add** button.

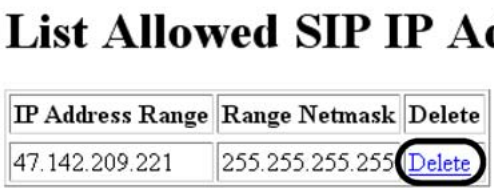
7 Use the following table to determine your next step:

If	Do
you want to add more IP address ranges	return to step 4
you want to view a list of existing Access Control Lists	skip to step 8
you want to delete a range IP addresses	skip to step 9

8 If you want to view a list of existing Access Control Lists, click the **List IP ranges** link. Otherwise skip to the last step.

The List Access Link Maps page is presented.

9 If you want to delete an IP range for a specific remote server, click the **List IP ranges** link. Otherwise skip to the last step.



10 Click the **Delete** link next to the IP address/netmask range you want to remove from the database.

Ensure that any SIP servers that use this address range are not in use. If you attempt to delete an address range that is in use, the request is denied by the system.

The system responses:

```
Do you really wish to delete IP address
<IP_address>?
```

11 Click **OK** to confirm the deletion of the address range.

12 Return to step 3 if you want to make other changes to other Remote SIP Servers, otherwise continue with step 13.

13 Remember to set parameter enableAccessControlList to Yes in the Config Data.

—End—

Adding and managing SIP-T GWCs

Purpose of this procedure

Use the following procedure to add, delete, modify parameters for or list the SIP-T GWCs used for DPT (dynamic packet trunking) calls for the SIP Gateway application.

Limitations and restrictions

CAUTION
Possible loss of service
Deleting a SIP-T GWC entry from the database that is being used for SIP call processing may result in a service outage. Before deleting a SIP-T GWC, ensure that it is not being used for call processing services.

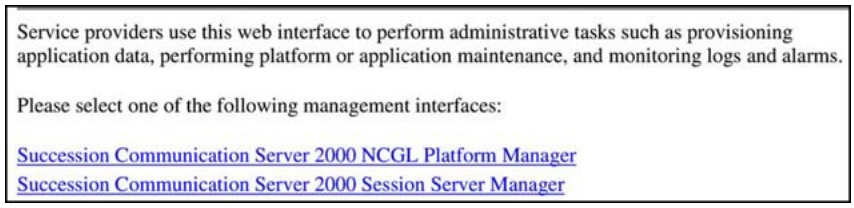
Prerequisites

SIP-T GWCs must be provisioned in the GWC Manager database. Refer to procedures in the *Nortel Gateway Controller Configuration Management* (NN10205-511) to determine if SIP-T GWC types have already been provisioned.

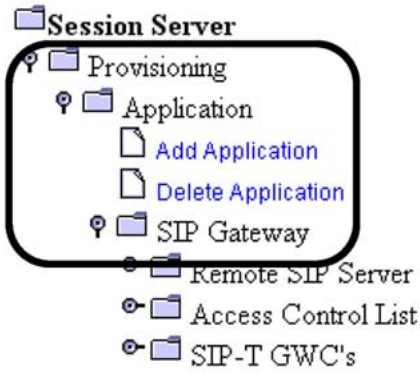
In a Multi-SST configuration, all DPT GWCs in use for SST calls need to be provisioned on all SST nodes carrying SIP calls on the CS 2000. The shared GWCs report the state of inservice where the link status of the last GWC to report is enforced. Provisioning all the DPT GWCs on all SST nodes is necessary to ensure correct reporting of the SST associated trunk states.

Action

Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



2 At the Session Server folder, click the **Provisioning folder**, then the **Application** folder and finally the **SIP Gateway** folder.



3 Click on the **SIP-T GWC** folder. A list of SIP-T GWCs currently in the SIP Gateway application database (if any) is shown.

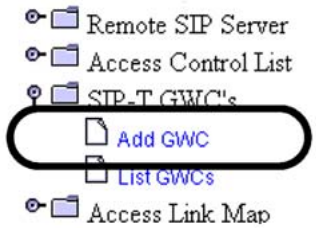
4 Click **List GWCs** to list all SIP-T GWCs existing in the SIP Gateway application database.

5 Use the following table to determine your next step:

If	Do
you are adding a SIP-T GWC to the SIP GW Application database	step 6
you are modifying a SIP-T GWC already listed in the SIP GW Application database	step 10
you are deleting a SIP-T GWC from the SIP GW Application database	step 14

6 Click the **Add** GWC link to add a new SIP-T GWC to the list of dynamic packet trunking GWCs available for use.

If no SIP-T GWCs are available for use, you must add them into the GWC Manager database. Refer to procedure Adding and configuring a GWC node, found in the *GWC Configuration Management* (NN10205-511).

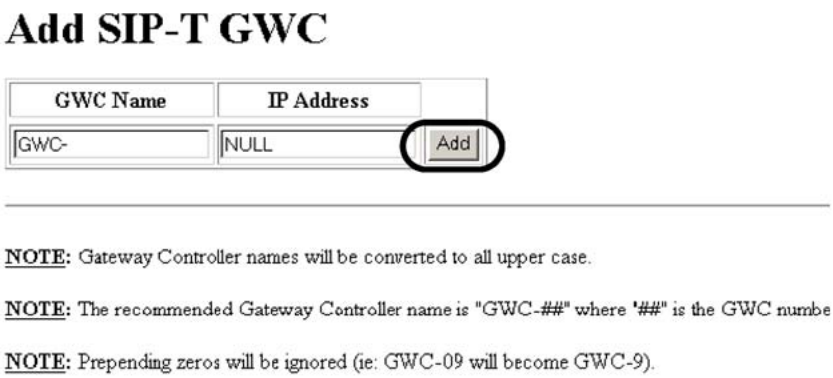


7 Datafill the GWC name and IP address of the active GWC unit in the GWC node, then click the **Add** button.

ATTENTION
GWC names and GWC IP addresses cannot be reused.

The required format for the Gateway Controller name is "GWC-##" where "##" is the GWC number. Prepended zeros in the GWC name are ignored. GWC names are converted to all upper case.

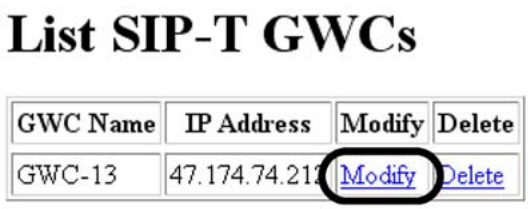
Example: gwc-09 becomes GWC-9. You can determine the correct IP address and name of the active GWC node by referring to procedure "Viewing GWC node characteristics," found in the *GWC Configuration Management* (NN10205-511).



8 If you want to add more SIP-T GWCs to the database, return to step 6, otherwise return to step 5.

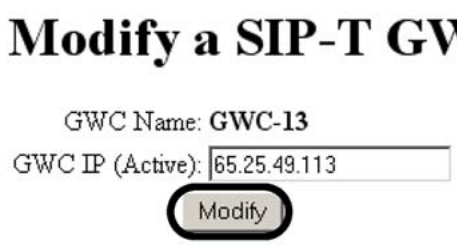
9 Click **List GWCs** to list all SIP-T GWCs existing in the SIP Gateway application database.

10 Click the **Modify** link for the SIP-T GWC entry you want to change the active GWC IP address for.



11 Datafill the new IP address of the active GWC unit in the GWC node, then click the **Modify** button. Only the IP address of the GWC can be changed.

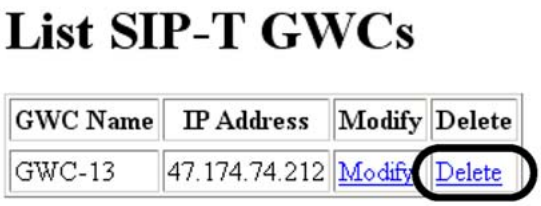
The IP address entered must match the logical IP address for the *active* GWC card (not the GWC unit IP address) in the GWC node as shown in the Provisioning panel of the CS 2000 GWC Manger GUI. Refer to "Viewing GWC node characteristics," found in the *GWC Configuration* (NN10205-511).



12 If you are finished modifying SIP-T GWCs in the SIP Gateway application database, return to step 10, otherwise return to step 5.

13 Click **List GWCs** to list all SIP-T GWCs existing in the SIP Gateway application database.

14 Click the **Delete** link next to the SIP-T GWC you want to delete from the SIP Gateway application database.



Ensure that any SIP-T GWCs that you want to delete are not in use. If you attempt to delete a GWC that is in use, a service outage may occur.

The system responses:

```
Do you really wish to delete GWC <GWC-nn>?
```

15 Click **OK** to confirm deleting the GWC, otherwise click **Cancel** to abort the deletion.

16 If you want to delete other SIP-T GWCs from the database, return to step 14.

—End—

Adding and managing telephony profiles

Purpose of this procedure

Use the following procedure to create (add) a telephony profile to the SIP Gateway application database and to manage existing telephony profiles. A telephony profile is a simple character string or numerical Trunk Group ID Prefix that is mapped to a SIP Access Link, as defined in core table SIPLINK, and a Remote SIP Server that the trunks terminate on.

Limitations and restrictions

If adding a new telephony profile, Refer to "Adding DPT trunk group connections handled by SST" (page 13) to ensure that all prerequisite activities have been completed.

When adding a telephony profile, ensure that the same name/numeric is used on both the near-end office (the office with the SST installed) and the far-end office for the interconnecting SIP trunks. For instance:

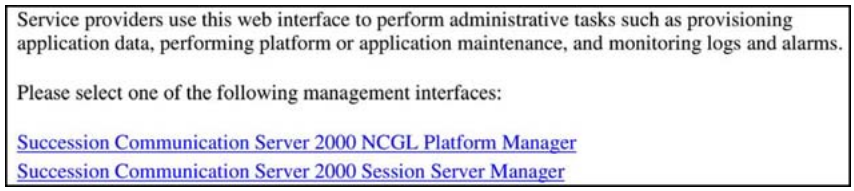
- In the case where you are interconnecting an SST with a VRDN SIP Gateway, the Telephony Profile name entered must match the name of the Telephony Profile defined in core table TELEPROF on the far end office.
- In the case where you are interconnecting between two SST (on different networks), then the Telephony Profile names must match one another as defined on the Telephony Profiles table on this web page and used in the Access Link MAP table, as shown in procedure "Adding and managing Access Link Maps" (page 73).
- In the case where you are using a Trunk Group ID Prefix, the character length of the Telephony Profile must be equal to the value of the Trunk Group ID Prefix parameter defined in the Remote SIP Server.

Prerequisites

Complete this procedure before procedure "Adding and managing Access Link Maps" (page 73).

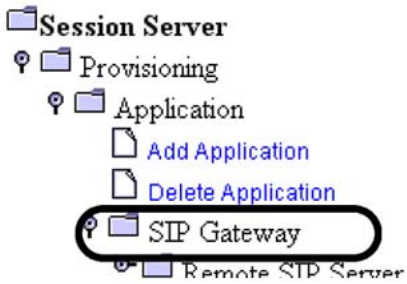
Action

Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.

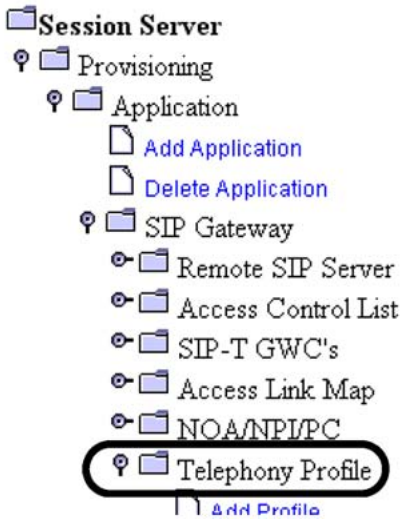


2 At the Session Server folder, click the **Provisioning folder**, then the **Application** folder.

3 Click on the **SIP Gateway** folder to open the folder.



4 Click on the Telephony Profile link to open it.



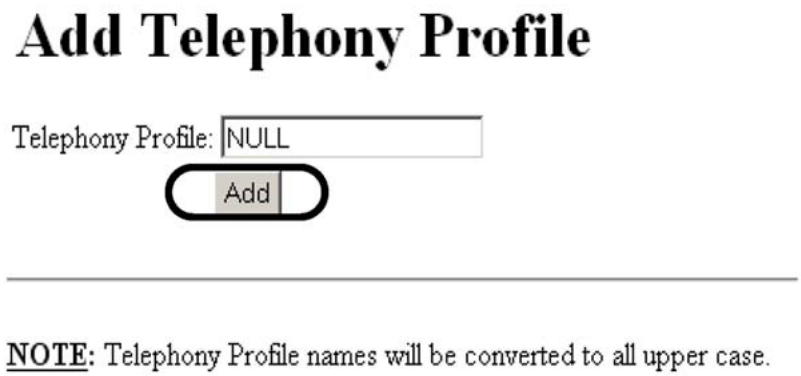
5 Use the following table to determine your next step:

If	Do
you are adding a Telephony profile to the SIP GW Application database	step 6
you are listing or deleting a Telephony profile from the SIP GW Application database	step 9

6 Click the **Add Profile** link.

7 Enter a telephony profile name, up to 32 alphanumeric characters, or Trunk Group ID Prefix (refer to "Recommended or default Remote SIP Server provisioning parameters" (page 31) for the required string length as defined by the Trunk Group ID Prefix parameter), and click the **Add** button.

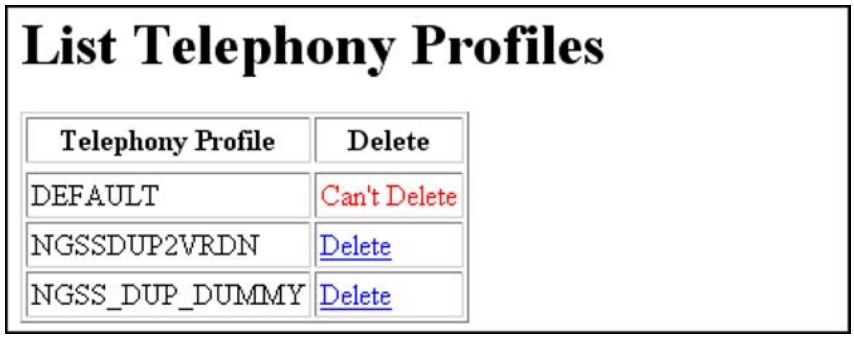
Telephony profile names, with the exception of Trunk Group ID Prefixes, should start with TP. To avoid confusion, do not use the same name for trunk names, telephony profile names and SIP link names.



8 Return to step 6 if you want to create additional telephony profiles, otherwise return to step 5.

9 Click on the **List Profiles** link.

10 Review the list of available telephony profiles.



11 If you want to delete a profile, click the **Delete** button to the right of the profile to be deleted, otherwise return to step 3.

You cannot delete the default telephony profile.

The system responds:

```
Do you really wish to delete Telephony Profile
<telephony profile>?
```

12 Click **OK** to confirm deleting the profile.

13 Return to return to 5 if you are finished deleting profiles.

—End—

Adding and managing Access Link Maps

Purpose of this procedure

Use the following procedure to set up and manage the Access Link Map page, used to set up the routing of incoming and outgoing SIP calls. Access Link Maps show the relationship between the Link Name defined in core table SIPLINK, the Telephony Profile and Remote SIP server that terminates the trunk group.

Limitations and restrictions

Once the access link mappings are listed, modifications to the mappings are not allowed. You must delete a particular mapping and then re-add it with the changes.

In a office with multiple SST nodes, link names should not be duplicated between SST nodes (in the access link mappings tables), otherwise undesirable behavior may result.

Prerequisites

If adding a new link map for use with a new trunk group, first see "Adding DPT trunk group connections handled by SST" (page 13) to ensure that all prerequisite activities have been completed.

A link map to a remote SIP server must not be in use by the SIP Gateway application. A new link map should first be configured to ensure that routing of outgoing and incoming SIP calls to the remote SIP server is maintained.

CAUTION
This is a service affecting procedure. Improperly removing a link map from the SIP Gateway application database may interrupt all SIP media communications.

Ensure that the following procedures have been executed before using this procedure:

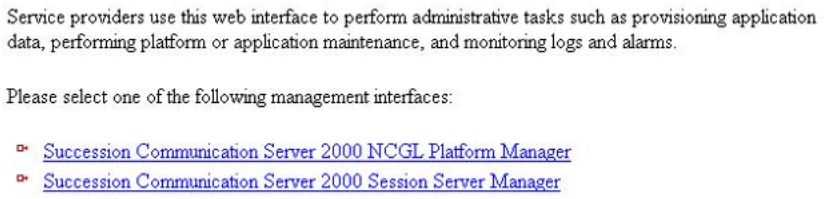
- Refer to *Nortel Installation Method SST Commissioning*, IM 24-0122, for instructions to ensure that core table SIPLINK is properly datafilled. Table SIPLINK provides link names needed to complete this procedure.
- Use procedure "Adding and managing telephony profiles" (page 68) to ensure that a telephony profile is available.
- Use procedure "Configuring Remote SIP Servers" (page 26) to ensure that a remote SIP server is available.

Action

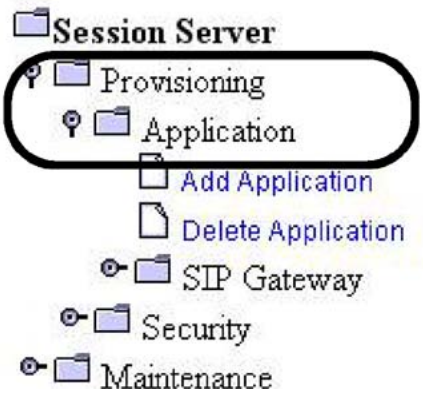
Step	Action

At the CS 2000 Session Server Launch Point

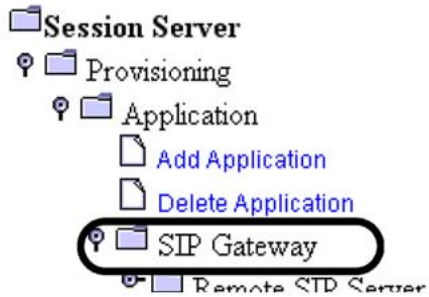
1 Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



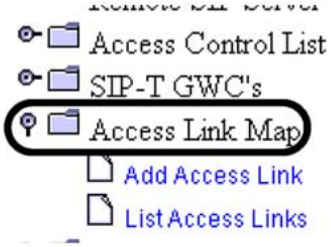
2 At the Session Server folder, click the **Provisioning folder**, then the **Application** folder.



3 Click on the **SIP Gateway** folder to open the folder.



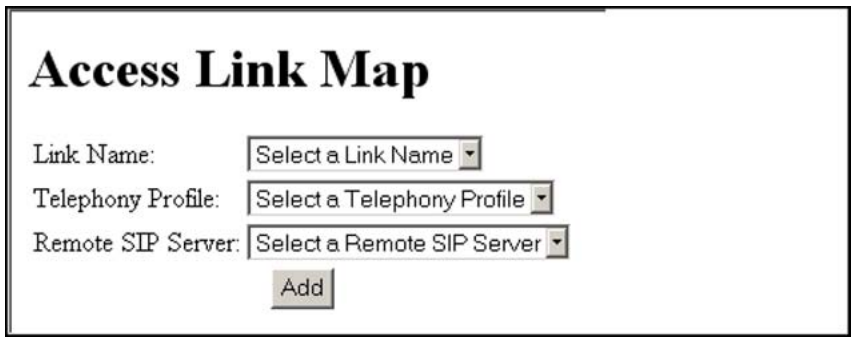
4 Click on the **Access Link Map** link to open it.



5 Use the following table to determine your next step:

If	Do
you are adding an Access Link map to the SIP Gateway application database	step 6
you are listing existing Access Links in the database	step 10
you are deleting an Access Link Map from the SIP Gateway application database	step 12

6 Click the **Add Access Link** link.



7 Select the correct profile information when creating a new access link map:

- Select a link name from the drop down menu.

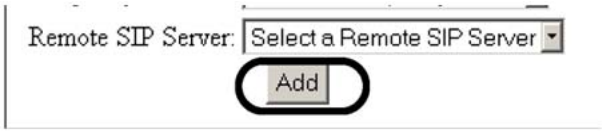
  The link name is derived from datafill in core table for each trunk group defined in table SIPLINK. Link names are created and updated in table SIPLINK through associations with SIP-based DPT trunk groups that are also datafilled in table TRKOPTS. The link information is passed on to the SIP-T GWCs provisioned in the GWC Manager database. After a SIPT-GWC is provisioned in the SIP Gateway application using procedure "Adding and managing SIP-T GWCs" (page 62), the SST sends an *mtc_discovery* message to the associated SIP-T GWC. The

associated SIP-T GWC then responds with information about available link names.

ATTENTION
Do not select a Link Name that is used by another SST node, otherwise undesirable behavior may result.

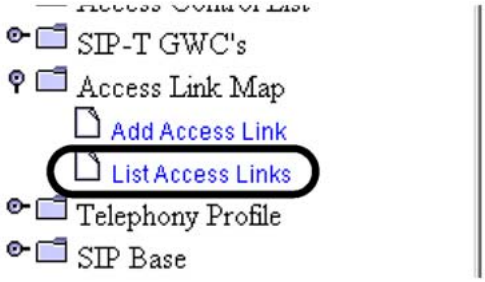
- Select a telephony profile from the drop down menu. Refer to procedure "Adding and managing telephony profiles" (page 68) if a telephony profile is unavailable.
- Select a remote SIP server from the drop down menu. If there are no remote SIP servers to choose, refer to procedure "Configuring Remote SIP Servers" (page 26).

8 Once all selections are made and verified as correct, click the **Add** button.

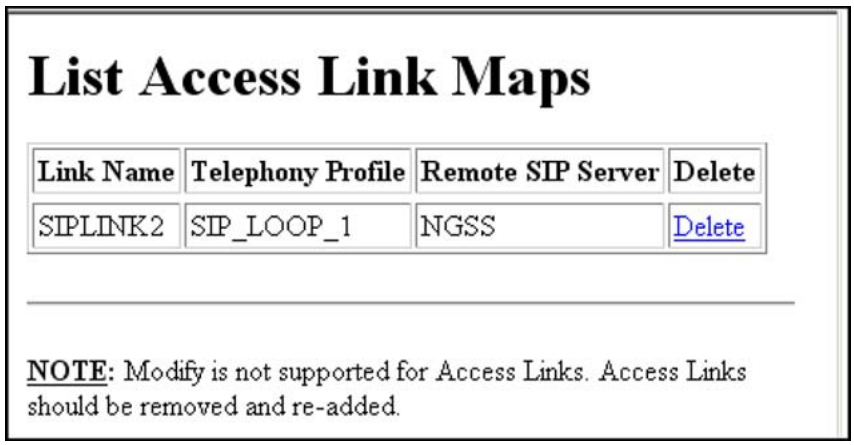


9 Return to step 6 if you want to create additional Access Link Maps, otherwise return to step 3.

10 If you want to list or delete an Access Link map, click the **List Access Link** link.



11 Review the list of available Access Link Maps.

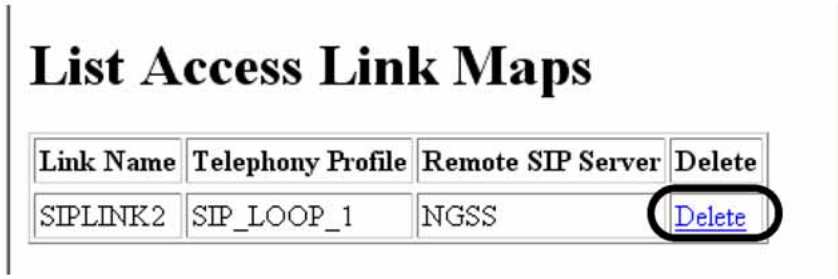


List Access Link Maps

Link Name	Telephony Profile	Remote SIP Server	Delete
SIPLINK2	SIP_LOOP_1	NGSS	Delete

NOTE: Modify is not supported for Access Links. Access Links should be removed and re-added.

12 If you want to delete an Access Link Map, click the **Delete** link, to the right of the entry, otherwise skip to the next step.



List Access Link Maps

Link Name	Telephony Profile	Remote SIP Server	Delete
SIPLINK2	SIP_LOOP_1	NGSS	Delete

13 If you want to make other changes to the Access Link Map page return to step 3, otherwise continue with the next step.

14 If you have added, modified or deleted any access link maps, then you may need to execute procedures "Suspending the SIP Gateway application" (page 167) and "Unsuspending the SIP Gateway application" (page 170) in the order listed to force any parameter changes or maps to take effect.

CAUTION
If the related SIP trunk is in the INB state, performing a Suspend and Unsuspend does not cause the trunk to go to in-service state.

Otherwise, the procedure is complete.

—End—

Adding and managing NOAs, NPIs, and Phone Context maps

Purpose of this procedure

Use the following procedure to create Phone Context maps, and to add, change or delete NOA (Nature of Address) and NPI (Numbering Plan Indicator) tuples from existing Phone Context (PC) maps.

Limitations and restrictions

The following restrictions apply to using this procedure:

- Any new Phone Context maps are created as identical to the selected base mapping, but can later be modified as needed. If the base map is empty of NOA mapping tuples then it must be populated.
- You cannot delete the DEFAULT Phone Context map.
- You cannot create new NOA tables. Only the existing NOA table can be modified by adding and deleting entries.
- NOA (Nature of Address) entries should be unique across all interconnected systems.
- Only user-defined Phone Context mappings can be deleted. System default PC mappings can not be deleted.
- Ensure that any PC maps or mapping tuples that you want to delete are not in use. If you attempt to delete a PC map or mapping tuple that is in use by a Remote SIP Server or the SIP Gateway application, the request is denied.
- It is not recommended that the same NOA name be used for multiple NOA numbers.

Prerequisites

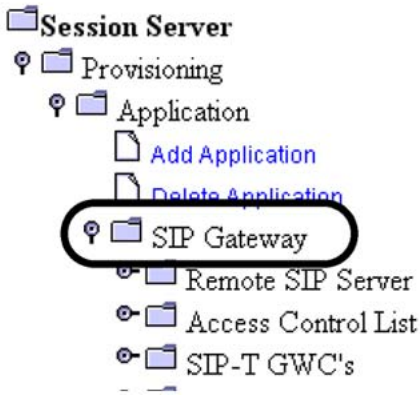
There are no prerequisites for performing this procedure.

Action

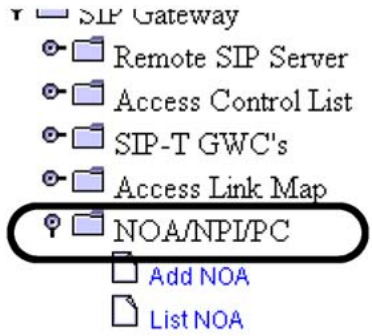
Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.

2 At the Session Server folder, click the **Provisioning folder**, then the **Application** folder.

3 Click on the **SIP Gateway** folder to open the folder.



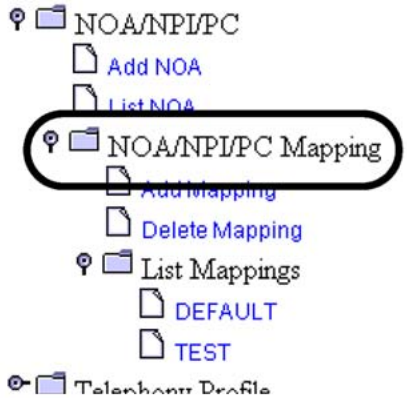
4 Click on the **NOA/NPI/PC** folder to open it.



5 Use the following table to determine your next step:

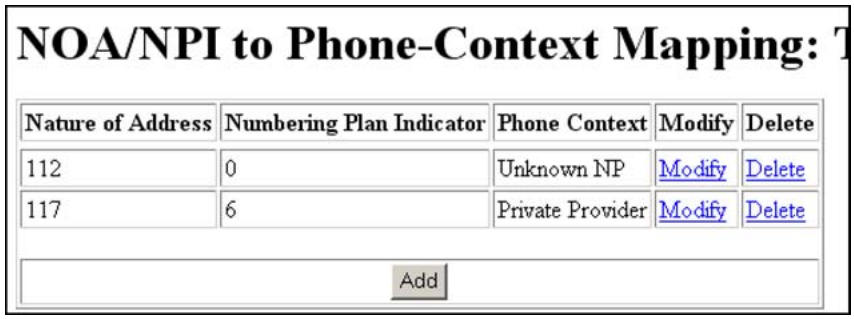
If	Do
you are listing contents for an existing Phone Context map	continue with step 6
you are modifying an existing Phone Context map	skip to step 10d
you are adding a new Phone Context map	skip to step 11
you are deleting an existing Phone Context map	skip to step 15
you are listing (reviewing) the contents of the NOA table	skip to step 19
you are deleting NOA entries from the NOA table	skip to step 22
you are adding an NOA entry to the NOA table	skip to step 10a

6 Click the **NOA/NPI/PC Mapping** link.



7 Click the **List Mappings** link and select the Phone Context map you want to review NOA/NPI-to-Phone Context tuples for.

8 Review the list of existing NOA/NPI tuples in the Phone Context mapping.



NOA/NPI to Phone-Context Mapping: T

Nature of Address	Numbering Plan Indicator	Phone Context	Modify	Delete
112	0	Unknown NP	Modify	Delete
117	6	Private Provider	Modify	Delete

Add

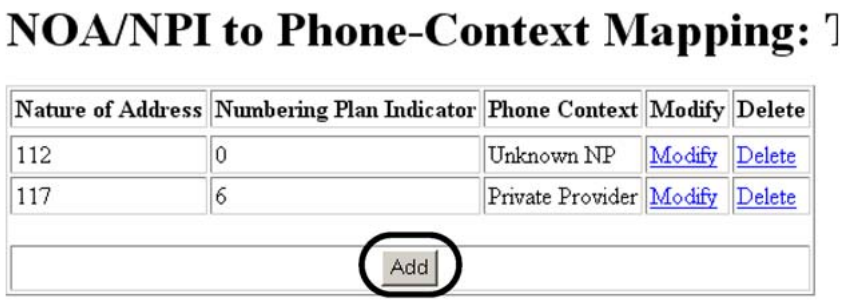
9 Use the following table to determine your next step:

If	Do
you are finished reviewing this Phone Context map	return to step 5
you want to add NOA-NPI tuples to the PC map	skip to step 10a
you want to modify NOA-NPI tuples for this PC map	skip to step 10d
you want to delete NOA-NPI tuples from this PC map	skip to step 10g
you are finished adding, modifying or deleting tuples for this PC map	skip to step 5

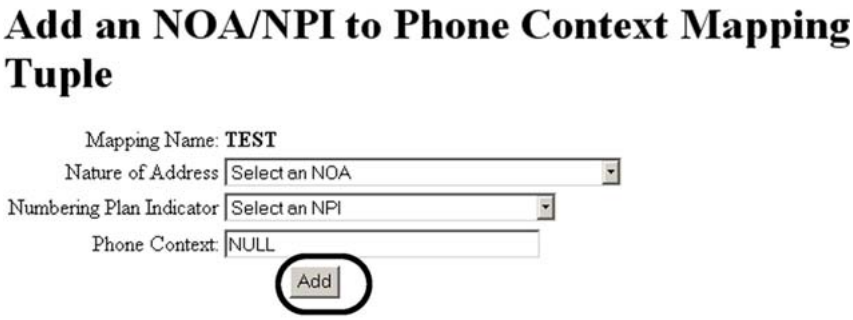
10 Use the following sub-steps to configure the selected Phone Context map.

a. To add a NOA/NPI tuple to the PC map, click the **Add** link below the table of listed tuples.

If this PC map is new, it may be empty of tuple content.



b. Using "Table of available NOAs and NPIs" (page 87), create a new NOA/NPI tuple by selecting the appropriate NOA and NPI values from the drop-down menus, then give the tuple a unique name. When you are finished making your selections, click the **Add** button.

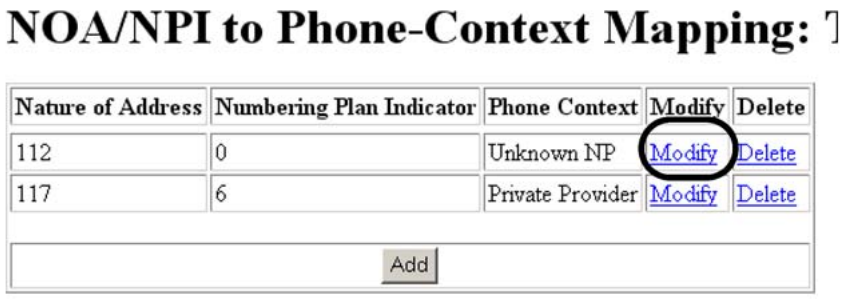


c. Return to a to add more tuples.

or

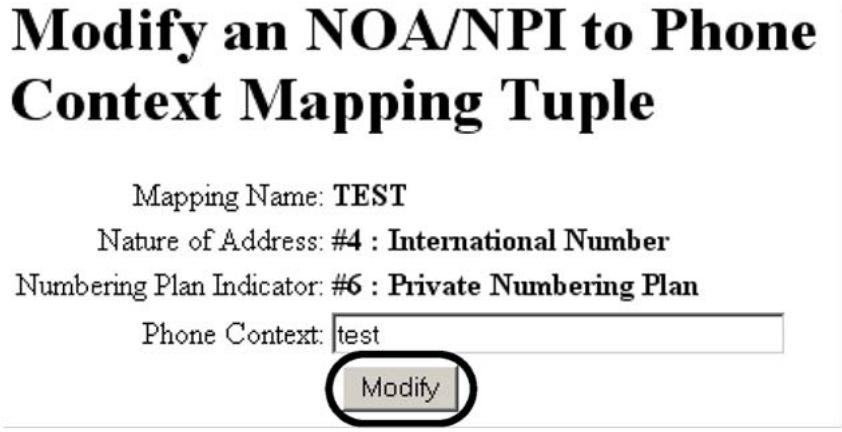
Return to step 9 when you are finished adding NOA/NPI tuples.

d. If you want to modify an NOA/NPI tuple in the existing PC map, click the **Modify** link to the right of the appropriate NOA/NPI tuple.



e. Use "Table of available NOAs and NPIs" (page 87) to assist you in modifying a NOA/NPI tuple, then click the **Modify** when you are finished. For each mapping tuple, you can modify:

- the phone context name

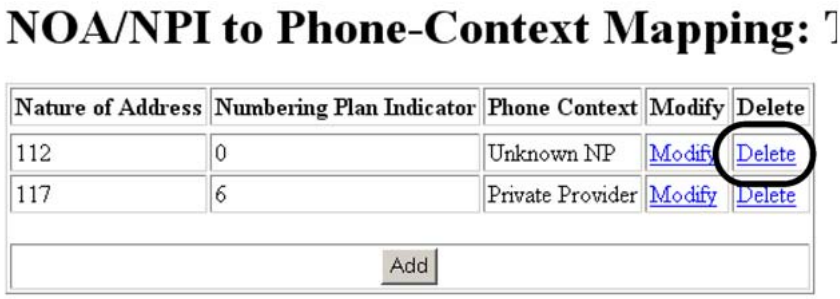


f. Return to d to modify more tuples.

or

Return to step 9 when you are finished modifying NOA/NPI tuples for this Phone Context map.

g. If you want to delete a NOA/NPI tuple from an existing PC map, click the **Delete** link to the right of the NOA/NPI tuple.



The system responds:

```
Do you really wish to delete tuple <tuplename>?
```

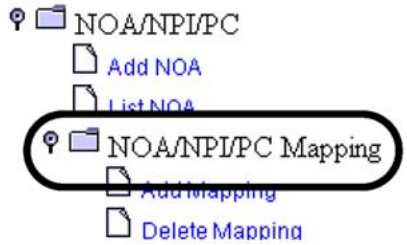
h. Click **OK** to confirm the deletion.

i. Return to g to delete more tuples.

or

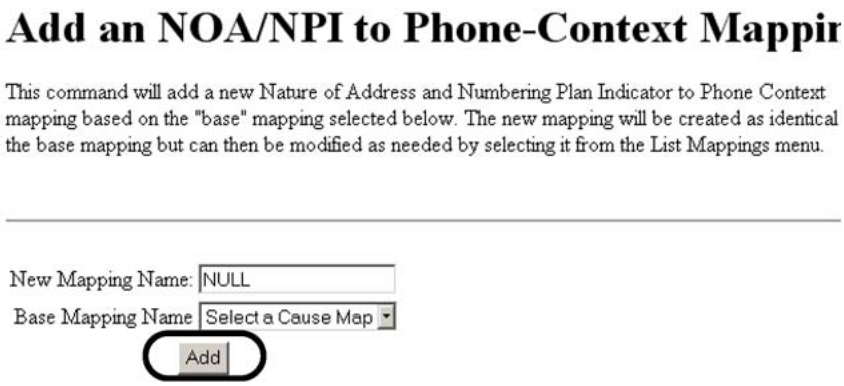
Return to step 9 when you are finished deleting NOA/NPI tuples.

11 To create (add) a new Phone Context map, click the **NOA/NPI/PC Mapping** link.



12 Click the **Add Mappings** link.

13 Type a new Phone Context map name, select a base mapping (usually the DEFAULT map) and click the **Add** button.

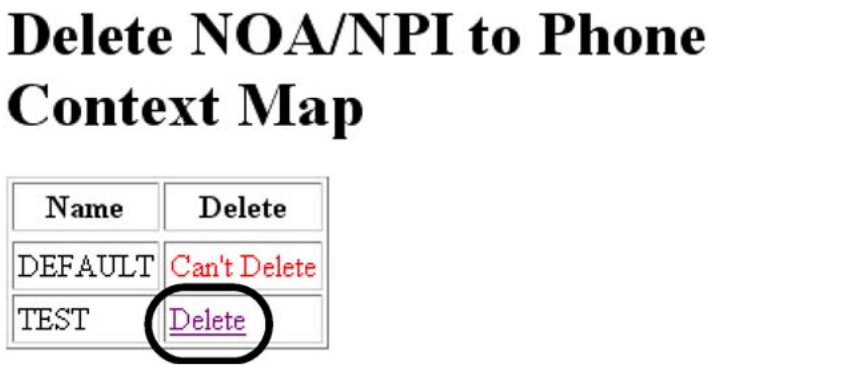


14 Return to step 3 when you are finished adding a PC map.

15 Click the **Delete Mappings** link and select the Phone Context map you want to delete.

16 To delete an existing Phone Context map, click the **Delete** link to the right of the map name.

You cannot delete the DEFAULT PC map.



The system responses:

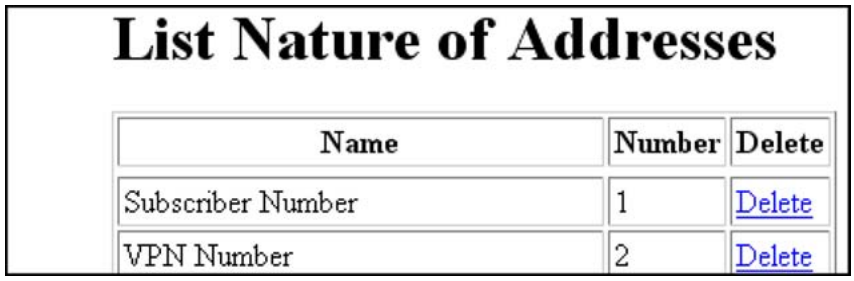
```
Do you really wish to delete the mapping <mapname>?
```

17 Click **OK** to confirm the deletion of the PC map.

18 Return to step 5 when you are finished deleting Phone Context maps.

19 To list (review) the NOA (Nature of Address) table, click the **List NOA** link.

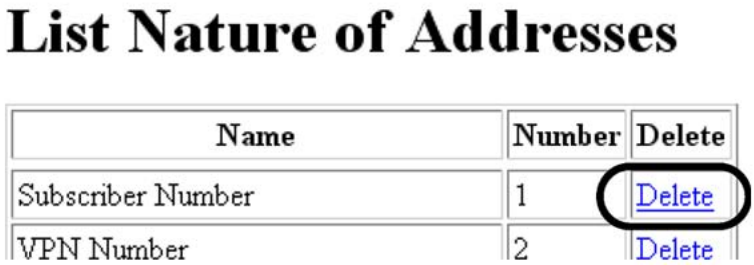
20 Review the list of existing NOAs in the table.



21 If you want to delete an NOA entry, continue with step 22, otherwise return to step 5.

22 To delete an existing NOA entry from the NOA table, click the **Delete** link to the right of the NOA entry number.

Ensure that any NOA entry that you want to delete is not in use. If you attempt to delete an NOA entry that is in use, the request is denied.



The system responses:

```
Do you really wish to delete the NOA named <NOA_name>?
```

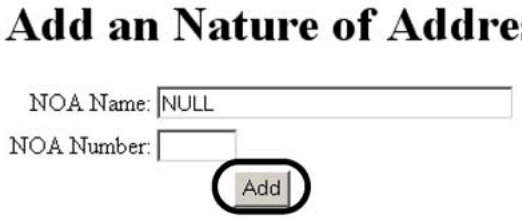
23 Click **OK** to confirm the deletion of the NOA entry.

24 Return to step 5 when you are finished deleting NOA entries.

25 Click the **Add NOA** link to add an NOA entry.

---

26 Type a new NOA entry name up to 32 alphanumeric characters, (spaces, hyphens and periods are also supported), assign an unused NOA number, then click the **Add** button.



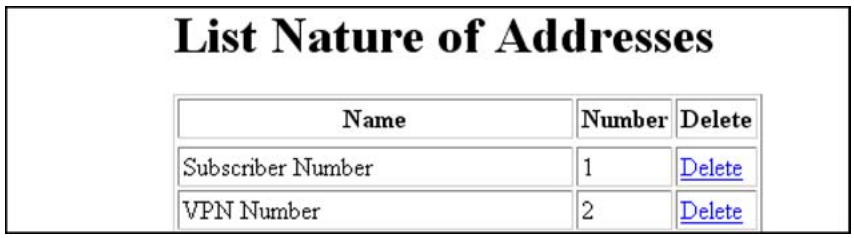
When the new NOA entry is created, the NOA table displays a list of existing entries, along with the newly created NOA entry.

The system retains the lower and upper case of the characters you enter.

Assigned NOA entries should be unique across all interconnected systems. Acceptable NOA numbers range from 1 to 150.

It is not recommended that the same NOA name be used for multiple NOA numbers.

27 Verify that the NOA you added shows up in the NOA list.


List Nature of Addresses

Name	Number	Delete
Subscriber Number	1	Delete
VPN Number	2	Delete

28 Return to step 5 when you are finished adding new mappings.

—End—

Table of available NOAs and NPIs

The Nature of Address (NOA) Indicator identifies the scope (a network, geographical region or other) in which a phone number is valid (such as the local area or country). This allows shortening the number, and its translation process, to the digits that are actually relevant in that scope. The different scopes are defined together with a numbering plan indicator (NPI).

Use the following table to make changes to an existing NOA mapping.

NOA Name	Number
Subscriber Number	1
VPN Number	2
National Significant Number	3
International Number	4
Abbreviated Number	6
Treated Call Operator Request	112
Subscriber Number Operator Request	113
National Number Operator Request	114
International Number Operator Request	115
No Number Present Operator Request	116
No Number Present Cut Thru	117

NOA Name	Number
APN Number	120
International Inbound Operator Call	122

The NPI identifies a numbering scheme for users of telecommunications services in different telecommunication networks. The SST has the capability to translate one specific numbering plan (such as a generic numbering plan used by nodes in subsystems of the SS7 network on a PSTN) to be mapped to a SIP equivalent.

Use the following table to make changes to an existing NPI mapping.

NPI Name	Number
Unknown Numbering Plan	#0
ISDN Telephony Numbering Plan	#1
Private Numbering Plan	#6

Adding and managing SIP base protocols

Purpose of this procedure

Use the following procedure to provision a new SIP base. A SIP Base is a simple character string that represents base protocols utilized when provisioning ISUP to SIP variants. Seven protocol defaults exist.

Limitations and restrictions

Deleting predefined SIP base protocol tuples is not allowed. However, the customer can create new base tuples for their specific SIP processing needs.

Only user-defined SIP Base tuples can be deleted. System default tuples can not be deleted.

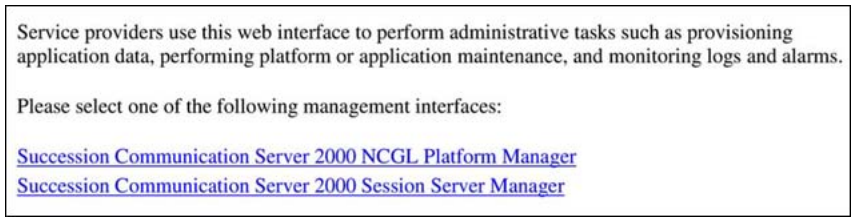
Ensure that any SIP base tuple that you want to delete is not in use. If you attempt to delete a SIP base tuple that is in use by a Remote SIP Server, the request is denied by the system.

Prerequisites

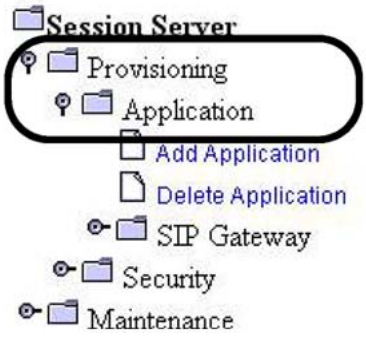
There are no prerequisites for performing this procedure.

Action

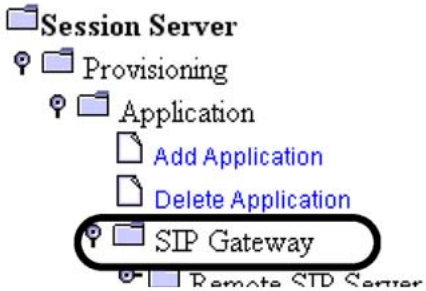
Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



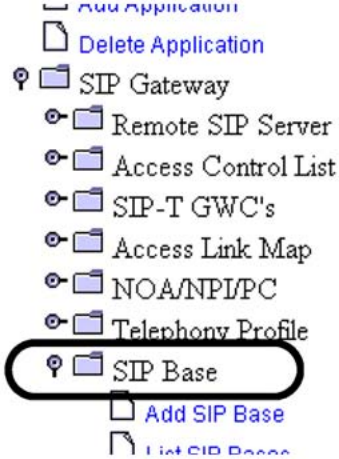
2	At the Session Server folder, click the **Provisioning folder**, then the **Application** folder.



3 Click on the **SIP Gateway** folder to open the folder.



4 Click on the **SIP Base** folder to open it.

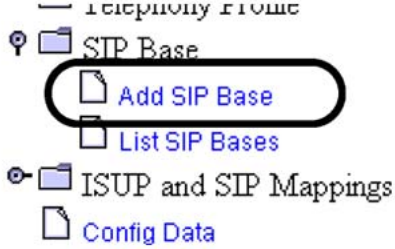


5 Use the following table to determine your next step:

If	Do
you are adding a SIP base tuple to the SIP Gateway application database	step 6

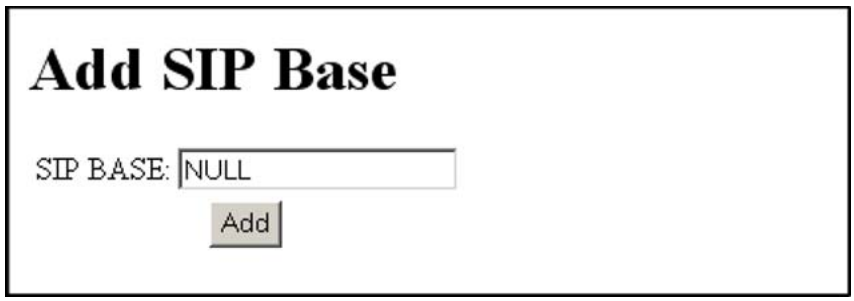
If	Do
you want to list existing SIP base tuples currently in the database	step 9
you are deleting a SIP base tuple from the SIP Gateway application database	step 10

6 Click the **Add SIP Base** link.



7 Enter a SIP base tuple name in DNS format, up to 32 characters in length (alphanumerics, hyphens and underscores), then click the **Add** button.

All alpha characters entered are converted to upper case.

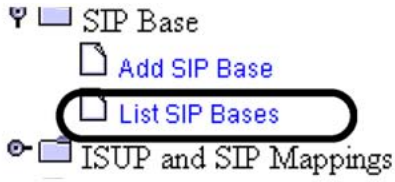


A table of all SIP bases is displayed for the map you just created.

8 Use the following table to determine your next step:

If	Do
you want to create additional SIP base tuples	return to step 7
you want to list or delete other-user defined SIP base tuples	skip to step 9

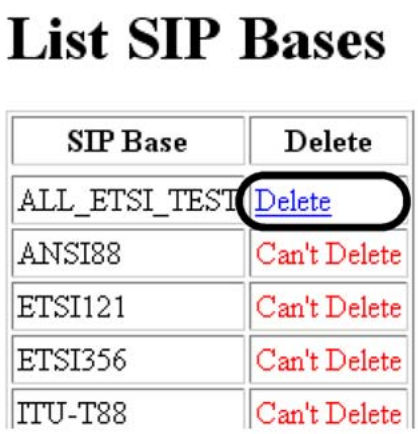
9 Click on the **List SIP Bases** page to open it.



A table of listed SIP base tuples is displayed, including the system base tuples that cannot be deleted.

10 If you want to delete a SIP base tuple, click the **Delete** link next to the base tuple you want to remove from the database. Otherwise, the procedure is complete.

Ensure that any SIP base tuple that you want to delete is not in use. If you attempt to delete a SIP base tuple that is in use by a Remote SIP Server, the request is denied by the system.



The system responses:

```
Do you really wish to delete SIP base entry <basename>?
```

11 Click **OK** to confirm the deletion.

12 Return to step 5 if you want to add or delete other SIP base tuples. Otherwise, the procedure is complete.

—End—

Table of available default SIP base protocol tuples

Protocol	Purpose
ANSI88	ISUP (ISDN User Part) variant
ANSI_UCP	ISUP variant

Protocol	Purpose
ITU-T88	ISUP variant
ITU-T92-PLUS	ISUP variant
ETSI121	ISUP variant
ETSI356	ISUP variant
TTC93-PLUS	ISUP variant

Adding and managing ISUP to SIP mapping

Purpose of this procedure

Use the following procedure to map an ISUP Release Cause to a SIP Response code. An ISUP Cause to SIP Response mapping table can consist of nearly eighty ISUP Release Causes mapped to SIP response codes. Along with each mapping is a SIP Text Reason Phrase and an ISUP Text Reason Phrase. A table at the end of this procedure provides all of the codes available in the current release.

Limitations and restrictions

The ISUP Cause to SIP Response mapping is optional because a predefined mapping table exists in the database. This predefined mapping table is called "DEFAULT" in the drop down menu and may be selected when provisioning a Remote SIP Server using procedure "Configuring Remote SIP Servers" (page 26). This predefined mapping table cannot be modified.

The default mapping cannot be deleted or modified.

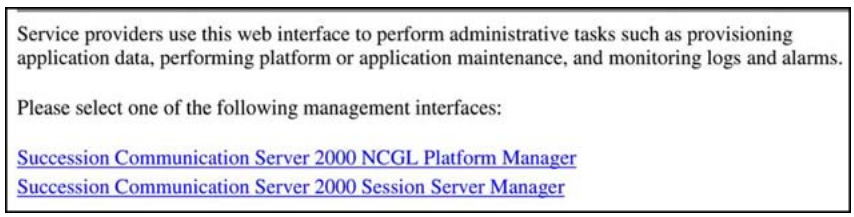
Ensure that any mapping that you want to delete is not in use. If you attempt to delete a mapping that is in use by a Remote SIP Server, the request is denied by the system.

Prerequisites

There are no prerequisites for performing this procedure.

Action

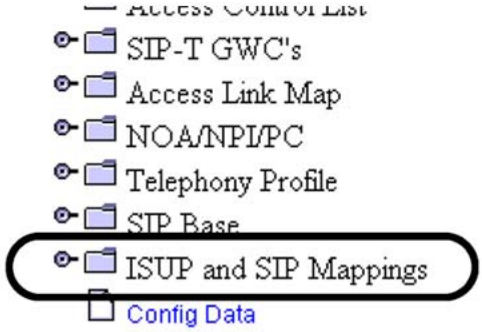
Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



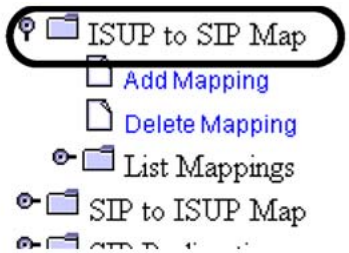
2	At the Session Server folder, click the **Provisioning folder**, then the **Application** folder.

3 Click on the **SIP Gateway** folder to open the folder.

4 Click on the **ISUP and SIP Mappings** folder to open it.



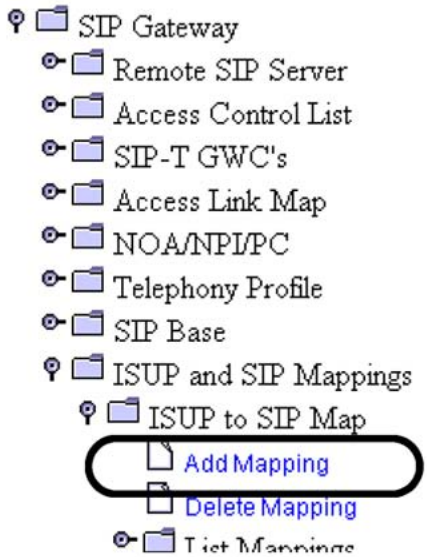
5 Click on the **ISUP to SIP Map** link to open it.



6 Use the following table to determine your next step:

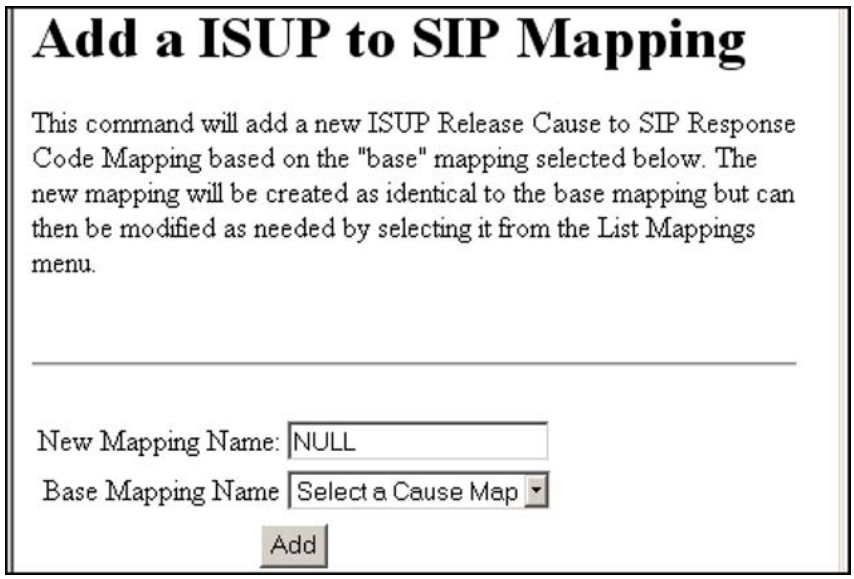
If	Do
you are adding an ISUP to SIP Map to the SIP Gateway application database	step 7
you want to list or modify an existing ISUP to SIP Map currently in the database	step 12
you are deleting an ISUP to SIP Map from the SIP Gateway application database	step 18

7 Click the **Add Mapping** link.



8 Enter a mapping name up to characters in length, in DNS format up to 32 characters, (spaces, hyphens and periods are also supported).

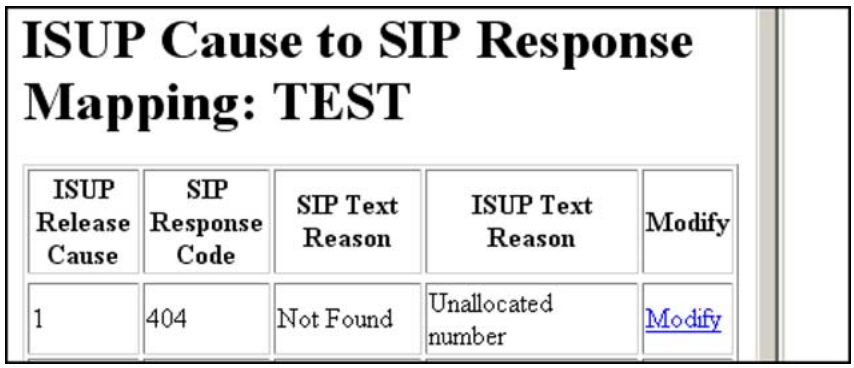
All alpha characters entered are converted to upper case.



9 Select a Base Mapping Name from the drop down menu. This is usually DEFAULT, unless you have other customized base maps already added to your database.

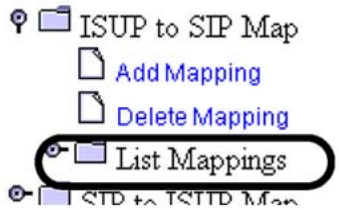
10 Once all selections are made and verified as correct, click the **Add** button.

An *ISUP Cause to SIP Response Mapping table* is displayed for the map you just created.



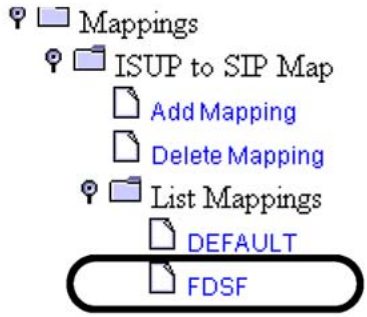
11 If you want to add another ISUP to SIP Map, return to step 7 otherwise return to step 6

12 Click on the **List Mappings** folder to open it.



A list of existing maps is displayed, including the DEFAULT map.

13 Click on the map name you want to review.



The mapping table is displayed for your review

14 If you want to modify a particular tuple in the selected mapping table, click the **Modify** link found to the far right of the table entry. Otherwise skip to step 17.

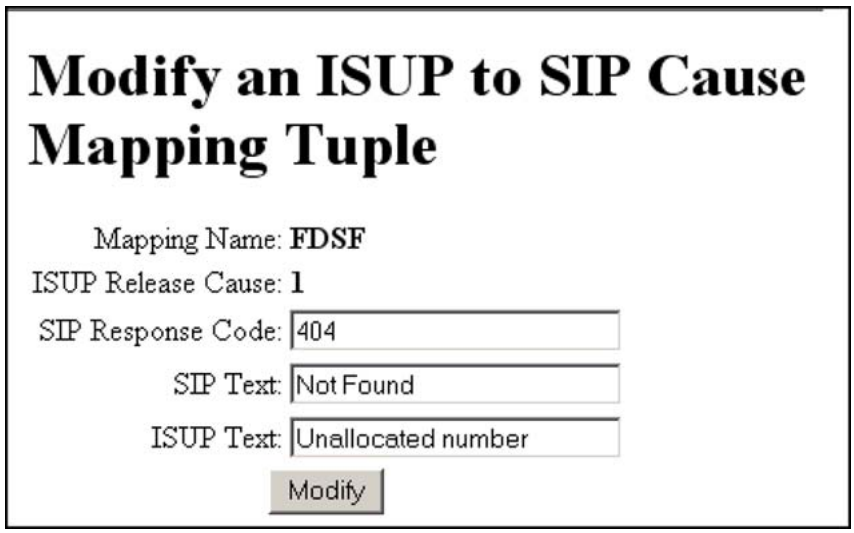
ISUP Cause to SIP Response Mapping: FDSF

ISUP Release Cause	SIP Response Code	SIP Text Reason	ISUP Text Reason	Modify
1	404	Not Found	Unallocated number	Modify
2	404	Not Found	No route to network	Modify
3	404	Not Found	No route to destination	Modify

15 For each cause tuple, you can modify:

- the SIP Response Code
- the SIP text
- the ISUP text

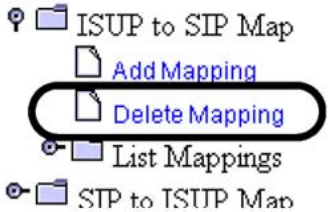
You cannot change the ISUP release Cause number.



16 Click the **Modify** button when you are finished.

17 If you want to list or modify another ISUP to SIP Map, return to step 12. Otherwise return to step 6

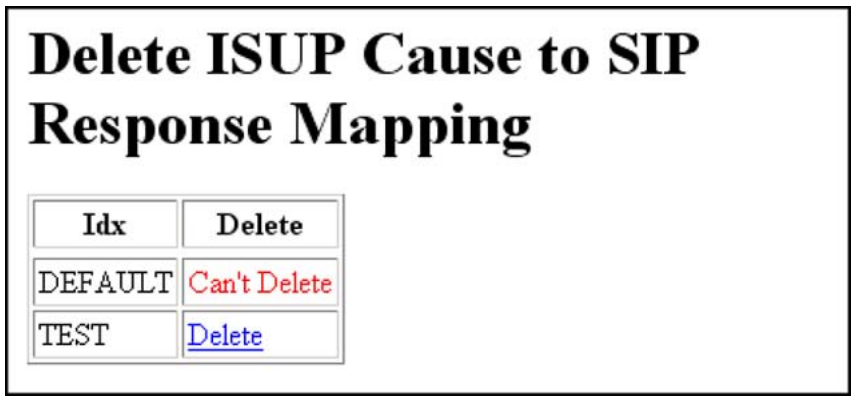
18 If you want to delete a map, click the **Delete Mapping** link, otherwise return to step 6



A list of current maps is displayed

19 Click the **Delete** link next to the map you want to remove from the database.

Ensure that any mapping that you want to delete is not in use. If you attempt to delete a mapping that is in use by a Remote SIP Server, the request is denied by the system. You can never delete the default mapping.



The system responses:

```
Do you really wish to delete mapping <mapname>?
```

20 Click **OK** to confirm the deletion.

21 Return to step 6 if you want to make changes to other maps, otherwise the procedure is complete.

—End—

Table of Default ISUP Release Cause to SIP Response Codes

ISUP Release Cause	SIP Response Code	SIP Text Reason Phrase	ISUP Text Reason Phrase
1	404	Not Found	Unallocated number
2	404	Not Found	No route to network
3	404	Not Found	No route to destination
4	487	Request Terminated	Send Special Tone Information
5	404	Not Found	Misdialed trunk prefix
6	480	Temporarily Unavailable	Channel Unacceptable
7	487	Request Terminated	Call awarded and being delivered in an established channel
8	487	Request Terminated	Preemption
9	487	Request Terminated	Preemption-circuit reserved for use
16	487	Request Terminated	Normal call clearing
17	486	Busy Here	User busy
18	408	Request Timeout	No User responding

ISUP Release Cause	SIP Response Code	SIP Text Reason Phrase	ISUP Text Reason Phrase
19	480	Temporarily Unavailable	No answer from the user
20	480	Temporarily Unavailable	Subscriber absent
21	403	Forbidden	Call rejected
22	410	Gone	Number changed (w/o diagnostics)
23	410	Gone	Redirection to new Destination
25	483	Too Many Hops	Exchange Routing Error
26	404	Not Found	Non-Selected User Clearing
27	502	Bad Gateway	Destination out of order
28	484	Address Incomplete	Address Incomplete
29	501	Not Implemented	Facility rejected
30	487	Request Terminated	Response to Status Inquiry
31	487	Request Terminated	Normal Unspecified
34	503	Service Unavailable	No Circuit Available
38	503	Service Unavailable	Network out of order
39	487	Request Terminated	Permanent Frame Mode Connection Out of Service
40	487	Request Terminated	Permanent Frame Mode Connection Operational
41	503	Service Unavailable	Temporary Failure
42	503	Service Unavailable	Switch Equipment Congestion
43	503	Bad gateway	Access Information discarded
44	503	Service Unavailable	Requested Channel not Available
45	503	Service Unavailable	Service Unavailable
46	487	Request Terminated	Precedence Call Blocked
47	503	Service Unavailable	Resource Unavailable
49	503	Service Unavailable	QoS Unavailable
50	503	Service Unavailable	Facility Not Subscribed
51	503	Service Unavailable	Service Unavailable
53	403	Forbidden	Outgoing calls barred within CUG
54	503	Service Unavailable	Service Unavailable
55	403	Forbidden	Incoming calls barred within CUG

ISUP Release Cause	SIP Response Code	SIP Text Reason Phrase	ISUP Text Reason Phrase
57	403	Forbidden	Bearer Capability Not Authorized
58	503	Service Unavailable	Bearer Capability not presently available
62	403	Forbidden	Inconsistency in designated outgoing access information and subscriber class
63	503	Service Unavailable	Service/Option Not Available
65	488	Not Acceptable Here	Bearer capability not implemented
66	503	Service Unavailable	Channel Type not Implemented
69	503	Service Unavailable	Requested Facility not Implemented
70	488	Not Acceptable Here	Only restricted digital information bearer capability is available
79	501	Not Implemented	Service or option not implemented
81	400	Bad Request	Invalid Call Reference Value
82	480	Temporarily Unavailable	Identified Channel does not exist
83	400	Bad Request	Suspended call exists but this call identity does not
84	400	Bad Request	Call identity in use
85	400	Bad Request	No Call Suspended
86	408	Request Timeout	Call having the requested call identity has been cleared
87	403	Forbidden	User Not Member of CUG
88	503	Service Unavailable	Incompatible Destination
90	400	Bad Request	Non-Existent CUG
91	502	Bad Gateway	Invalid Transit Network Selection
95	400	Bad Request	Invalid message
96	400	Bad Request	Mandatory Information Element is Missing
97	400	Bad Request	Message type non-existent or not implemented
98	400	Bad Request	Message not compatible with call state or message type non-existent or not implemented

ISUP Release Cause	SIP Response Code	SIP Text Reason Phrase	ISUP Text Reason Phrase
99	400	Bad Request	Information element non-existent or not implemented
100	400	Bad Request	Invalid Information Elements Contents
101	400	Bad Request	Message Not Compatible with Call State
102	504	Gateway Timeout	Recovery of Timer Expiry
103	400	Bad Request	Parameter Non-Existent or Not Implemented, Passed on
110	400	Bad Request	Message with Unrecognized Parameter Discarded
111	500	Server Internal Error	Protocol error
127	500	Server Internal Error	Interworking Unspecified

Adding and managing SIP to ISUP mapping

Purpose of this procedure

Use the following procedure to map a SIP Response Code to ISUP Cause release cause. A single SIP Response to ISUP Cause mapping table consists of nearly forty SIP Response Codes mapped to ISUP Release Causes. A table at the end of this procedure provides all of the codes available in the current release.

Limitations and restrictions

The SIP Response Code to ISUP Cause mapping is optional because a predefined mapping table exists in the database. This predefined mapping table is called "DEFAULT" in the drop down menu may be selected when provisioning a Remote SIP Server using procedure "Configuring Remote SIP Servers" (page 26). This predefined mapping table cannot be modified.

Only user-defined mappings can be deleted. System default mappings can not be deleted.

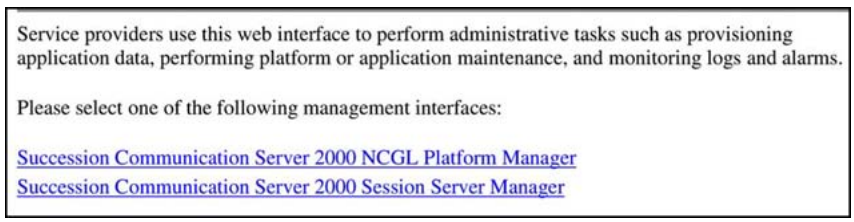
Ensure that any mapping that you want to delete is not in use. If you attempt to delete a mapping that is in use by a Remote SIP Server, the request is denied by the system.

Prerequisites

There are no prerequisites for performing this procedure.

Action

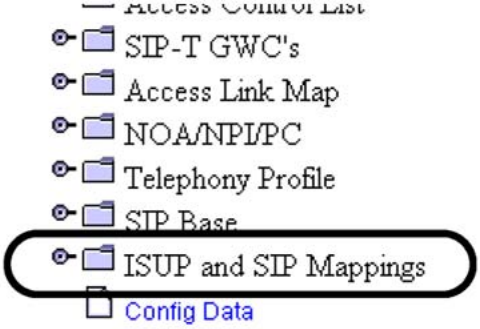
Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



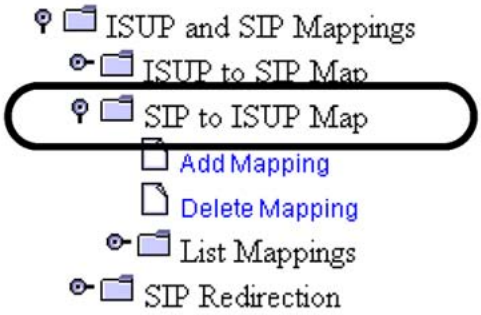
2	At the Session Server folder, click the **Provisioning folder**, then the **Application** folder.

3 Click on the **SIP Gateway** folder to open the folder.

4 Click on the **ISUP and SIP Mappings** folder to open it.



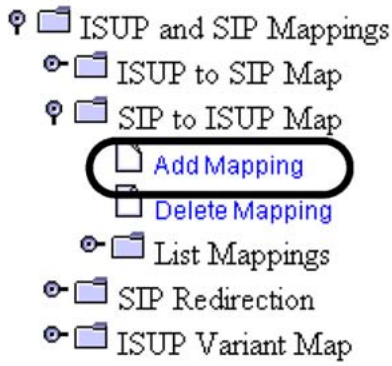
5 Click on the **SIP to ISUP Map** link to open it.



6 Use the following table to determine your next step:

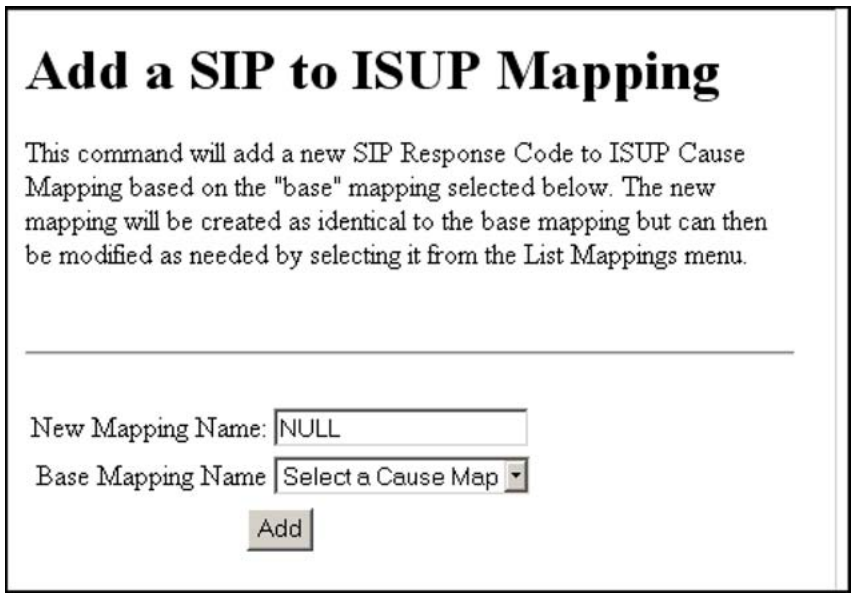
If	Do
you are adding a SIP to ISUP Map to the SIP Gateway application database	step 7
you want to list or modify an existing SIP to ISUP Map currently in the database	step 12
you are deleting an SIP to ISUP Map from the SIP Gateway application database	skip to step 18
you are finished with this procedure	skip to step 21

7 Click the **Add Mapping** link.



8 Enter a mapping name up to 32 alphanumeric characters in length.

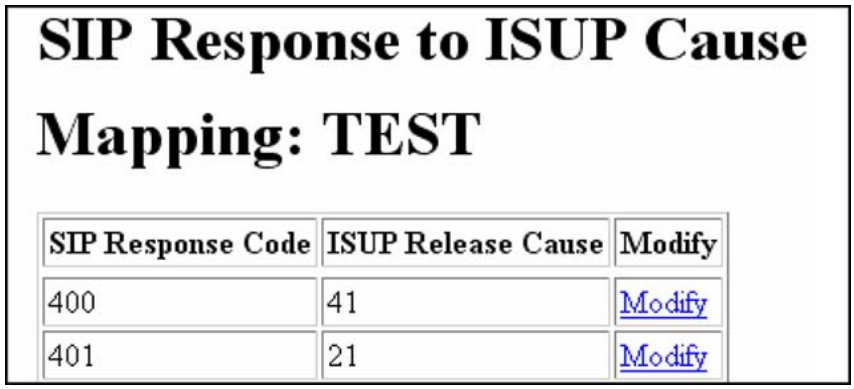
All alphabet characters entered are converted to upper case.



9 Select a Base Mapping Name from the drop down menu. This is usually DEFAULT, unless you have other customized base maps already in your database.

10 Once all selections are made and verified as correct, click the **Add** button.

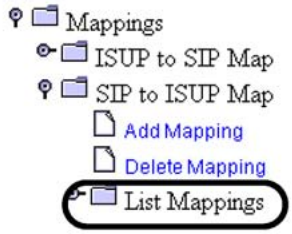
A *SIP Response to ISUP Cause Mapping table* is displayed for the map you just created.



11 If you want to add another ISUP to SIP Map, return to step 7 otherwise return to step 6 to perform other activities.

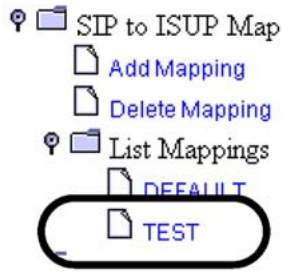
12 Click on the **List Mappings** folder to open it.

A list of existing maps is displayed, including the DEFAULT map.

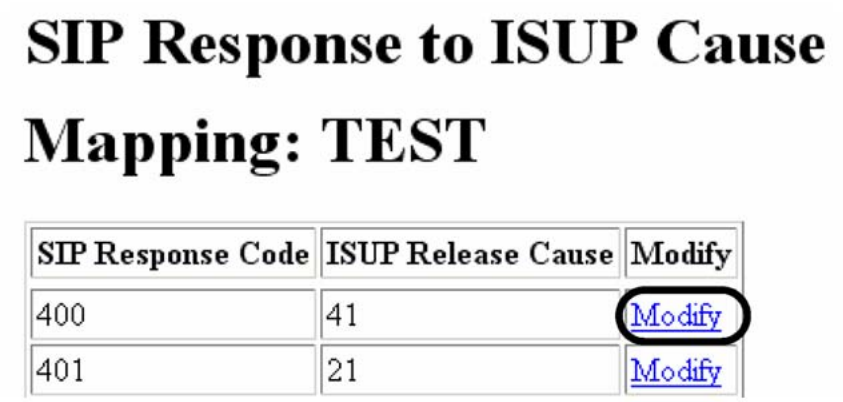


13 Click on the map name you want to review.

The mapping table is displayed.

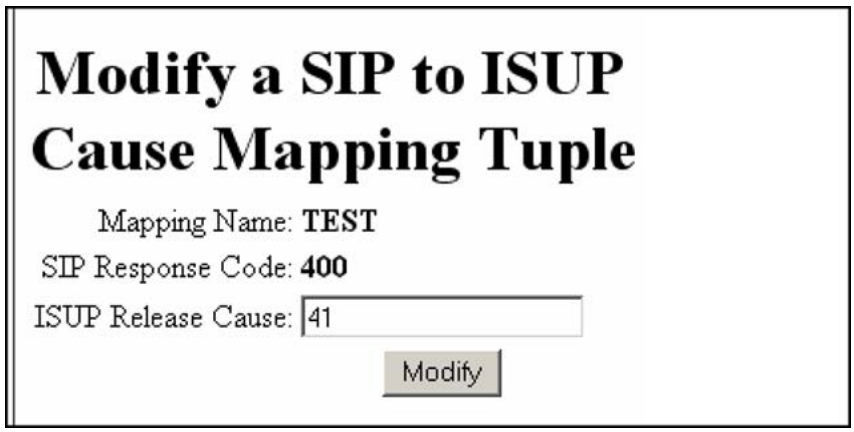


14 If you want to modify a particular tuple in the selected mapping table, click the **Modify** link found to the far right of the table entry. Otherwise skip to step 17.



15 For each cause tuple, you can modify:

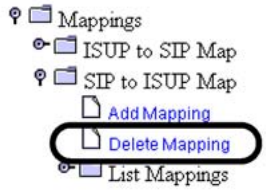
the ISUP release Cause number



16 Click the **Modify** button when you are finished.

17 If you want to list or modify another ISUP to SIP Map, return to step 12 otherwise return to step 6.

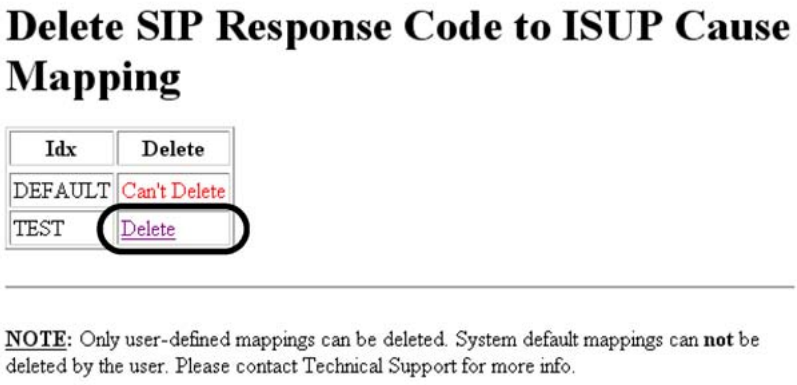
18 If you want to delete a map, click the **Delete Mapping** link. Otherwise skip to step 6.



A list of current maps is displayed

19 Click the **Delete** link next to the map you want to remove from the database.

Ensure that any mapping that you want to delete is not in use. If you attempt to delete a mapping that is in use by a Remote SIP Server, the request is denied by the system.



The system responses:

```
Do you really wish to delete mapping <mapname>?
```

20 Click **OK** to confirm the deletion.

21 Return to step 6 if you want to make changes to other maps, otherwise you have completed this procedure.

—End—

Table of SIP Response Code to ISUP Release Cause mapping

SIP Response Code	ISUP Release Cause		SIP Response Code	ISUP Release Cause
400	41		480	18
401	21		481	41
402	21		482	25
403	21		483	25
404	1		486	17
405	63		487	16
406	79		500	41
407	21		501	79
408	102		502	38
409	41		503	41
411	127		504	41
413	127		505	127
414	127		513	127
415	79		580	127

SIP Response Code	ISUP Release Cause		SIP Response Code	ISUP Release Cause
416	127		600	17
420	127		603	21
421	127		604	1
423	127			

Adding and managing SIP Redirection mapping

Purpose of this procedure

Use the following procedure to set up SIP Redirection Mapping. SIP Redirection Mapping is a mapping of 3XX SIP redirection response messages to associated 300-699 response codes. This mapping allows the customer to configure a call receiving a 3XX redirection message to be processed as a 300 or 699 related value.

Limitations and restrictions

Changing SIP Redirection Mapping datafill is optional. A predefined mapping table exists in the database and is called "DEFAULT" in the drop down menu. If you want to change any of the predefined defaults, you must create new mapping tables for your specific needs.

Only user-defined mappings can be deleted. System default mappings can not be deleted.

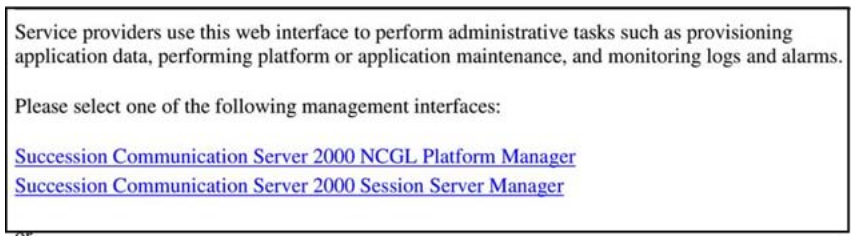
Ensure that any mapping that you want to delete is not in use. If you attempt to delete a mapping that is in use by a Remote SIP Server, the request is denied by the system.

Prerequisites

There are no prerequisites for performing this procedure.

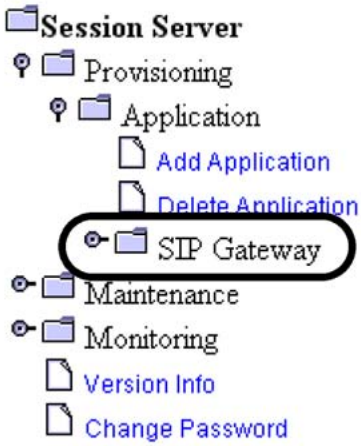
Action

Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.

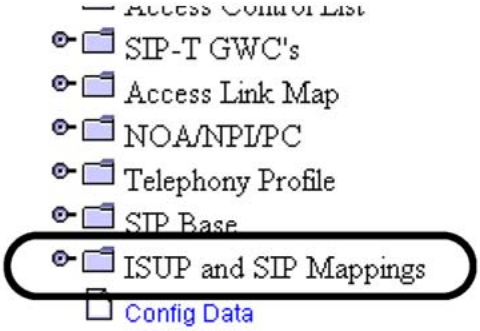


2	At the Session Server folder, click the **Provisioning folder**, then the **Application** folder.

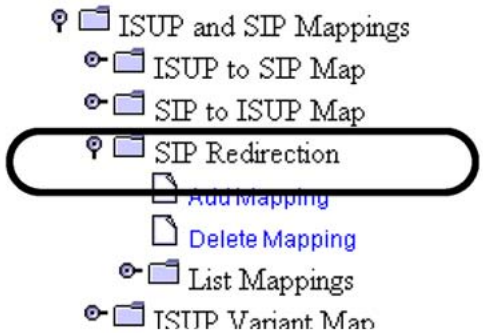
3 Click on the **SIP Gateway** folder to open the folder.



4 Click on the **ISUP and SIP Mappings** folder to open it.



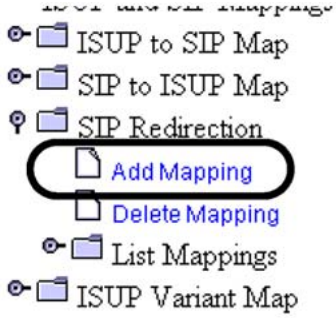
5 Click on the **SIP Redirection** link to open it.



6 Use the following table to determine your next step:

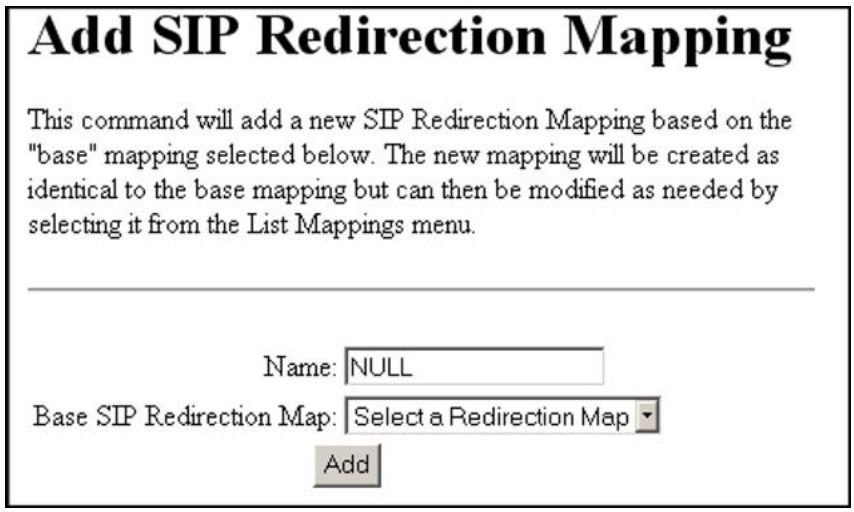
If	Do
you are adding a SIP Redirection Map to the SIP Gateway application database	continue with step 7
you want to list or modify an existing SIP Redirection Maps currently in the database	skip to 12
you are deleting a SIP Redirection Map from the SIP Gateway application database	skip to 18
you are finished with this procedure	skip to step 21

7 Click the **Add Mapping** link.



8 Enter a SIP redirection mapping name up to 32 alphanumeric characters in length.

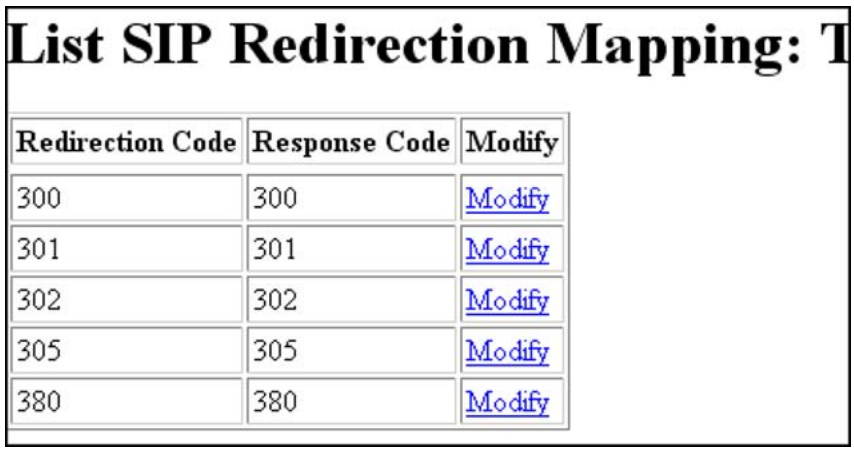
All alpha characters entered are converted to upper case.



9 Select a Base SIP Redirection Map from the drop down menu. This is usually DEFAULT, unless you have other customized base maps already in your database.

10 Once all selections are made and verified as correct, click the **Add** button.

A SIP Redirection Map is displayed for the map you just created.



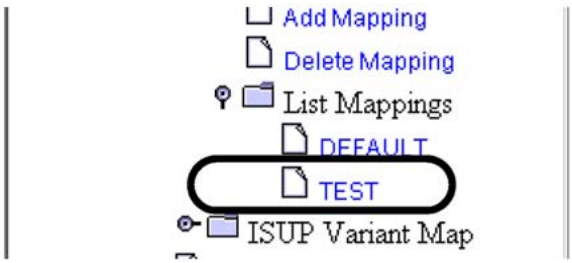
11 If you want to add another SIP redirection map, return to step 7 otherwise return to step 6 to perform other activities.

12 Click on the **List Mappings** folder to open it.

A list of existing maps is displayed, including the DEFAULT map.

13 Click on the map name you want to review.

The mapping table is displayed.



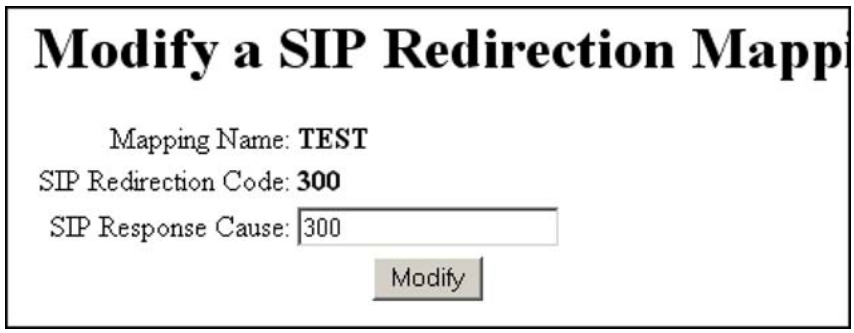
14 If you want to modify a particular tuple in the selected mapping table, click the **Modify** link found to the far right of the table entry. Otherwise skip to step 17.

List SIP Redirection Mapping:

Redirection Code	Response Code	Modify
300	300	Modify
301	301	Modify
302	302	Modify
305	305	Modify
380	380	Modify

15 For each mapping tuple, you can modify:

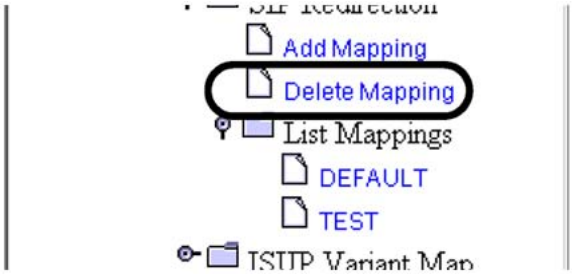
- the SIP Response Code



16 Click the **Modify** button when you are finished.

17 If you want to list or modify another ISUP to SIP Map, return to step 12, otherwise return to step 6.

18 If you want to delete a map, click the **Delete Mapping** link. Otherwise skip to step 21.



A list of current maps is displayed

19 Click the **Delete** link next to the map you want to remove from the database.

Ensure that any mapping that you want to delete is not in use. If you attempt to delete a mapping that is in use by a Remote SIP Server, the request is denied by the system.

The system responses:

```
Do you really wish to delete mapping <mapname>?
```

20 Click **OK** to confirm the deletion.

21 Return to step 6 if you want to make changes to other maps, otherwise the procedure is complete.

—End—

Table of SIP Response Redirection mapping defaults

SIP Redirection Code	Response Code
300	300
301	301
302	302
305	305
380	380

Adding and managing ISUP variant mappings

Purpose of this procedure

Use the following procedure to add an ISUP Protocol, version, and variant to a SIP Base and Version.

Limitations and restrictions

Changing mapping datafill is optional. A predefined mapping table exists in the database and is called "DEFAULT" in the drop down menu. However, if the customer does not want to change any of the above predefined defaults, they can create new mapping tables for their specific processing needs.

Only user-defined mappings can be deleted. System default mappings can not be deleted.

Ensure that any mapping that you want to delete is not in use. If you attempt to delete a mapping that is in use by a Remote SIP Server, the request is denied by the system.

Prerequisites

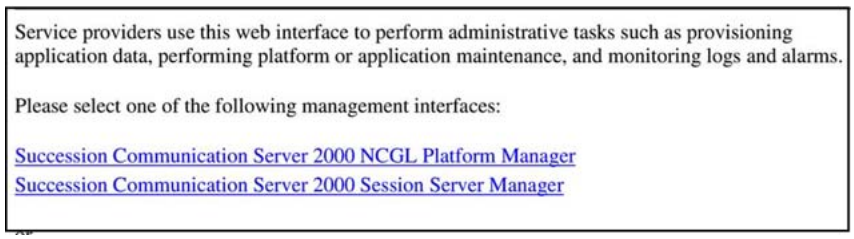
When adding the remote SIP servers, if you plan to select a custom mapping value for 'ISUP Variant to SIP Version Map', then add a new variant mapping table.

Action

Step	Action

At the CS 2000 Session Server Launch Point

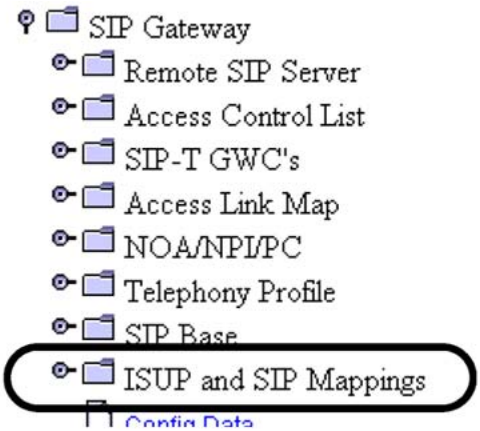
1 Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



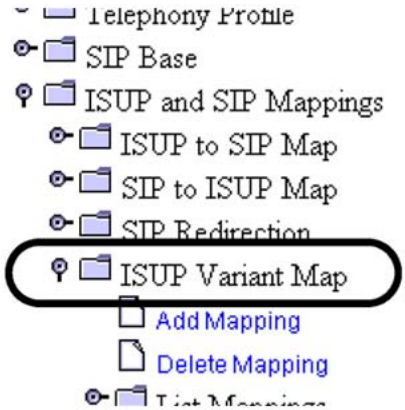
2 At the Session Server folder, click the **Provisioning folder**, then the **Application** folder.

3 Click on the **SIP Gateway** folder to open the folder.

4 Click on the **ISUP and SIP Mappings** folder to open it.



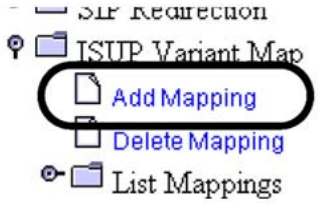
5 Click on the **ISUP Variant Map** link.



6 Use the following table to determine your next step:

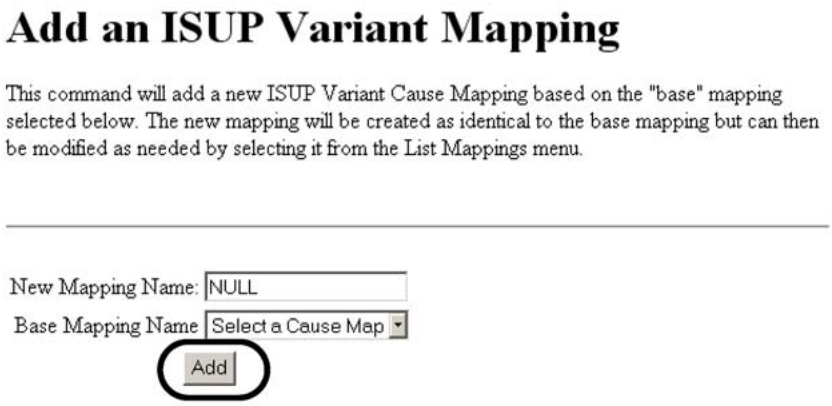
If	Do
you are adding an ISUP Variant Mapping to the SIP GW Application database, including modifying a new ISUP Variant Mapping	continue with step 7
you are listing or modifying the tuples of an existing ISUP Variant Mapping	skip to step 11
you are deleting an existing ISUP Variant Mapping (and not individual map tuples) from the database	skip to step 15
you are finished adding, reviewing, changing or deleting variant mappings	skip to the last step

7 Click the **Add Mapping** link.

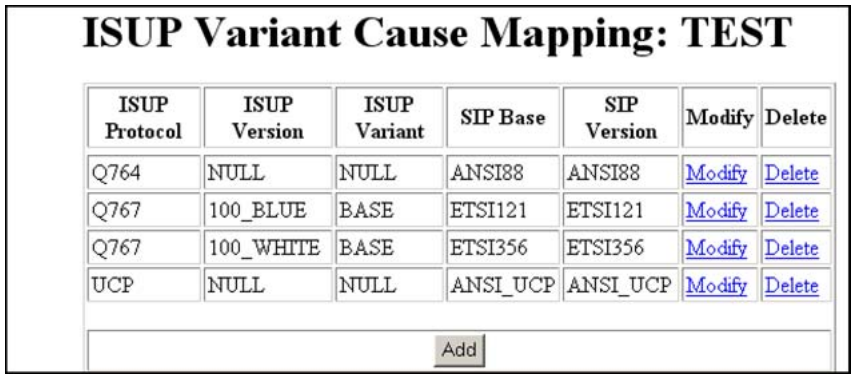


8 At the *Add Mapping* page, type a new mapping name up to 32 alphanumeric characters in length, select the base mapping from the drop down list, then click the **Add** button.

All alpha characters entered are converted to upper case.



A new mapping is created. When a new mapping is created, it uses the mapping content based on the selected base mapping. If a mapping that is empty of tuple content is used, then the new table will also be empty of tuple content. This action also applies to the DEFAULT base mapping if the database is being rebuilt.



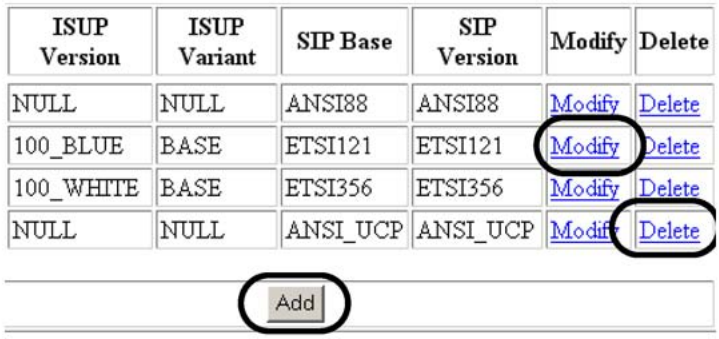
ISUP Variant Cause Mapping: TEST

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version	Modify	Delete
Q764	NULL	NULL	ANSI88	ANSI88	Modify	Delete
Q767	100_BLUE	BASE	ETSI121	ETSI121	Modify	Delete
Q767	100_WHITE	BASE	ETSI356	ETSI356	Modify	Delete
UCP	NULL	NULL	ANSI_UCP	ANSI_UCP	Modify	Delete

Add

9 If you want to modify the new mapping by adding, modifying or deleting tuples, continue with the following set of sub-steps.

Tuples within an ISUP Variant mapping table that are added or modified must adhere to specific datafill rules. The legal combinations of variables in a tuple are listed in "Table of ISUP Variant to SIP Version mappings" (page 128).

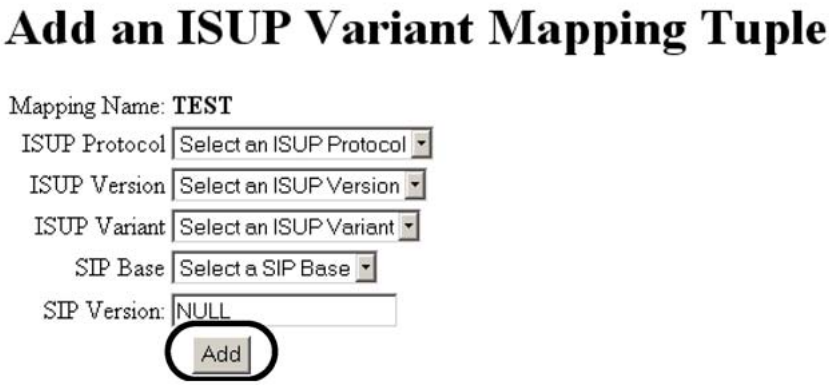


ISUP Version	ISUP Variant	SIP Base	SIP Version	Modify	Delete
NULL	NULL	ANSI88	ANSI88	Modify	Delete
100_BLUE	BASE	ETSI121	ETSI121	Modify	Delete
100_WHITE	BASE	ETSI356	ETSI356	Modify	Delete
NULL	NULL	ANSI_UCP	ANSI_UCP	Modify	Delete

Add

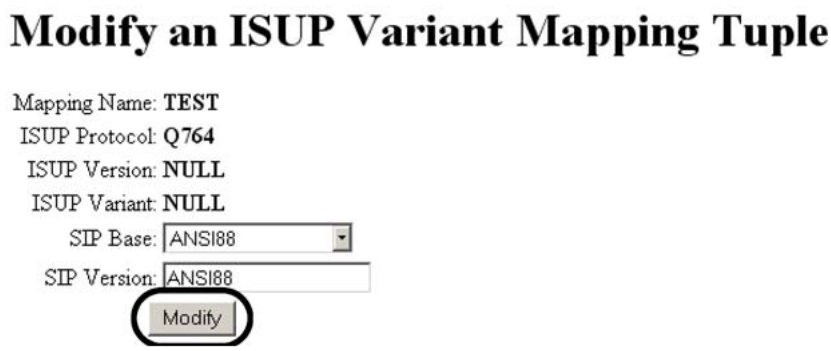
a. To add a tuple to the mapping, click the **Add** link below the table of listed tuples.

b. Using "Table of ISUP Variant to SIP Version mappings" (page 128), create a new tuple by selecting the appropriate values from the drop-down menus and entering a SIP version. When you are finished, click the **Add** button.



c. If you want to modify a tuple in the mapping, click the **Modify** link to the right of the mapping name. For each mapping tuple, you can modify:

- the SIP Base
- the SIP Version



If you make an error in modifying a tuple, the system returns a *Modification of Mapping Tuple Error* message. Click the link at the bottom of the message to return to the tuple and correct the error.

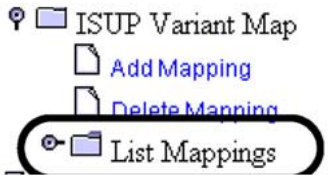
d. If you want to delete a tuple from the mapping, click the **Delete** link next to the appropriate mapping name.

The system responses:

```
Do you really wish to delete tuple
<tuplename>?
```

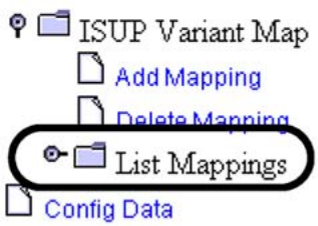
e. Click **OK** to confirm the deletion.

f. Click again on the **List Mappings** link and select the variant map you just modified to review all changes you have made to tuples in the variant map.



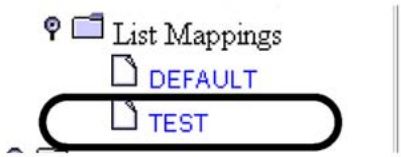
10 When you are finished making changes to the new variant map, return to step 6.

11 Click on the **List Mappings** folder to open it.



A list of existing maps is displayed, including the DEFAULT map.

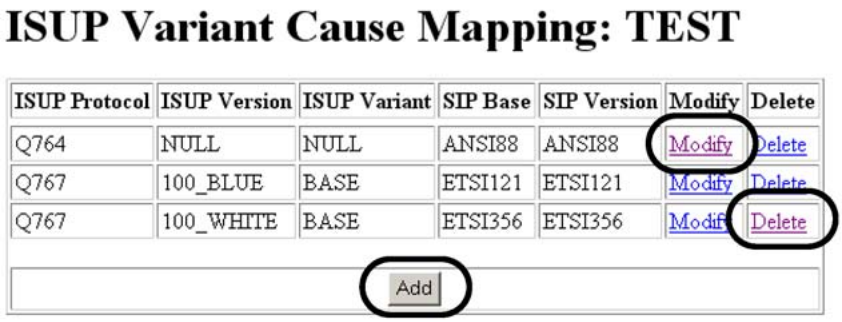
12 Click on the map name you want to review.



The mapping table is displayed.

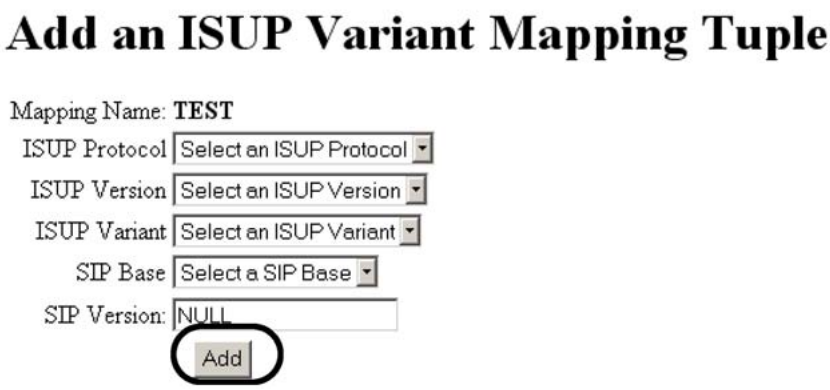
13 If you want to modify the listed mapping by adding, modifying or deleting tuples, continue with the following set of sub-steps.

Tuples within an ISUP Variant mapping table that are added or modified must adhere to specific datafill rules. The legal combinations of variables in a tuple are listed in "Table of ISUP Variant to SIP Version mappings" (page 128).



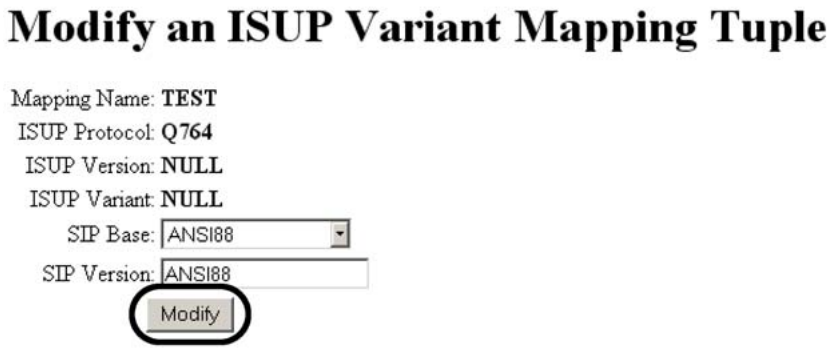
a. To add a tuple to the mapping, click the **Add** link below the table of listed tuples.

b. Using "Table of ISUP Variant to SIP Version mappings" (page 128), create a new tuple by selecting the appropriate values from the drop-down menus and entering a SIP version. When you are finished, click the **Add** button.



c. If you want to modify a tuple in any of the mappings, click the **Modify** link next to the appropriate mapping name. For each mapping tuple, you can modify:

- the SIP Base
- the SIP Version



If you make an error in modifying a tuple, the system returns a *Modification of Mapping Tuple Error* message. Click the link at the bottom of the message to return to the tuple and correct the error.

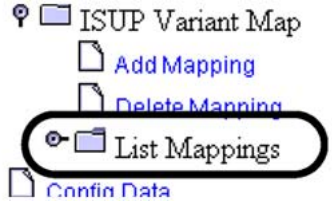
d. If you want to delete a tuple from any of the mappings, click the **Delete** link next to the appropriate mapping name.

The system responses:

```
Do you really wish to delete tuple
<tuplename>?
```

e. Click **OK** to confirm the deletion.

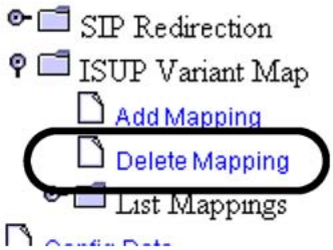
f. Click again on the **List Mappings** link and select the variant map you just modified to review all changes you have made to tuples in the variant map.



14 When you are finished making changes to this variant map, return to step 6.

15 Click the **Delete Mapping** link to remove an ISUP variant map (not individual variant map tuples) from the SIP Gateway application database.

Ensure that any variant map that you want to delete is not in use. If you attempt to delete a map that is in use, the request is denied by the system.



16 Select the mapping you want to delete then click the **Delete** button.

The system responses:

```
Do you really wish to delete mapping <mapname>?
```

17 Return to step 6 when you are finished deleting mappings. Otherwise, the procedure is complete.

—End—

Table of ISUP Variant to SIP Version mappings

The following table lists the valid combinations of tuples that may be added to an ISUP Variant to SIP Version mapping to be used for communicating using a VRDN configuration.

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
BTUP			GB_IUP	GB_IUP
Q764			GR394	GR394
UCP			ANSI88	UCP_ANSI88
MCI			ANSI88	MCI_ANSI88
Australian ISUP			ANSI88	AU_ANSI88
Q767	100_blue	France	ETSI121	FR_SSUTR2
Q767	100_blue	Base V1	ETSI121	ETSI121
Q767	100_blue	Italy	ETSI121	IT_ETSI121
Q767	100_blue	Spain	ETSI121	ES_ETSI121
Q767	100_blue	Norway	ETSI121	NO_ETSI356
Q767	100_blue	New Zealand	ETSI121	NZ_ETSI121
Q767	100_blue	Brazil	ETSI121	BR_ETSI121
Q767	100_blue	Mexico	ETSI121	MX_ETSI121
Q767	100_blue	Turkey	ETSI121	TR_ETSI121
Q767	100_blue	Portugal	ETSI121	PT_ETSI121
Q767	100_blue	Denmark	ETSI121	DK_ETSI121
Q767	100_blue	Czech	ETSI121	CZ_ETSI121
Q767	100_white	Base V2	ETSI356	ETSI356
Q767	100_white	Australia	ETSI356	AU_ETSI356
Q767	100_white	ACIF_Australia	ETSI356	AU_ETSI356
Q767	100_white	Germany	ETSI356	DE_ETSI356
Q767	100_white	Belgium	ETSI356	BE_ETSI356
Q767	100_white	Sweden	ETSI356	SE_ETSI356
Q767	100_white	Israel	ETSI356	IL_ETSI356
Q767	100_white	Papua New Guinea	ETSI356	PG_ETSI356
Q767	100_white	Chile	ETSI356	CL_ETSI356
Q767	100_white	Costa Rica	ETSI356	CR_ETSI356
Q767	100_white	Ethiopia	ETSI356	ET_ETSI121
Q767	100_white	Georgia	ETSI356	GE_ETSI356

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
Q767	100_white	Myanamar	ETSI356	MM_ETSI356
Q767	100_white	Vietnam	ETSI356	VN_ETSI356
Q767	100_white	Israeli Defence Force	ETSI356	IL_DF_ETSI356
Q767	100_white	Saudi Arabia	ETSI356	SA_ETSI356
Q767	100_white	Hungary	ETSI356	HU_ETSI356
Q767	100_white	Peru	ETSI356	PE_ETSI356
Q767	100_white	Argentina	ETSI356	AR_ETSI356
Q767	100_white	China	ETSI356	CN_ETSI356
Q767	100_white	Spain	ETSI356	ES_ETSI356
Q767	100_white	Turkey	ETSI356	TR_ETSI356
Q767	100_white	Hong Kong	ETSI356	HK_ETSI356
Q767	100_white	RUSSIA	ETSI356	RU_ETSI356
Q767	100_EIV3	Base V3	ETSI356	ETSI356
Q767	100_EIV3	UK-ISUP	ETSI356	GB_ETSI356
Q767	100_EIV3	France SPIROU	ETSI356	FR_ETSI356
Q767	CCITT7_White		ETSI356	ETSI356
Q767	CCITT7_Blue		ETSI121	ETSI121

Protocols, versions, and variants used for VRDN communication

Use the following table to assist you with configuring ISUP variant mappings in support of an SST to VRDN communications configuration.

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
Q764	NUL	NULL	GR394	GR394
UCP	NULL	NULL	ANSI88	UCP_ANSI88
ccitt	V1	base	ETSI121	ETSI121
ccitt	v2	base	ETSI356	ETSI356
btup	null	null	GB_IUP	GB_IUP

Managing TLS security parameters

Purpose of this procedure

Use the following procedure to manage the values of the Transport Layer Security (TLS) parameters of the Security Parameter Configuration Page.

Limitations and restrictions

Procedures for managing security certificates can be found in the *Session Server Trunks Security and Administration* (NN10346-611).

ATTENTION

Changing some security parameters (those marked in orange text) requires a restart (lock and suspend, then unsuspend and unlock) of the SIP Gateway application to enable the new parameter value to take effect. Parameters written in green take effect immediately.

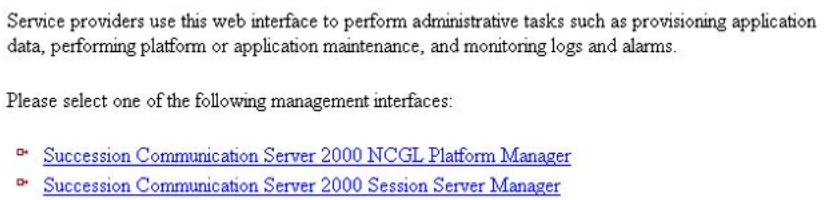
Prerequisites

Verify that the remote SIP server supports TLS connections.

Security setting made to the Configurable Security Parameters page must match the settings made to the remote SIP server. It is recommended that all SST have the same values for security parameters.

Action

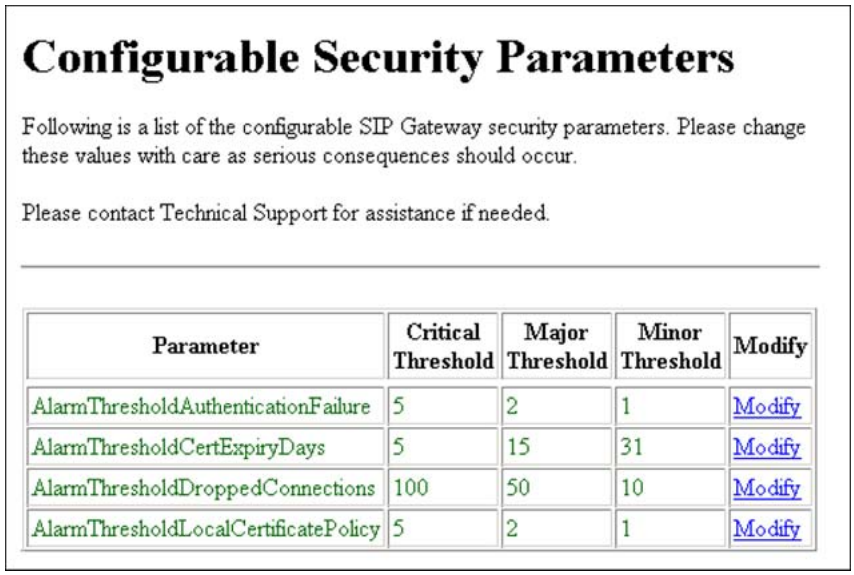
Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



2	Select **Provisioning > Security > SIP Gateway > Security Config Data** from the left side menu.

The Configurable Security Parameters page opens in the right side frame.

3 Review the current values for the Configurable Security Parameters page. Determine if any values must be changed.



Configurable Security Parameters

Following is a list of the configurable SIP Gateway security parameters. Please change these values with care as serious consequences should occur.

Please contact Technical Support for assistance if needed.

Parameter	Critical Threshold	Major Threshold	Minor Threshold	Modify
AlarmThresholdAuthenticationFailure	5	2	1	Modify
AlarmThresholdCertExpiryDays	5	15	31	Modify
AlarmThresholdDroppedConnections	100	50	10	Modify
AlarmThresholdLocalCertificatePolicy	5	2	1	Modify

This figure only shows the top of the Configurable Security Parameters page.

4 Use the following table to determine your next step:

If	Do
you are only reviewing the current parameters and their values	continue with step 6
you are modifying one or more parameter values	continue with step 5

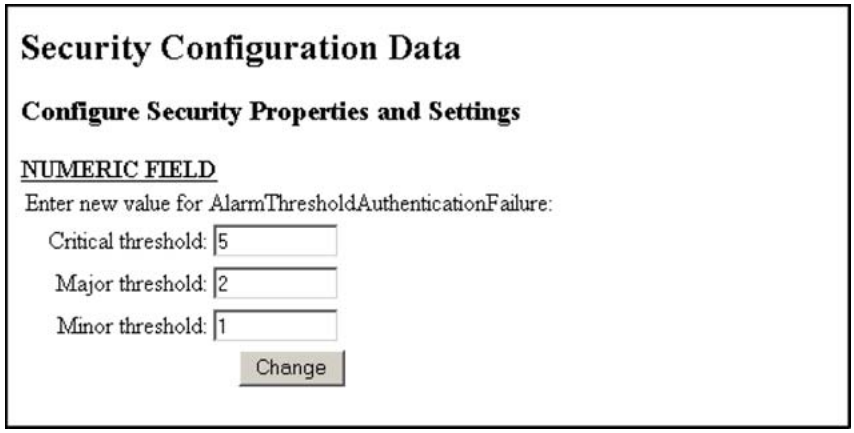
5 If you want to modify one or more security values, click the **Modify** link to the right of the value you want to change.

Parameter	Critical Threshold	Major Threshold	Minor Threshold	Modify
AlarmThresholdAuthenticationFailure	5	2	1	Modify
AlarmThresholdCertExpiryDays	5	15	31	Modify
AlarmThresholdDroppedConnections	100	50	10	Modify
AlarmThresholdLocalCertificatePolicy	5	2	1	Modify

The page refreshes and the Configure Securities Properties and Settings opens in the right side frame.

6 Refer to the table in section "Additional Information" (page 48) to assist you with setting or changing a value for the security parameters, then click **Change**.

Modifications to parameters in green text take effect immediately. Parameters in orange text do not take effect until the SIP Gateway application is restarted in step 8.



7 Return to step 4 to change other security parameters. Otherwise, continue with step 8.

8 The SIP Gateway application must be stopped and restarted to allow it to load the new security parameters. Lock, suspend, unsuspend, and then unlock the SIP Gateway application. Refer to *Session Server Trunks Security and Administration* (NN10346-611) for assistance.

CAUTION
If the related SIP trunk is in the INB state, performing a Suspend and Unsuspend does not cause the trunk to go to in-service state.

—End—

Additional TLS security information

Use the following table to assist you in modifying the Configurable Security Parameters table using the recommended values and ranges:

Enforcement of all field values and ranges is handled by the database. For all Boolean (Y/N) fields, the case (upper or lower) for the variable is preserved as entered.

Parameter Name	Description	Default Value	Range
Alarm Threshold Authentication Failure	Number of failed authentications allowed before raising a SIPS301 alarm. Authentication failures indicate that a remote certificate cannot be validated against local certificates and may be related to certificate expiration on a remote SIP server.	Critical: 5 Major: 2 Minor: 1	1 - 32767, critical > major > minor
Alarm Threshold CertExpiry Days	Number of days before certificate expiration to raise a SIP302 alarm. For example, 31 days before certificate expiration, a minor SIP302 is raised. If a local certificate expires, calls will not complete over a signalling trunk designated as TLS.	Critical: 5 Major: 15 Minor: 31	1 - 32767, critical < major < minor
Alarm Threshold Dropped Connections	Number of dropped connections allowed before raising a SIP300 alarm. Connections are dropped either because of throttling or TLS engine failure.	Critical: 100 Major: 50 Minor: 10	1 - 32767, critical > major > minor
Alarm Threshold Local Certificate Policy	Alarm SIPS308 is raised when the number of certificate policy check failures exceed the threshold in one minute.	Critical: 5 Major: 2 Minor: 1	1 - 32767, critical > major > minor

Parameter Name	Description	Default Value	Range
Alarm Minimum DisplayTime Minutes	Number of minutes to leave the following alarms raised after the event is not continuously observed. • AlarmThresholdLocal CertificatePolicy • AlarmThreshold AuthenticationFailure • AlarmThresholdDropped Connections	60	1 - 32767
ExitOnFailTLS Initialization	Indicates whether to exit the application or continue with the application initialization and attempt to service calls while the issue is resolved. **CAUTION** The TLS engine fails to initialize under the following conditions: • if the key file or certificate file is not present or corrupted • if the system is running out of memory and having trouble initializing TLS • the certificate does not match the local policy • the key-certificate pair do not match If the value is changed to N, to allow application initialization, then parameter TlsEnabled can be set to Y to initialize TLS.	Y	Y or N
MaxTLS Sessions	The Maximum number of TLS sessions allowed. **CAUTION** Setting the value lower than the number of clients (peer remote servers) trying to connect to the SIP Gateway application results in some clients being denied a secure connection. Set the value as high as the maximum number of peer remote servers that are expected to connect to this SIP Gateway application.	256	10 - 400

Parameter Name	Description	Default Value	Range
RequireLocal Certificate Policy	This parameter enables certificate policy checking. For Packet Cable conformance, this must be set to Y.	N	Y or N
Require authority KeyIdentifier	This value ensures whether the authority key identifier is present in the X.509 version 3 certificate extensions. For Packet Cable conformance, this must be set to Y. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to Y to have effect	N	Y or N
Requirebasic Constraints	This value ensures whether the basic constraints is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to Y to have effect	N	Y or N
Requireext KeyUsage	This value ensures whether the individual key usage settings are present in the X.509 version 3 certificate extensions. Checklist options are none of or any combination of serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, OCSPSigning. For Packet Cable conformance, serverAuth and clientAuth must be set. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to Y to have effect	.	Checklist
Requireissue AltName	This value ensures whether the issuer alternative name is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to Y to have effect	N	Y or N

Parameter Name	Description	Default Value	Range
Requirekey Usage	This value ensures whether the key usage settings is present in the X.509 version 3 certificate extensions. Checklist options are none of or any combination of digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly, decipherOnly. For Packet Cable conformance, dig italSignature and keyEncipherment must be set. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to Y to have effect	.	Checklist
Requireprivate KeyUsage Period	This value ensures whether the private key usage field is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to Y to have effect	N	Y or N
Require subject AltName	This value ensures whether the subject alternative name is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to Y to have effect	N	Y or N
Require subject KeyIdentifier	This value ensures whether the subject key identifier is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to Y to have effect	N	Y or N

Parameter Name	Description	Default Value	Range
SessionCache Size	Defines the maximum size of the client and server side TLS session cache. This recommended value is 8x the number of remote SIP servers using TLS, then rounding up to an allowed value. This value should not normally be decreased. A larger session cache increases the performance of TLS connection requests for enabled clients. A session cache setting of 1000 uses 1 MB of system memory.	10	10, 100, 1000, 2000, 3200
Session Cache Valid Duration	The duration for which sessions are stored in the session cache. The session data is removed from the cache after the selected interval from the time it was first inserted into the cache. If peer servers support session caching and make frequent connection requests, increase the duration values to improve performance with those servers. Changing the values impacts all future TLS sessions, but does not impact entries already in the cache.	7_Days	24_Hours, 7_Days, 3_Months
Session Caching Enabled	Determines whether session caching is enabled or not. This value enables or disables client side and server side session caching. Session caching improves performance over TLS connections where traffic is fairly low and over SWACT. If few or no peer servers to the SST have session-caching-enabled clients, then little or no performance increase will be observed for TLS connection requests. It is recommended that all remote peer servers have TLS session caching functionality enabled. Remote peer servers are considered clients when they initiate a connection request. Turning off session caching does not clear the cache. Items are removed from the server side and client side cache when they expire. Items may also be removed from the server cache when the server cache is full in order to make room for a new entry.	Y	Y or N

Parameter Name	Description	Default Value	Range
TLSAllowed Cipher Suites	The cipher suites that TLS is allowed to use in secure communications. TLS_RSA_WITH_AES_128_CBC_SHA is required, and the following are optional: TLS_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA, TLS_RSA_WITH_3DES_EDE_CBC_SHA. AES128-SHA is mandatory. When TLS is enabled, the SIP Gateway application will always accept TLS connections requested with the AES128-SHA cipher. All listed ciphers support private key sizes of 1024, 1536, and 2048 bits; RSA authentication; and SHA (Secure Hash Algorithm) as the HMAC (Hashed Message Authentication Code).	TLS_RSA_WITH_AES_128_CBC_SHA	Checklist
ThrottleBurst Durationin Secs	The maximum number of TLS connections represented by ThrottleBurstEventThreshold that can be serviced in ThrottleBurstDurationinSecs seconds. ThrottleBurstDurationinSecs is recommended to be ThrottleSustainedDurationinSecs divided by 5. This value is applied immediately and requires ThrottleEnabled to be set to Y to have effect	1	1 - 10
ThrottleBurst Event Threshold	The maximum of number of TLS connections that can be serviced in ThrottleBurstDurationinSecs seconds. Recommended value 30. This value is applied immediately and requires ThrottleEnabled to be set to Y to have effect	30	1 - 10
Throttle Enabled	Enables or disables TLS connection throttling. Recommended value Y.	Y	Y or N

Parameter Name	Description	Default Value	Range
Throttle Sustained Durationin Secs	The maximum number of TLS connections represented by ThrottleSustainedEventThreshold that can be serviced in ThrottleSustainedDurationinSecs seconds. ThrottleSustainedDurationinSecs is recommended to be ThrottleBurstDurationinSecs multiplied by 5. This value is applied immediately and requires ThrottleEnabled to be set to Y to have effect	5	3 - 60
Throttle Sustained Event Threshold	The maximum of number of TLS connections that can be serviced in ThrottleSustainedDurationinSecs seconds. The recommended value is 100. This value is applied immediately and requires ThrottleEnabled to be set to Y to have effect	100	1 - 32767
TlsEnabled	By default, TLS is enabled. If the value is Y, it cannot be disabled. TlsEnabled is N only when ExitOnFailTLSInitialization is set to N and TLS fails to initialize. In that case, this boolean can be used to initialize TLS once the issue is resolved. Changing this value from N to Y restarts TLS initialization. The key file and certificate file must be present in order for TLS initialization to be successful. Once successful, look for the SIPS605 log. If memory allocation for TLS or the SIP Gateway application fails, then the SIP Gateway application will terminate.	Y	Y or N

Parameter Name	Description	Default Value	Range
localTLSport	The port number TLS uses on the local NGSS. Changing the default value changes the port that TLS uses.	5061	1024-65534

CAUTION
Changing this value from its default can affect call service. Do not change the TLS port number unless absolutely necessary. Port 5061 is the default port specified in the TLS standard (RFC 2246). Nortel recommends that the TLS standard be followed. Remote clients or remote peer servers may require intervention to properly (re)connect to TLS working under a different port number.

Viewing the operational status of the SIP Gateway application

Purpose of this procedure

Use the following procedure to view the service status of the SIP Gateway application.

Limitations and restrictions

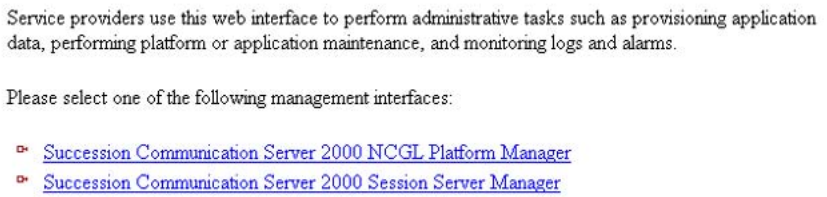
This procedure provides instructions for determining the service status of the SIP Gateway application software only. For instructions on determining the status of the platform and operating system, refer to procedure "Viewing the operational status of the NCGL platform" (page 146).

Prerequisites

There are no prerequisites for this procedure.

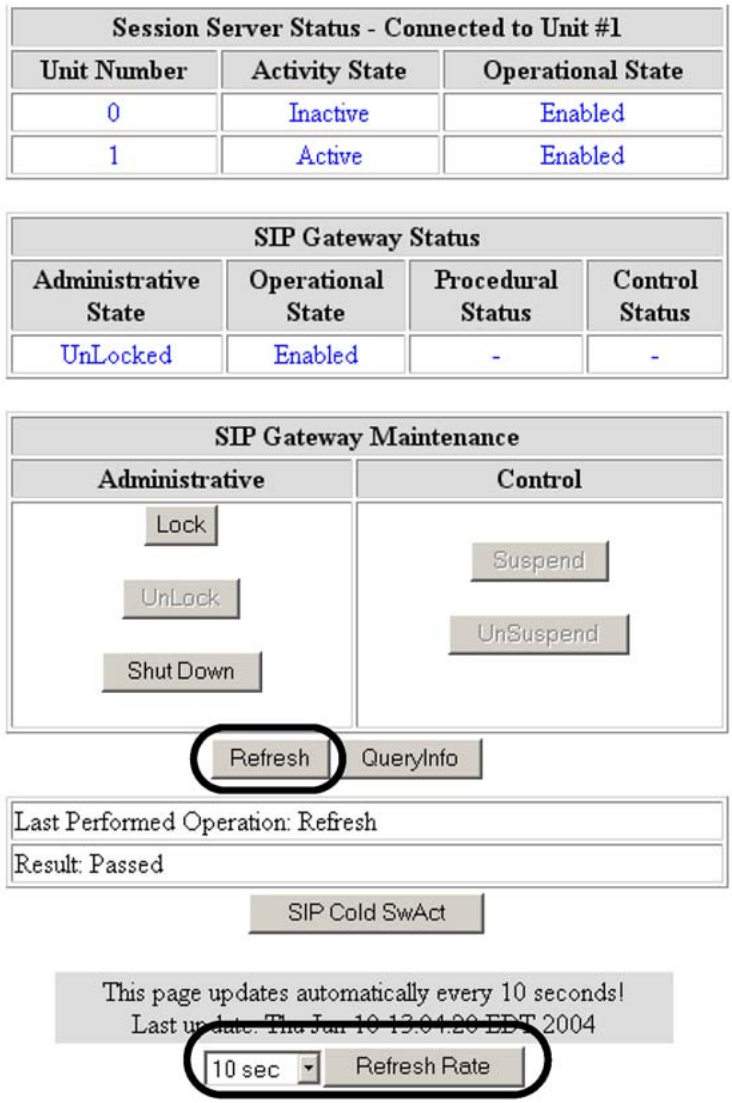
Action

Step	Action
	At the CS 2000 Session Server Manager or IEMS client
1	Select Succession Communication Server 2000 Session Server Manager from the launch point menu.



2	Select Session Server > Maintenance > Application > SIP Gateway from the left side menu.

3	Monitor the status of the SIP Gateway application from this view:



This view is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the Refresh Rate button or manually refresh the page by clicking the Refresh button.

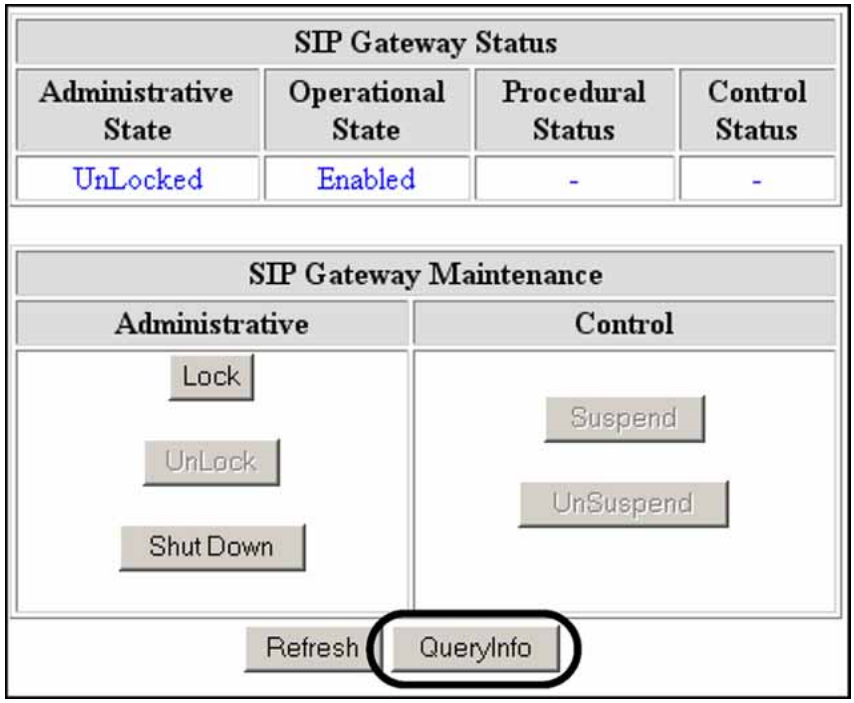
4 See "Interpreting SIP Gateway application status and maintenance fields" (page 144) to review the description of the various fields of this view.

For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section "Interpreting SIP Gateway application states" in *Session Server Trunks Security and Administration* (NN10346-611).

5 The following service affecting actions are available:

- Lock the SIP Gateway application
- Unlock the SIP Gateway application
- Suspend the SIP Gateway application
- Unsuspend the SIP Gateway application
- Cold SwAct the SIP Gateway application

6 To view the number of active calls currently being handled by the application and the synchronization status of the units, click QueryInfo.



7 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Interpreting SIP Gateway application status and maintenance fields

Use the following table to assist you in interpreting information displayed in the Status area:

Node status field descriptions

Field	Description
Unit Connection Status Bar	Indicates which unit in the node the CS 2000 Session Server Manager is connected to.
Unit Number	Identifies the two units in the node, labeled 0 and 1.
Activity State	Indicates which unit is Active and which is Inactive (standby). Also acts as an indirect indicator of fault-tolerant status; when both units have an Operational status of Enabled, the node is fault-tolerant.
Operational State	Indicates the service status of each unit, Enabled or Disabled.

Use the following table to assist you in interpreting information displayed in the SIP Gateway status area:

SIP Gateway application Status field descriptions

Field	Indication
Administrative State	Locked, Unlocked, or ShuttingDown
Operational State	Enabled or Disabled
Procedural Status	Terminating or -
Control Status	Suspended or -

Use the following table to assist you in interpreting the SIP Gateway area's CCITT X.731-style and related DMS-style status indicators:

SIP Gateway Maintenance field descriptions and interpretation of service states

Administrative State	Operational State	Procedural Status	Control Status	DMS style Service States
Locked	Disabled	-	Suspended	Offline (OFFL)
Locked	Enabled	-	-	Manual Busy(MANB)
Locked	Enabled	Terminating	-	Manual Busy Transitioning(MANBP)
Unlocked	Enabled	-	-	In Service(INSV)

Note: A dash (-) indicates a status of in-service.

Administrative State	Operational State	Procedural Status	Control Status	DMS style Service States
Unlocked	Disabled	-	-	System Busy(SYSB)
Shutting Down	Enabled	-	-	Going out of service(INSVD)

Note: A dash (-) indicates a status of in-service.

Viewing the operational status of the NCGL platform

Purpose of this procedure

Use the following procedure to view the service status of the hardware and NCGL operating system using the CS 2000 NCGL Platform Manager. This procedure can be used as a standalone task or as part of a high-level activity.

Limitations and restrictions

This procedure provides instructions for determining the service status of the SST NCGL platform only. For instructions on determining the status of the SIP Gateway application, refer to procedure "Viewing the operational status of the SIP Gateway application" (page 141).

Although some activities described in this procedure can be accomplished using the CS 2000 Session Server Manager, they are described instead using the more complete CS 2000 NGCL Platform Manager.

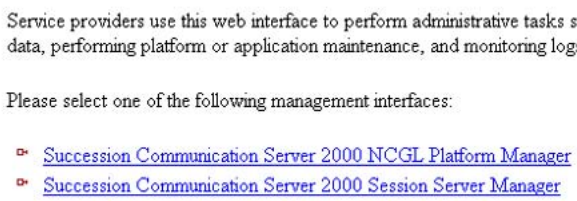
This procedure does not describe how to view customer logs or alarms. For detailed instructions about viewing customer logs or alarms, refer to procedures in *Session Server Trunks Fault Management* (NN10332-911).

Prerequisites

There are no prerequisites for using this procedure.

Action

Step	Action
	At the CS 2000 NCGL Platform Manager or IEMS client
1	Select Succession Communication Server 2000 NCGL Platform Manager from the launch point menu.



The Platform Main Page menu is displayed.

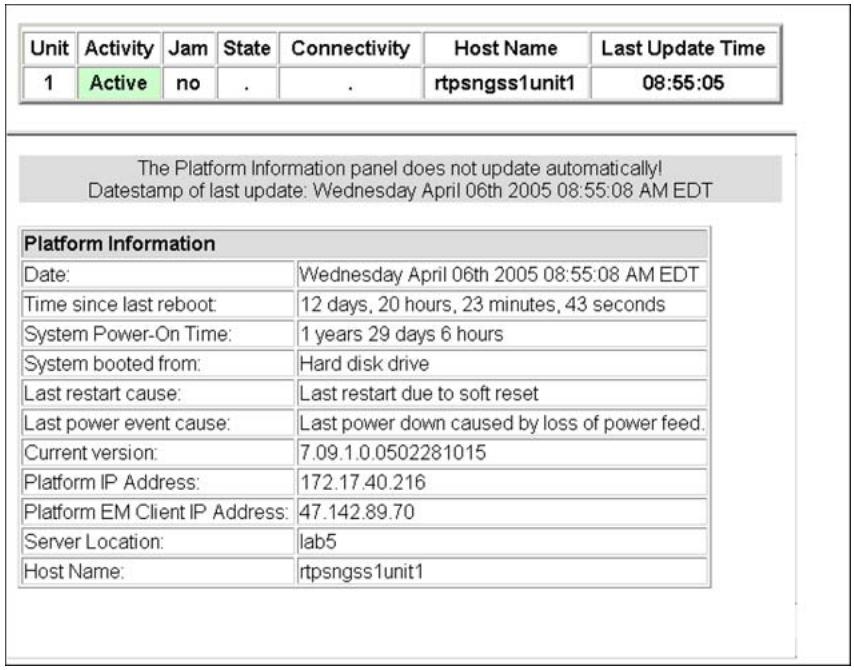
2 Use the following table to determine your next step:

If	Do
you want to review the version of the platform software load, boot statistics and platform IP address	Click the System Information link and go to step 3.
you want to review existing platform alarms	Go to step 17 and go to the procedure "Viewing SST alarms" in *Session Server Trunks Fault Management* (NN10332-911).
you want to review node maintenance status	Click the Node Maintenance link and go to step 5.
you want to review the status of system processes, CPU load and memory or related alarm thresholds	Click the System Status link and go to step 7.
you want to review the connectivity status of the network links. To perform link management activities, refer to *Session Server Trunks Security and Administration* (NN10346-611).	Click the Network Connectivity link and go to step 9.
you want to review storage related information including array status, disk capacity and disk alarm thresholds	Click the Disk Services link and go to step 10.
you want to review details about platform services including the network time protocol servers	Click the Services link and go to step 12.
you want to review platform version information only	Click the Administration link and go to step 14.
you want to review customer logs	Go to step 17 and refer to *Session Server Trunks Fault Management* (NN10332-911).
you want to change root passwords	Go to step 17 and refer to *Session Server Trunks Security and Administration* (NN10346-611).
you want to view TLS security information or manage security certificates	Go to step 17 and refer to "Managing TLS security parameters" (page 130).
you are finished reviewing information and want to log out from the GUI	step 16.

3 Review the system information page and use the following table to review the description of the various fields of the Platform (System) Information page:

ATTENTION

The Platform (System) Information panel does not update automatically. Click the System Information link again to update it.



Unit	Activity	Jam	State	Connectivity	Host Name	Last Update Time
1	Active	no	.	.	rtpsngss1unit1	08:55:05

The Platform Information panel does not update automatically!
Datestamp of last update: Wednesday April 06th 2005 08:55:08 AM EDT

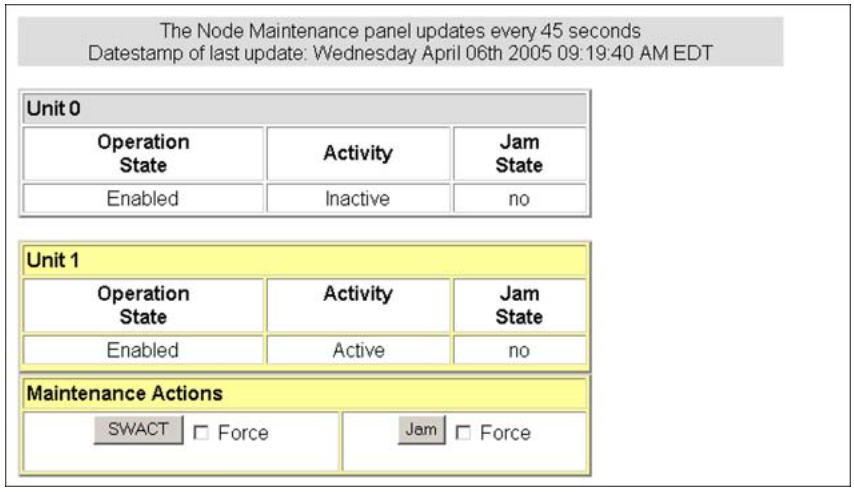
Platform Information	
Date:	Wednesday April 06th 2005 08:55:08 AM EDT
Time since last reboot:	12 days, 20 hours, 23 minutes, 43 seconds
System Power-On Time:	1 years 29 days 6 hours
System booted from:	Hard disk drive
Last restart cause:	Last restart due to soft reset
Last power event cause:	Last power down caused by loss of power feed.
Current version:	7.09.1.0.0502281015
Platform IP Address:	172.17.40.216
Platform EM Client IP Address:	47.142.89.70
Server Location:	lab5
Host Name:	rtpsngss1unit1

Field	Description
Unit	unit number in the node that you are logged into
Activity	activity of the unit (either active or standby)
Jam	indicates if the inactive unit is Jammed. The value is YES only if logged in to the inactive unit. From the active unit, the status is NO, but a JInact alarm indicates the inactive is Jammed.
State	indicates if the node is operating in a duplex (fault-tolerant) mode or a simplex mode (the standby unit is off line)
Connectivity	state of the network links on the node
Host Name	name of the unit (not node)
Date	system date as maintained by the network time protocol (NTP) server
Time since last reboot:	amount of time that has elapsed since the unit was last rebooted for any reason

Field	Description
System Power-On Time:	recorded system time that the unit has been powered up
System booted from:	indicates whether the unit is currently booted from the hard drive or DVD-ROM drive
Last restart cause:	indicates any event that forced a platform reboot (manual or system generated)
Last power event cause:	indicates any event that affected the power supply subsystem of the unit chassis
Current version:	installed version of the NCGL platform software
Platform IP Address:	unit IP address
Platform EM Client IP Address:	IP address of the client web browser. When a web proxy is used, the IP address of the machine performing the proxy is displayed
Server Location:	physical location of the unit
Host Name:	name of the unit

4 When you have completed reviewing System Information page, return to step 2.

5 Review the Node Maintenance page and use the following table to review the description of the various fields of the Node Maintenance page.

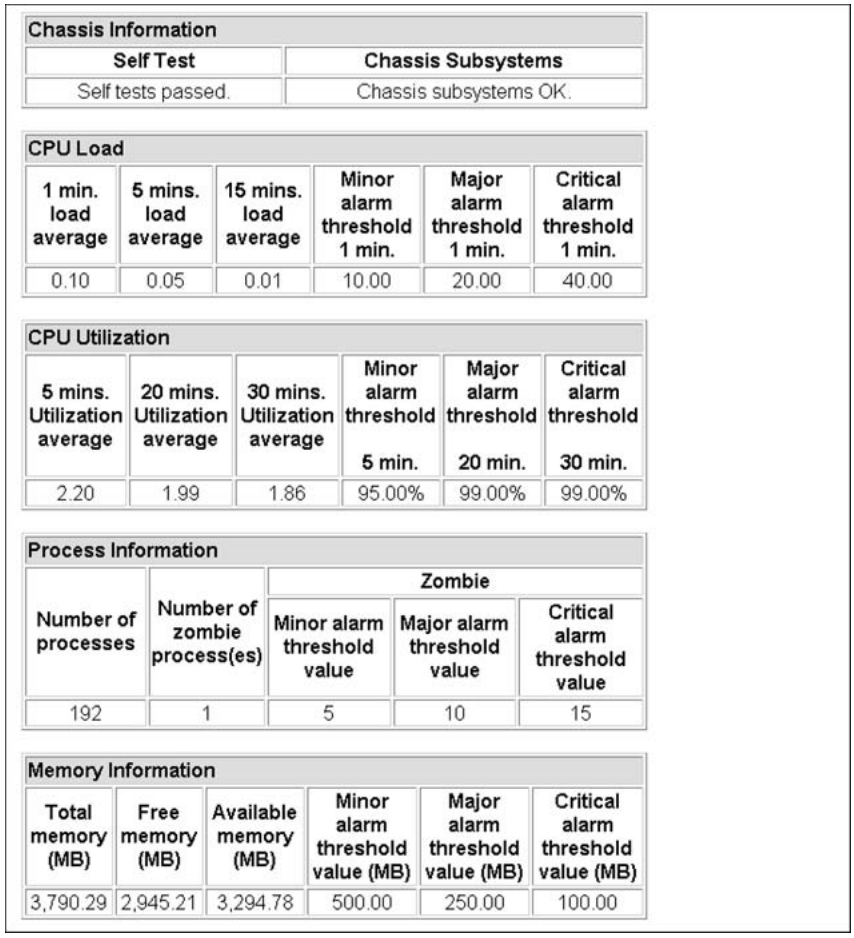


The Node Maintenance panel is refreshed every 45 seconds.

Field	Description
Operation State	indicates the operational state of the NCGL software
Activity	indicates the activity state of the platform software
Jam State	indicates if the inactive unit is Jammed
Maintenance Actions (active unit only)	maintenance panel for performing SwAct and to Jam. Refer to *Session Server Trunks Security and Administration* (NN10346-611), for procedures on performing a SwAct or Jam.

6 When you have completed reviewing the Node Maintenance page, return to step 2.

7 Review the System Status page and use the following table to review the descriptions of the various fields of the System Status page.



Chassis Information

Self Test	Chassis Subsystems
Self tests passed.	Chassis subsystems OK.

CPU Load

1 min. load average	5 mins. load average	15 mins. load average	Minor alarm threshold 1 min.	Major alarm threshold 1 min.	Critical alarm threshold 1 min.
0.10	0.05	0.01	10.00	20.00	40.00

CPU Utilization

5 mins. Utilization average	20 mins. Utilization average	30 mins. Utilization average	Minor alarm threshold 5 min.	Major alarm threshold 20 min.	Critical alarm threshold 30 min.
2.20	1.99	1.86	95.00%	99.00%	99.00%

Process Information

Number of processes	Number of zombie process(es)	Zombie		
		Minor alarm threshold value	Major alarm threshold value	Critical alarm threshold value
192	1	5	10	15

Memory Information

Total memory (MB)	Free memory (MB)	Available memory (MB)	Minor alarm threshold value (MB)	Major alarm threshold value (MB)	Critical alarm threshold value (MB)
3,790.29	2,945.21	3,294.78	500.00	250.00	100.00

The Chassis Information panel is not automatically refreshed.

Field	Description
Chassis information	
Self Test	status of the self test performed on the platform at boot up
Chassis Subsystems	status of the platform hardware subsystems including the memory, CPU, all drives, network connection, power supplies, cooling and other I/O connections
CPU Load	
Load average	indicates the 1, 5 and 15 minute load averages for the CPU utilization in percentages

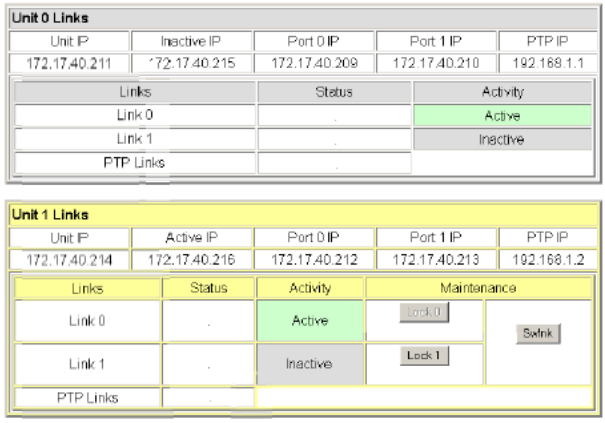
Field	Description
Load average threshold values	indicates the 1 minute CPU load average utilization threshold value in percentages. When the set threshold value is exceeded, the appropriate minor, major or critical alarm is raised.
CPU Utilization	
Utilization average	indicates the 5, 20 and 30 minute CPU utilization average in percentages. When the threshold value is exceeded, an alarm is raised.
Alarm threshold values	indicates the 5, 20 and 30 minute CPU utilization average threshold value in percentages. When the set threshold value is exceeded, an alarm is raised.
Process Information	
Number of Processes	total number of processes (non-threaded) that are running on the SST Platform
Number of zombie processes	number of defunct or terminated NCGL zombie processes. A zombie process is a process that has terminated either because it has been killed by a signal or because it has called an exit() and whose parent process has not yet received notification of its termination. A zombie process exists solely as a process table entry and consumes no other resources.
Zombie: minor alarm threshold value	maximum number of zombie processes allowed to be run by the CPU before a minor alarm is raised indicating that the set threshold has been exceeded
Zombie: major alarm threshold value	maximum number of zombie processes allowed to be run by the CPU before a major alarm is raised indicating that the set threshold has been exceeded
Zombie: critical alarm threshold value	maximum number of zombie processes allowed to be run by the CPU before a critical alarm is raised indicating that the set threshold has been exceeded
Memory Information	
Total Memory (MB)	total amount of RAM installed on the motherboard of each SST unit. Both units must have the same amount.

Field	Description
Free Memory (MB)	amount of memory available unallocated for use
Available memory (MB)	amount of memory available for programs
Minor alarm threshold value (MB)	indicates the threshold amount of available memory (in MB) that the system must drop below before a minor alarm is raised
Major alarm threshold value (MB)	indicates the threshold amount of available memory (in MB) that the system must drop below before a major alarm is raised
Critical alarm threshold value (MB)	indicates the threshold amount of available memory (in MB) that the system must drop below before a critical alarm is raised

8 When you have completed reviewing the System Status, return to step 2.

9 Review the Network Connectivity page and use the following table to review the description of the various fields of the Network Connectivity page.

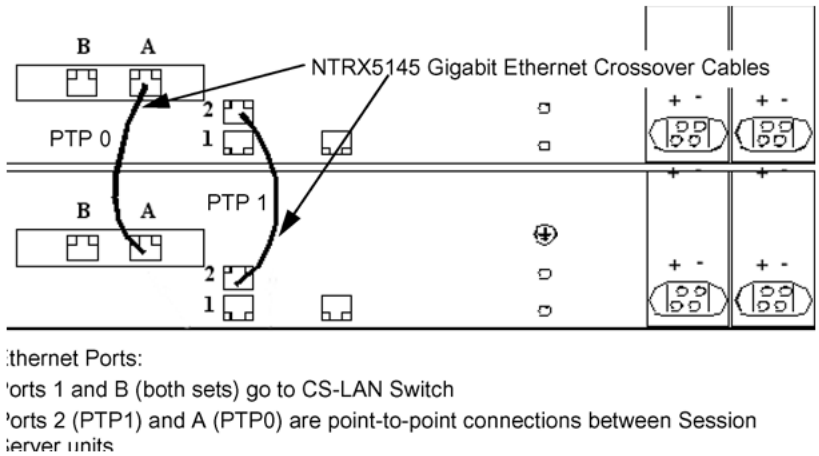
The Network Connectivity panel is refreshed every 45 seconds.



Field	Description
Unit 0,1 Links	indicates which Ethernet IP links are installed on the units (each unit has two links)
Unit 0,1 Status	status of the Ethernet links

Field	Description
Unit 0,1 Activity	activity status of the Ethernet links, either active or inactive
Unit 0,1 Maintenance	indicates the maintenance actions that can be performed on the Ethernet links, either Lock, Unlock or Swlink
Unit 0,1 PTP Links status	status of the PTP links between both units in the node
Unit IP	network IP address of the SST unit
Active IP	IP address of the local (active) SST unit
Inactive IP	IP address of the mate (inactive) SST unit
Port 0 IP	IP address of the active or inactive Ethernet port 0
Port 1 IP	IP address of the active or inactive Ethernet port 1
PTP IP	IP address of the active or inactive PTP link

Crossover and LAN Ethernet cable connections for SST units



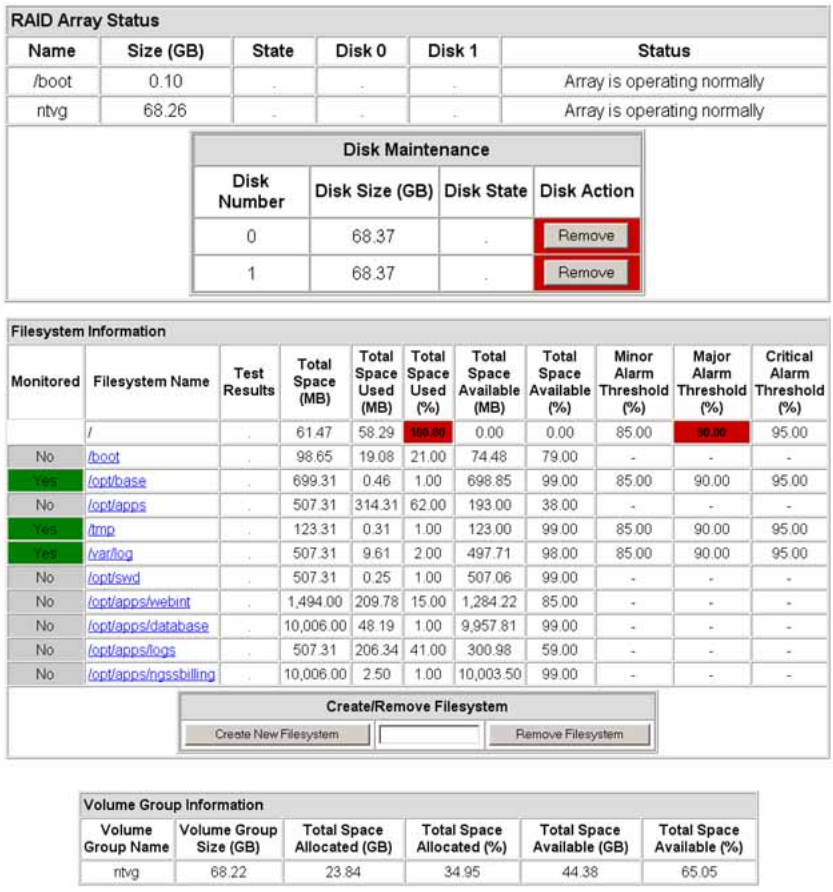
thernet Ports:
orts 1 and B (both sets) go to CS-LAN Switch
orts 2 (PTP1) and A (PTP0) are point-to-point connections between Session
erver units

10 Review the Disk Services page and use the following table to review the description of the various fields of the Disk Storage page.

ATTENTION

The Disk Services panel does not update automatically. Click the Disk Services link again to update it.

To create and remove file systems, refer to "Creating a filesystem" (page 220) and "Removing a filesystem" (page 225).



RAID Array Status

Name	Size (GB)	State	Disk 0	Disk 1	Status
/boot	0.10	.	.	.	Array is operating normally
ntvg	68.26	.	.	.	Array is operating normally

Disk Maintenance

Disk Number	Disk Size (GB)	Disk State	Disk Action
0	68.37	.	Remove
1	68.37	.	Remove

Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	Total Space Available (MB)	Total Space Available (%)	Minor Alarm Threshold (%)	Major Alarm Threshold (%)	Critical Alarm Threshold (%)
	/	.	61.47	58.29	100.00	0.00	0.00	85.00	90.00	95.00
No	/boot	.	98.65	19.08	21.00	74.48	79.00	-	-	-
Yes	/opt/base	.	699.31	0.46	1.00	698.85	99.00	85.00	90.00	95.00
No	/opt/apps	.	507.31	314.31	62.00	193.00	38.00	-	-	-
Yes	/tmp	.	123.31	0.31	1.00	123.00	99.00	85.00	90.00	95.00
Yes	/var/log	.	507.31	9.61	2.00	497.71	98.00	85.00	90.00	95.00
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00	-	-	-
No	/opt/apps/webint	.	1,494.00	209.78	15.00	1,284.22	85.00	-	-	-
No	/opt/apps/database	.	10,006.00	48.19	1.00	9,957.81	99.00	-	-	-
No	/opt/apps/logs	.	507.31	206.34	41.00	300.98	59.00	-	-	-
No	/opt/apps/ngssbilling	.	10,006.00	2.50	1.00	10,003.50	99.00	-	-	-

Create/Remove Filesystem

Create New Filesystem | Remove Filesystem

Volume Group Information

Volume Group Name	Volume Group Size (GB)	Total Space Allocated (GB)	Total Space Allocated (%)	Total Space Available (GB)	Total Space Available (%)
ntvg	68.22	23.84	34.95	44.38	65.05

Field	Description
RAID Array Status: Name	indicates the name of each RAID-1 array in the system
RAID Array Status: Size (GB)	indicates the size of the partition in gigabytes
RAID Array Status: State	Indicates a high level state for the array: - ".": indicates the array is functioning normally. - Missing: a disk was removed from the array. - Failed: a disk in the array has failed and needs to be replaced. - Rebuilding: the array is in the process of rebuilding to a fault-tolerant mode.
RAID Array Status: Disk 0	service status of disk 0
RAID Array Status: Disk 1	service status of disk 1

Field	Description
RAID Array Status: Status	Indicates the status of the array. Values are: - The array is operating normally - Missing - Failed - Rebuild
Disk Maintenance: Disk Number	indicates the disk number in the array, 0 or 1
Disk Maintenance: Disk Size (GB)	total capacity of the disk drive in gigabytes
Disk Maintenance: Disk State	installation state of the disk
Disk Maintenance: Disk Action	indicates whether a hard disk can be inserted into the RAID array
Filesystem Information: Monitor	indicates the status of individual file systems on the disk array
Filesystem Information: Filesystem Name	indicates the name of the file system on the disk array. Some file system names are reserved.
Filesystem Information: Test Results	indicates the results of any tests run on the filesystems. Tests are run approximately every 10 minutes to verify that all of the basic file system operations are working on each of the file system.
Filesystem Information: Total Space (MB)	total amount of disk space (in MB) allocated for this file system
Filesystem Information: Total Space Used (MB)	total amount of disk space (in MB) in use on this file system
Filesystem Information: Total Space Used (%)	total amount of disk space (in %) in use on this file system
Filesystem Information: Total Space Available (MB)	percentage of total disk space (in MB) free for use on this file system
Filesystem Information: Total Space Available (%)	amount of disk space (in %) available for use by platform processes and applications
Filesystem Information: Minor Alarm Threshold (%)	maximum amount of disk space (in %) that can be used before a minor alarm is raised indicating that the set threshold has been exceeded

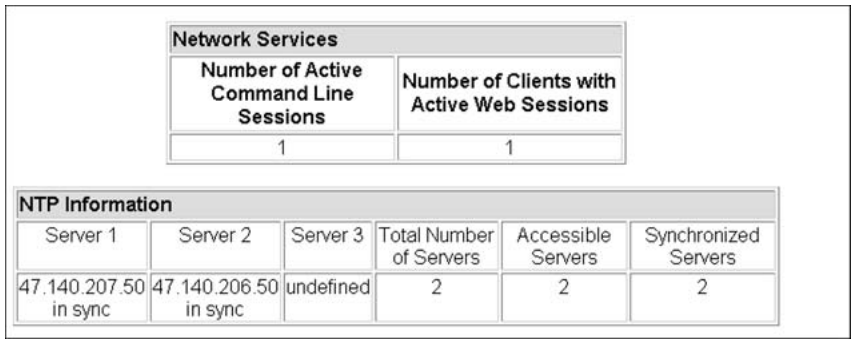
Field	Description
Filesystem Information: Major Alarm Threshold (%)	maximum amount of disk space (in %) that can be used before a major alarm is raised indicating that the set threshold has been exceeded
Filesystem Information: Critical Alarm Threshold (%)	maximum amount of disk space (in %) that can be used before a critical alarm is raised indicating that the set threshold has been exceeded
Volume Group Information: Volume Group Name	name of the volume group in the array
Volume Group Information: Volume Group Size (GB)	total size of the volume group in the array
Volume Group Information: Total Space Allocated (GB)	amount of volume group space, in gigabytes, currently allocated to file system
Volume Group Information: Total Space Allocated (%)	amount of volume group space (in %) currently allocated to file system
Volume Group Information: Total Space Available (GB)	amount of unallocated volume group space, in gigabytes, available for file system
Volume Group Information: Total Space Available (%)	amount of unallocated volume group space (in %) available for file systems

11 When you have completed reviewing the Disk Services page, return to step 2.

12 Review the Services page and use the following table to review the description of the various fields of the Platform Services page.

ATTENTION

The Services panel does not update automatically. Click the Services link again to update it.



Network Services	
Number of Active Command Line Sessions	Number of Clients with Active Web Sessions
1	1

NTP Information					
Server 1	Server 2	Server 3	Total Number of Servers	Accessible Servers	Synchronized Servers
47.140.207.50 in sync	47.140.206.50 in sync	undefined	2	2	2

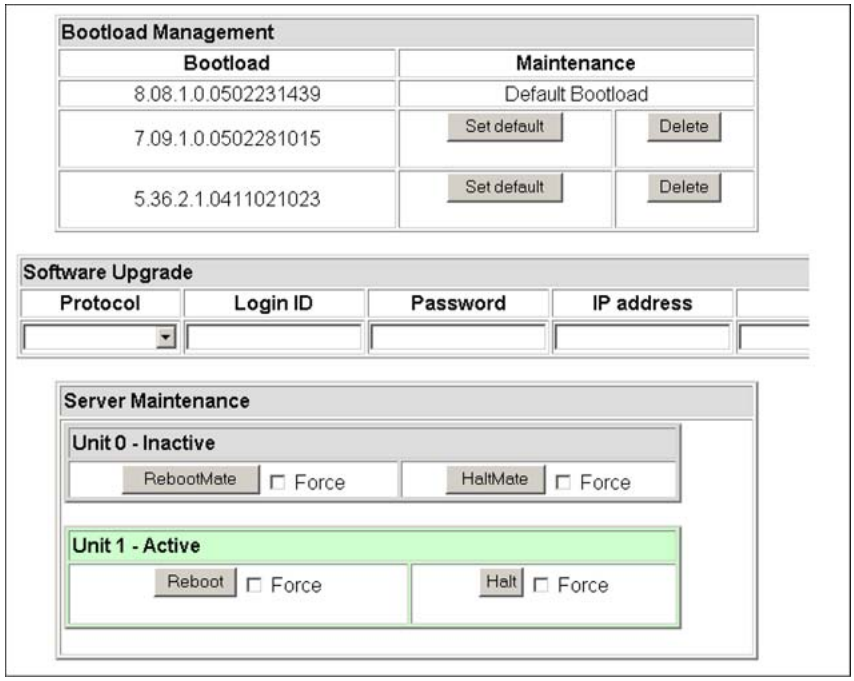
Field	Description
Network Services: Number of Active Command Line Sessions	number of command line interface (CLI) sessions (both remote and local) on the unit
Network Services: Number of Clients with Active Web Sessions	number of clients running one or more web GUI sessions
NTP Information: Server1 - Server 3	IP address of up to 3 Network Time Protocol (NTP) servers in the network, along with the status of the connection
NTP Information: Total Number of Servers	number of NTP servers registered with the CS-LAN network
NTP Information: Accessible Servers	number of NTP servers accessible to the SST
NTP Information: Synchronized Servers	number of NTP servers to which the unit is synchronized

13 When you have completed reviewing Platform Services status, return to step 2.

14 Review the Administration page and use the following table to review the description of the various fields of the Administration page:

ATTENTION

The Administration panel does not update automatically. Click the link again to update it.



Field	Description
Bootload Management: Bootload	load ID for the NCGL platform software load
Bootload Management: Maintenance	indicates whether the Bootload is the default. Can also allow choosing a new default bootload if there is more than one load available. Additional loads can come from maintenance releases.
Software Upgrade: Protocol	file transfer protocol or source location for the platform software upgrade: FTP, Anonymous FTP, HTTP, HTTPS, Local File, Local CD-ROM
Software Upgrade: Login ID	If a login ID is required to access the upgrade platform load from another server in the network, a login ID can be entered here.
Software Upgrade: Password	If a password is required to access the upgrade platform load from another server in the network, a password can be entered here.
Software Upgrade: IP Address	If it is required to access the upgrade platform load from another server in the network, an IP address can be entered here.

Field	Description
Software Upgrade: File	The target upgrade load path and filename is entered here.
Software Upgrade: ActionUpgrade button	The Upgrade button initiates a platform NCGL upgrade.
Server Maintenance (active and inactive units)	used to execute the Reboot, Halt, Rebootmate, and Haltmate functions. These are service affecting commands.

15 When you have completed reviewing the Administration page, return to step 2, or continue with step 16.

16 If you want to logout from CS 2000 NCGL Platform Manager, click the Logout button.

You are returned to the login page

17 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Locking the SIP Gateway application

Purpose of this procedure

Use the following procedure to change the administrative status of the SIP Gateway application to Locked.

Limitations and restrictions

This procedure provides instructions for changing the service status of the SIP Gateway application software only. The NCGL operating status is not affected.

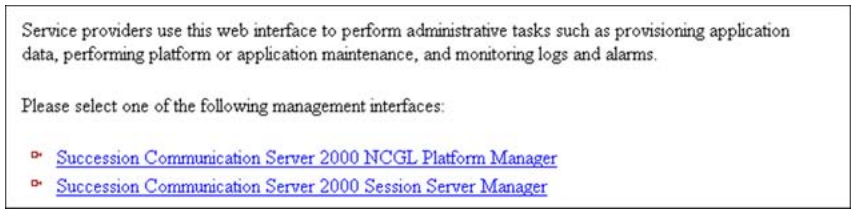
CAUTION
This is a service affecting procedure. Locking the SIP Gateway application releases all SIP calls in progress, regardless of call state, and causes an outage of all SIP media communications.

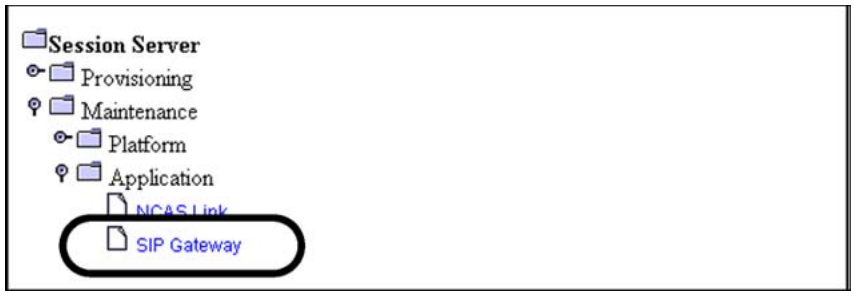
Prerequisites

There are no prerequisites for this procedure.

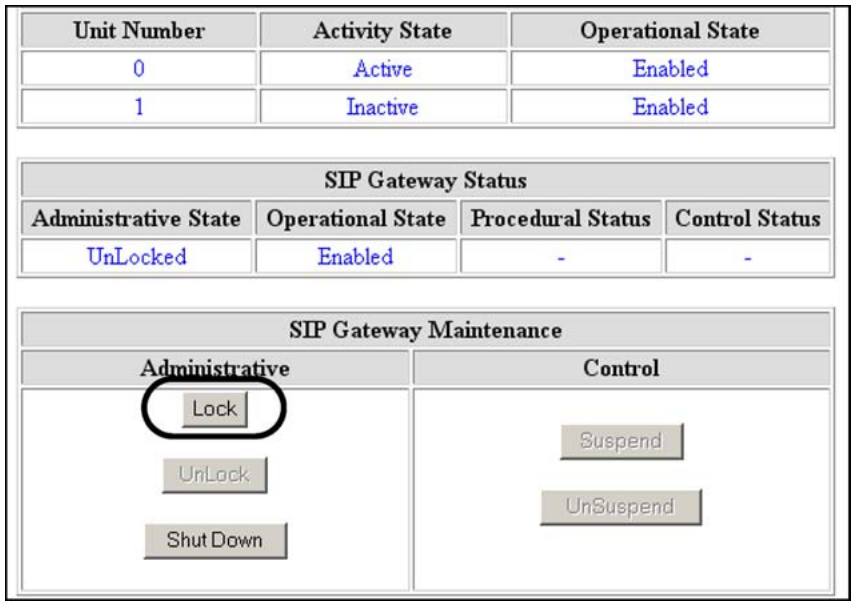
Action

Step	Action
	At the CS 2000 Session Server Manager or IEMS client
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.
2	Select **Session Server > Maintenance > Application > SIP Gateway**.





3 In the SIP Gateway panel click the Lock button.

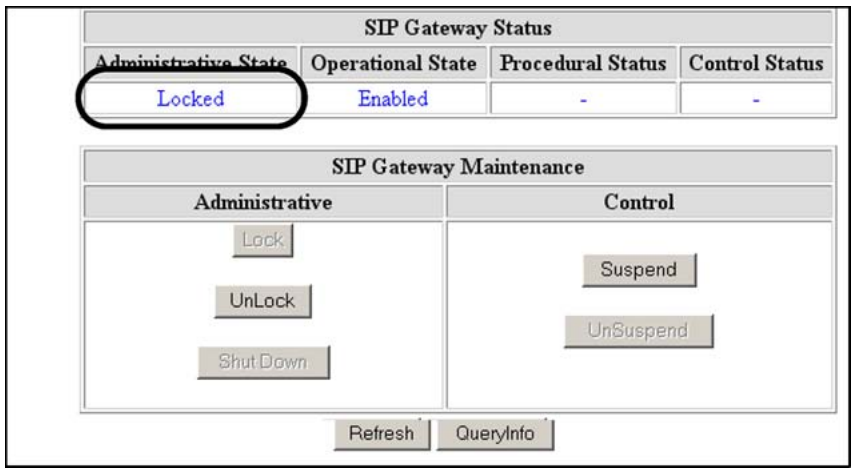


The system responds:

```
This action will release all existing SIP calls and
will cause a SERVICE OUTAGE on this Session Server.
There are x active calls.  Do you wish to continue?
```

4 Click **OK** to confirm locking the SIP Gateway application.

5 Monitor the status of the SIP Gateway application and ensure the Administrative State changes to Locked.



The status panel is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the Refresh Rate button. Otherwise, manually refresh the page by clicking on the Refresh button.

6 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Unlocking the SIP Gateway application

Purpose of this procedure

Use the following procedure to change the administrative status of the SIP Gateway application to Unlocked, bringing the application into service and enabling call processing to begin.

For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section of *Session Server Trunks Security and Administration* (NN10346-611).

Limitations and restrictions

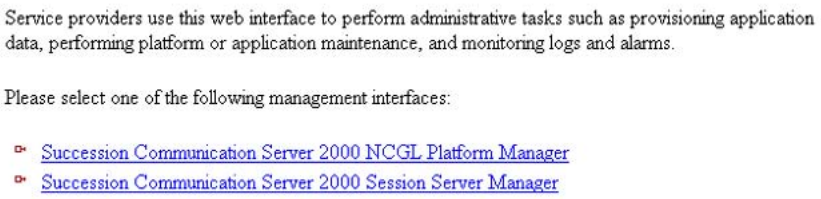
This procedure provides instructions for changing the service status of the SIP Gateway application software only. For instructions on determining the status of the platform and operating system, refer to procedure "Viewing the operational status of the NCGL platform" (page 146).

Prerequisites

The active unit must be in a locked Administrative state. If it is not locked or you are uncertain of the state of the application, refer to procedure "Locking the SIP Gateway application" (page 161).

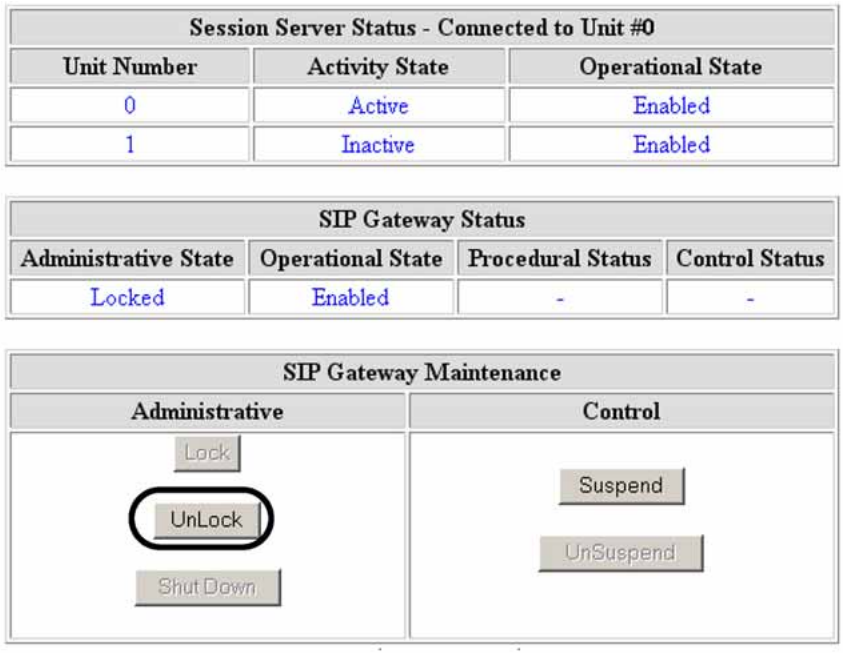
Action

Step	Action
	At the CS 2000 Session Server Manager or IEMS client
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



2	Select **Session Server > Maintenance > Application > SIP Gateway** from the left side menu:

3 In the SIP Gateway panel click **Unlock**.

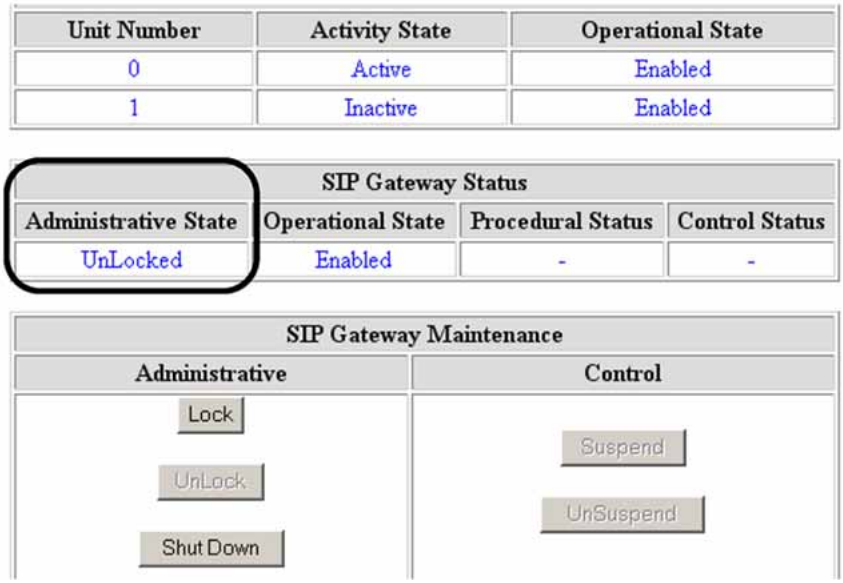


Session Server Status - Connected to Unit #0		
Unit Number	Activity State	Operational State
0	Active	Enabled
1	Inactive	Enabled

SIP Gateway Status			
Administrative State	Operational State	Procedural Status	Control Status
Locked	Enabled	-	-

SIP Gateway Maintenance	
Administrative	Control
Lock UnLock Shut Down	Suspend UnSuspend

4 Monitor the status of the SIP Gateway application in the SIP Gateway Status box and ensure the Administrative State changes to Unlocked.



Unit Number	Activity State	Operational State
0	Active	Enabled
1	Inactive	Enabled

SIP Gateway Status			
Administrative State	Operational State	Procedural Status	Control Status
UnLocked	Enabled	-	-

SIP Gateway Maintenance	
Administrative	Control
Lock UnLock Shut Down	Suspend UnSuspend

The status panel is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the Refresh Rate button. Otherwise, manually refresh the page by clicking on the Refresh button.

5 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Suspending the SIP Gateway application

Purpose of this procedure

Use the following procedure to temporarily take the SIP Gateway application out of service. This activity must be performed whenever selected SIP Gateway application provisioning changes are made and the application must be restarted for the changes to take effect.

For more detailed information about SIP Gateway application services states and administrative functions, refer to "Interpreting SIP Gateway application states" in the *Session Server Trunks Security and Administration* (NN10346-611).

Limitations and restrictions

This procedure can only be performed when the SIP Gateway application is in the following service states:

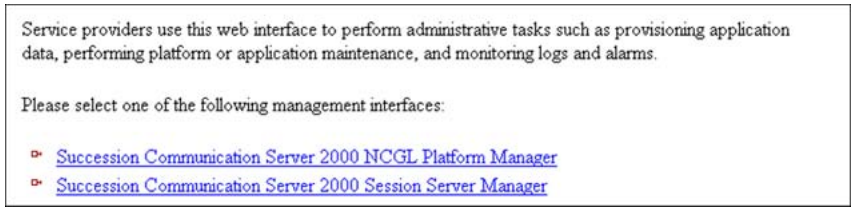
- the Operational State is Enabled
- the Administrative State is Locked

Prerequisites

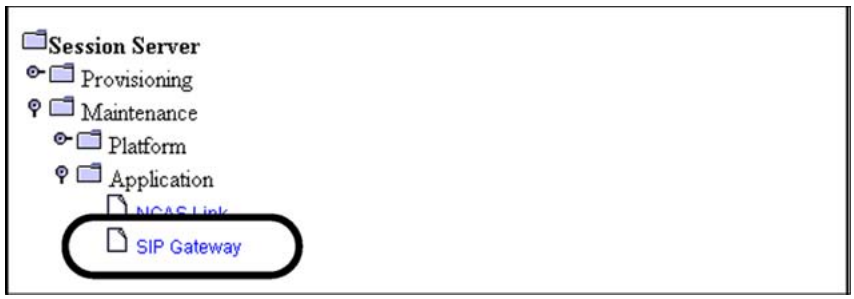
The SIP Gateway application must previously have been locked. If it is not locked or you are uncertain of the state of the application, refer to procedure "Locking the SIP Gateway application" (page 161).

Action

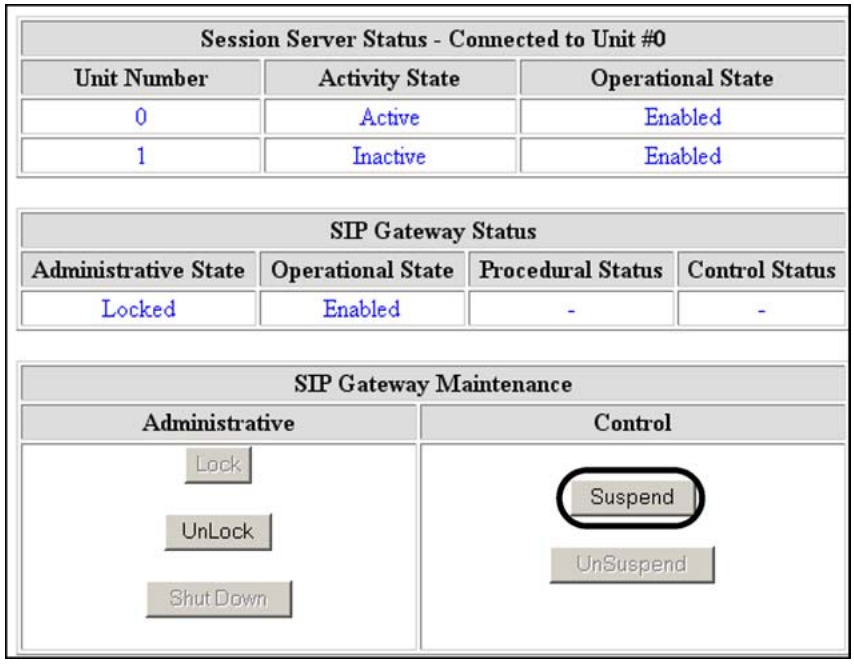
Step	Action
	At the CS 2000 Session Server Manager or IEMS client
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



2	Select **Session Server > Maintenance > Application > SIP Gateway** from the left side menu:

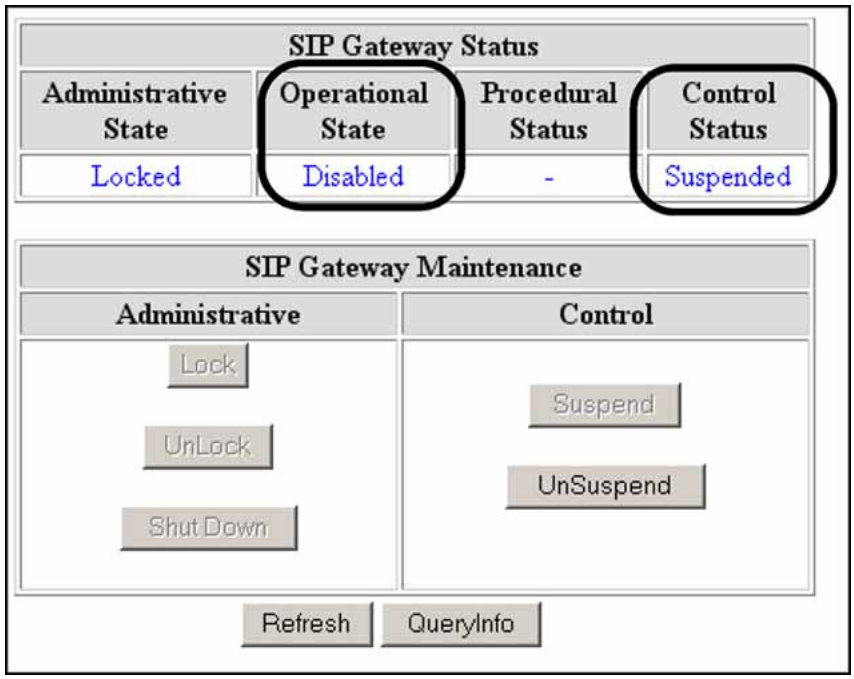


3 In the SIP Gateway panel click **Suspend**.



4 Monitor the status of the SIP Gateway application in the SIP Gateway Status box:

- the Operational State changes to Disabled
- the Control Status changes to Suspended



5 If applicable, restart the SIP Gateway application by executing procedures "Unsuspending the SIP Gateway application" (page 170) and "Unlocking the SIP Gateway application" (page 164), in the order shown.

6 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Unsuspending the SIP Gateway application

Purpose of this procedure

Use the following procedure to bring the SIP Gateway application back into service without restarting callP activity.

For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section "Interpreting SIP Gateway application states" in *Session Server Trunks Security and Administration* (NN10346-611).

Limitations and restrictions

This procedure can only be performed when the SIP Gateway application is in the following service states:

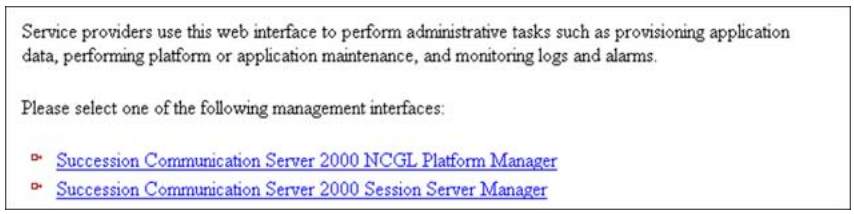
- the Operational State is Disabled
- the Administrative State is Locked
- the Control Status is Suspended

Prerequisites

The SIP Gateway application must previously have been suspended. If it is not suspended or you are uncertain of the state of the application, refer to procedure "Suspending the SIP Gateway application" (page 167).

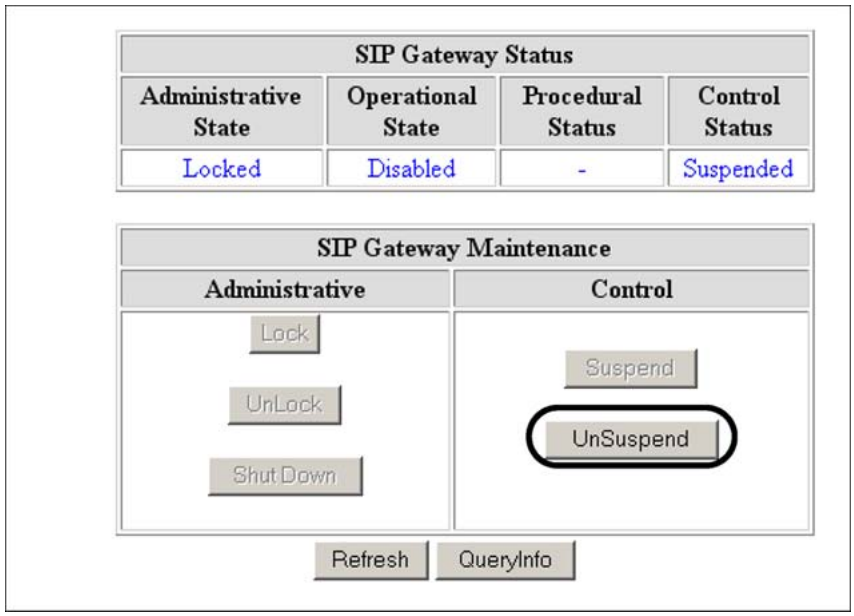
Action

Step	Action
	At the CS 2000 Session Server Manager or IEMS client
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



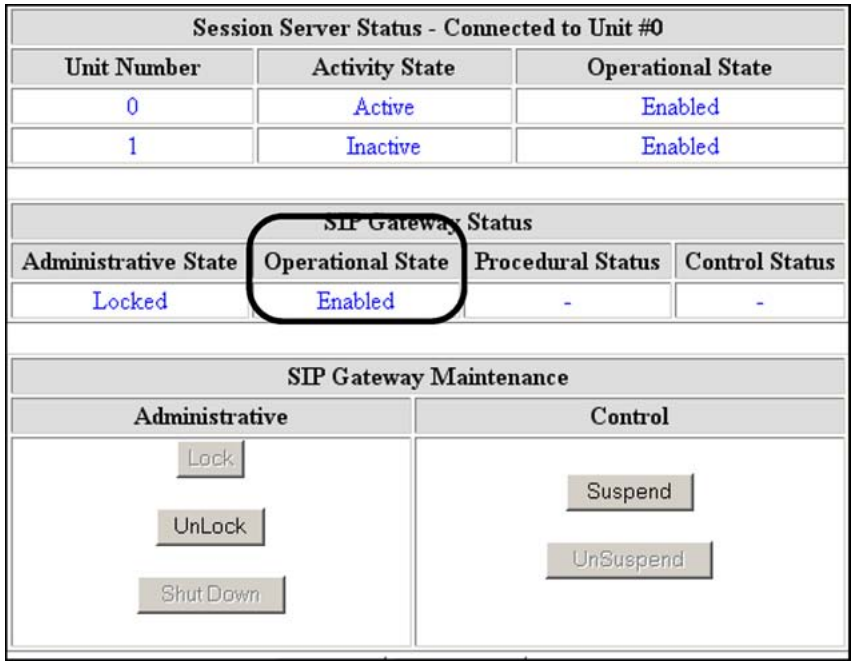
2	Select **Session Server > Maintenance > Application > SIP Gateway** from the left side menu:

3 In the SIP Gateway panel click **Unsuspend**.



4 Monitor the status of the SIP Gateway application in the SIP Gateway Status box:

- the Operational State changes to Enabled
- the Control status changes to



5 If necessary, bring the SIP Gateway application back into service by executing procedure "Unlocking the SIP Gateway application" (page 164).

6 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Modifying DPT trunk group connections supported by the SIP Gateway application

Purpose of this procedure

Use the following procedure to modify core table DPTRKMEM to change the maximum number of call connections that can be handled by a specific DPT trunk group managed by SST.

Limitations and restrictions

Do not use this procedure to add trunk groups to the network. To add trunk groups, refer to procedure "Provisioning SIP-T DPTs in an office with a Session Server," found in the CS 2000 Configuration NTP applicable to your solution.

Prerequisites

You must be able to calculate the MAXCALLS value for DPTRKMEM, based on the amount of traffic that the particular trunk group is expected to handle. This calculation is similar to the calculation used to determine the number of trunk members needed for a particular TDM trunk group. The calculated value must be high enough to support the maximum number of DPT simultaneous calls you want the trunk group to handle. For more information, consult your Engineering Guidelines or the CS 2000 Configuration NTP applicable to your solution.

Action

Step	Action
	At a MAPCI console connected to the Call Server
1	Refer to procedure *Using the table editor to edit an existing tuple in a table* found in the CS 2000 Configuration NTP applicable to your solution to modify field MAXCALLS in table DPTRKMEM to increase the number of connections handled by an existing trunk group using the MAXCALLS Entry.
2	Refer to procedure "Adding and managing telephony profiles" (page 68) and verify whether the values for the usage limit for either SOC CS2B0008 or SOC CS2B0009 need to be adjusted based on the changes you made to the trunk group limits.

—End—

Modifying SST maximum DPT call limits

Purpose of this procedure

Use the following procedure to modify the several core usage SOC options (CS2B0008 and CS2B0009) that are used to limit the maximum number of simultaneous calls that are allowed through the SST.

- The usage-controlled CS2B0008 SOC uses a peg counter that keeps track of DPT connections using SIP-T signaling that are routed from call server-to-call server or between a call server and a MCS 5200.
- The usage-controlled CS2B0009 SOC uses a peg counter that keeps track of DPT connections using SIP-T signaling that are routed from any 3rd party application server to a call server.
- The usage-controlled base DPT CS2B0005 SOC uses a peg counter that keeps track of the total of all DPT connections regardless of connection type. In general, the sum of the counters for each of the CS2B0009 and CS2B0008 SOCs is equal to the value of the counter of the CS2B0005 SOC. The value of the CS2B0005 SOC sets office parameter DPT_MAX_PORTS in table OFCVAR.

Each of the counters keep track of the current number of calls matching the above criteria. For each new call of either type, the current value in the respective counter is checked against the limiting value in the SOC. If the addition of a new call would exceed the SOC limit, the call is sent to treatment; otherwise, the counter is incremented and the call is allowed to proceed. When the call is ended, the counter is decremented.

Limitations and restrictions

If the SOC limit set for CS2B0008 or CS2B0009 exceeds the limit of the Base DPT SOC CS2B0005, the CS2B0005 is the limiting factor in determining the maximum number of simultaneous calls regardless of call type. In such cases where the number of calls of either type exceeds the total number of allowable DPT calls set by the CS2B0005 SOC, consider increasing the usage-limit value in the CS2B0005 SOC.

OM field CS2ASOVF in XA-Core OM group NGSSOM is used to measure the number of times the CS2B0009 SOC limit call count setting is exceeded.

Prerequisites

There are no prerequisites for performing this procedure.

Action

Step	Action
	At a MAPCI console connected to the Call Server
1	Use procedure *Assigning a usage limit to an option*, found in the DMS-Series Software Optionality Control User Manual, NTP 297-8991-901, to change the usage limit for any one of the following SOCs: • Base DPT SOC CS2B0005 • Call Server-to-Call Server (VRDN) DPT SOC CS2B0008 • Call Server-to-SIP Application Server DPT SOC CS2B0009 **ATTENTION** You must have access to your SOC key code assigned by Nortel (made up of 20 alphanumeric characters) and the SOC order code assigned by Nortel (made up of 8 alphanumeric characters) for setting a usage limit for any of these SOC options.
2	If you changed the usage limit for either SOC CS2B0008 or SOC CS2B0009, refer to procedure "Configuring SIP Gateway application parameters" (page 46) and ensure that the value for field parameter maxCallLegs is updated to match the sum of the usage limit values entered for both SOC CS2B0008 and SOC CS2B0009 call types.
	—End—

Adding an SST node to the SPFS server web proxy

Purpose of this procedure

Use the following activity to add web proxy services to the SPFS server, (part of the CS 2000 Management Tools server) for supporting an SST node or to replace an existing web proxy entry for an SST entry with updated values like a new IP address or tagname.

Limitations and restrictions

DNS services are enabled on the CS 2000 Management Tools server. However, if you get an error message asking you to enable DNS while executing this procedure, quit the procedure, then complete procedure Configuring the Domain Name Service on a Sun server found in the *Nortel ATM/IP Solution-level Configuration* (NN10409-500).

CAUTION
Executing this activity causes the Apache web service to stop and start multiple times.

You cannot modify existing web proxy entries. If you want to change web proxy IP addresses or tag names for an existing SST node, add new web proxy entries for the node using the new values. Deleting the old entries is not necessary.

Prerequisites

Ensure that the account you use to log into the CS 2000 Management Tools server has root privileges.

Observe all limitations and prerequisites applicable to other procedures referenced in this activity.

See "Understanding SST node IP addressing" (page 12) for more information about SST IP addressing and naming schemes needed to complete this activity. The following IP addresses are referenced in this activity:

- Unit 0 (the IP address of physical unit0)
- Unit 1 (the IP address of physical unit 1)
- Active unit (the IP address of the logically active unit, also used for accessing the CS 2000 Session Server Manager GUI)

Action

Step	Action
	At the applicable network element interface
1	Verify that an HTTPS Certificate has been installed on the CS 2000 Management Tools Server SPFS platform. For assistance use procedure *Installing an HTTPS certificate on a Sun server* found in the *Nortel Carrier Voice over IP Upgrade and Patches* (NN10440-450) or the *Nortel ATM/IP Solution-level Administration and Security* (NN10402-600).
2	Log onto the CS 2000 Management Tools server and complete the following sub-steps to add the SST node to the proxy. If needed, you can refer to procedure *Configuring the Apache Web Server for HTTPS proxy*, in the *Nortel ATM/IP Solution-level Configuration* (NN10409-500).
3	Change to the root user by typing **`su - root`** and pressing the Enter key.
4	Enter the root password and press Enter.

5	Start the command line interface application by typing
	`cli`
	and pressing the Enter key.
	The system responds:
	`Command Line Interface`
	`1 - View`
	`2 - Configuration`
	`3 - Other`
	`X - exit`
	`select -`

6	Access the Configuration level by typing
	`2`
	and pressing the Enter key.
	The system responds:
	`Configuration`
	`1 - NTP Configuration`
	`2 - Apache Proxy Configuration`
	`3 - DCE Configuration`
	`.`

```
   .
   .
   18 - snmp_poller (SNMP Poller Configuration)
   X - exit
select -
```

7 Access the Apache Proxy Configuration level by typing

2

and pressing the Enter key.

The system responds:

```
Apache Proxy Configuration
1 - add_proxy_conf (Add an IP to the Apache Proxy
Module configuration)
2 - del_proxy_conf (Delete an IP from the Apache Proxy
Module configuration)
3 - list_proxy_conf (List the Apache Proxy Module
configuration)
X - exit
select -
```

8 Complete the following sub-steps to add a Session Server physical **Unit 0** to the proxy.

a. Add Session Server Unit 0 to the Apache Proxy Module configuration by typing

1

and pressing the Enter key.

The system responds:

```
=== Executing "add_proxy_conf"
```

b. Enter the IP address for Session Server Unit 0 and press the Enter key.

c. Enter the same IP address for the hostname/tag associated with Session Server Unit 0 and press the Enter key.

d. Skip entering (leave blank) the optional remote hostname/tag associated with Unit 0 by pressing the Enter key.

e. Enter the port number associated with the IP address for Session Server Unit 0 and press the Enter key.

Use "443" for the port number.

Sample system response:

```
Accept the following values:
    IP Address = 10.65.99.67
    Hostname   = 10.65.99.67
```

```
    Remote Tag =
    Port Num    = 443
!!WARNING!! This will result in WEBSERVER going down
(restarting) for a short time.Continue? [Y/N]:
```

f. Confirm the values you entered for Session Server Unit 0 by typing

y

and pressing the Enter key.

The Apache web service stops and restarts, then returns to the Apache Proxy Configuration menu.

9 Complete the following sub-steps for the Session Server physical **Unit 1** to the proxy.

a. Add Session Server Unit 1 to the Apache Proxy Module configuration by typing

1

and pressing the Enter key.

The system responds:

```
=== Executing "add_proxy_conf"
```

b. Enter the IP address for Session Server Unit 1 and press the Enter key.

c. Enter the same IP address for the hostname/tag associated with Session Server Unit 1 and press the Enter key.

d. Skip entering (leave blank) the optional remote hostname/tag associated with Unit 1 by pressing the Enter key.

e. Enter the port number associated with the IP address for Session Server Unit 1 and press the Enter key.

Use "443" for the port number.

Sample system response:

```
Accept the following values:
    IP Address = 10.65.99.70
    Hostname   = 10.65.99.70
    Remote Tag =
    Port Num   = 443
!!WARNING!! This will result in WEBSERVER going down
(restarting) for a short time.Continue? [Y/N]:
```

f. Confirm the values you entered for the Unit 1 by typing

y

and pressing the Enter key.

The Apache web service stops and restarts, then returns to the Apache Proxy Configuration menu.

10 Complete the following sub-steps to add a Session Server logically **Active** unit to the proxy.

a. Add a Session Server active unit to the Apache Proxy Module configuration by typing

1

and pressing the Enter key.

The system responds:

```
=== Executing "add_proxy_conf"
```

b. Enter the IP address for the Session Server active unit and press the Enter key.

c. Enter the same IP address for the hostname/tag associated with the active unit and press the Enter key.

d. Skip entering (leave blank) the optional remote hostname/tag associated with the active unit by pressing the Enter key.

e. Enter the port number associated with the IP address for Session Server active unit and press the Enter key.

Use "443" for the port number.

Sample system response:

```
Accept the following values:
    IP Address = 10.65.99.72
    Hostname   = 10.65.99.72
    Remote Tag =
    Port Num   = 443
!!WARNING!! This will result in WEBSERVER going down
(restarting) for a short time.Continue? [Y/N]:
```

f. Confirm the values you entered for the active Session Server unit by typing

Y

and pressing the Enter key.

The Apache web service stops and restarts, then returns to the Apache Proxy Configuration menu.

11 Complete the following sub-steps to add an entry for the CS 2000 Session Server Manager GUI to the proxy.

a. From the Apache Proxy Configuration level, add the CS 2000 Session Server Manager GUI to the Apache Proxy Module configuration by typing

1

and pressing the Enter key.

The system responds:

```
=== Executing "add_proxy_conf"
```

b. Enter the IP address for the Session Server active unit and press the Enter key.

The CS 2000 Session Server Manager GUI must always be loaded from the active Session Server unit.

c. Enter the Session Server tagname for the hostname/tag associated with the Session Server active unit and press the Enter key.

ATTENTION

The tagname entered here must be the same one entered on both Session Server units when the application was installed. If the correct tagname is not entered, you will be unable to access the CS 2000 Session Server Manager GUI.

d. Enter the Session Server tagname for the remote hostname/tag associated with the Session Server active unit and press the Enter key.

e. Enter the port number associated with the proxy IP address for active unit's CS 2000 Session Server Manager GUI and press the Enter key.

For the port number, use "8443".

Sample system response:

```
Accept the following values:
    IP Address = 10.65.99.72
    Hostname   = prov
    Remote Tag = prov
    Port Num   = 8443
!!WARNING!! This will result in WEBSERVER going down
(restarting) for a short time.Continue? [Y/N]:
```

f. Confirm the values you entered for the active unit by typing

Y

and pressing the Enter key.

The Apache web service stops and restarts, then returns to the Apache Proxy Configuration menu.

12 Exit the Apache Proxy Configuration level by typing

x

and pressing the Enter key.

You are returned to the SPFS operating system.

13 Exit the Configuration level by typing

x

and pressing the Enter key.

You are returned to the SPFS operating system.

14 Exit the CLI by typing

x

and pressing the Enter key.

You are returned to the SPFS operating system.

15 If applicable, logout from the workstation.

At a Session Server command line interface (CLI)

16 Use procedure "Modifying NCGL platform provisioning" (page 202), found in this NTP to configure the SNMP trap IP address and the web proxy IP address of the IEMS server on the Session Server.

—End—

Using multiple tag names for multiple SST nodes

Starting in SN08, multiple SST nodes (made of the active and inactive units) are allowed in the same CS-LAN network. Therefore, as a rule, you must use a different tag name for each node installed in the network. Ensure that the tag name used in the web proxy entry is the correct one for that node, based on the tag name entered when the node was installed. For assistance, match the tag name to the active unit IP addresses used in the web proxy entry to ensure a correct match. Failure to follow this rule will prevent you from accessing a node's GUIs properly.

The following figure shows the anatomy of a web proxy configuration file for a two SST nodes. The first node uses the prov tag name. The second node uses the *ss-sipapp2* tag name. The tag name values were selected when installing SST. The use of unique tag names allows multiple SST

nodes, each with two physical units (active and inactive), to co-exist in the same CS-LAN network. Both physical units in the node must use the same tag name.

The tag name for this (first) Session Server node proxy entry is **prov**

ProxyPass /10.65.99.67/ https://10.65.99.67:443/	Entry for physical unit 0
ProxyPassReverse /10.65.99.67/ https://10.65.99.67:443/	
ProxyPass /10.65.99.70/ https://10.65.99.70:443/	Entry for physical Unit 1
ProxyPassReverse /10.65.99.70/ https://10.65.99.70:443/	
ProxyPass /10.65.99.72/ https://10.65.99.72:443/	Entry for active unit
ProxyPassReverse /10.65.99.72/ https://10.65.99.72:443/	
*ProxyPass /**prov**/ https://10.67.99.72:8443/**prov**/*	Entry for active unit GUI
*ProxyPassReverse /**prov**/ https://10.67.99.72:8443/**prov**/*	

The tag name for this second Session Server node proxy entry is **ss-sipapp2**

ProxyPass /172.65.99.67/ https://172.65.99.67:443/	Entry for physical unit 0
ProxyPassReverse /172.65.99.67/ https://172.65.99.67:443/	
ProxyPass /172.65.99.70/ https://172.65.99.70:443/	Entry for physical unit 1
ProxyPassReverse /172.65.99.70/ https://172.65.99.70:443/	
ProxyPass /172.65.99.72/ https://172.65.99.72:443/	Entry for active unit
ProxyPassReverse /172.65.99.72/ https://172.65.99.72:443/	
ProxyPass /**ss-sipapp2**/ https://172.67.99.72:8443/**ss-sipapp2**/	Entry for active unit GUI
ProxyPassReverse /**ss-sipapp2**/ https://172.67.99.72:8443/**ss-sipapp2**/	

Viewing web proxy settings in SPFS for SST

Purpose of this procedure

Use the following activity to view the configuration of existing node web proxy services on the SPFS server (part of the CS 2000 Management Tools server).

Limitations and restrictions

If the web proxy entry for a particular node requires changing, you must configure a new proxy entry with the modified values, then remove the obsolete proxy entry. Do not use this procedure to add a new node to the proxy service configuration. To perform this activity, refer to procedure "Adding an SST node to the SPFS server web proxy" (page 176).

Prerequisites

Ensure that the account you use to log into the CS 2000 Management Tools server has root privileges.

Observe all limitations and prerequisites applicable to other procedures referenced in this activity.

For more information about IP addressing and naming schemes needed to complete this activity, see "Understanding SST node IP addressing" (page 12). The following IP addresses are referenced in this activity:

- Unit 0 (the IP address of physical unit0)
- Unit 1 (the IP address of physical unit 1)
- Active unit (the IP address of the logically active unit, also used for accessing the CS 2000 Session Server Manager)

Action

Step	Action
	At the NCGL CLI or IEMS client
1	Verify that a security certificate has been installed on the CS 2000 Management Tools Server SPFS platform. For assistance use procedure "Installing an HTTPS certificate on a Sun server" in *Nortel Carrier Voice over IP Upgrade and Patches* (NN10440-450).
2	Log in to the CS 2000 Management Tools server.
3	Change to the root user by typing `su - root`

4 Enter the **root** password and press Enter.

5 Start the command line interface application:

cli

The system responds:

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

6 Access the Configuration level:

2

The system responds:

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
.
.
18 - snmp_poller (SNMP Poller Configuration)
X - exit
select -
```

7 Access the Apache Proxy Configuration level:

2

The system responds:

```
Apache Proxy Configuration
1 - add_proxy_conf (Add an IP to the Apache Proxy
Module configuration)
2 - del_proxy_conf (Delete an IP from the Apache Proxy
Module configuration)
3 - list_proxy_conf (List the Apache Proxy Module
configuration)
X - exit
select -
```

8 List the current Apache Proxy Configuration entries:

3

The system responds:

```
=== Executing "list_proxy_conf"
#Begin Proxy Config
<IfModule mod_proxy.c>
   ProxyRequests On
   # Add Proxy Entries Here
```

```
   ProxyPass /47.174.74.184/ https://47.174.74.184:443/
   ProxyPassReverse /47.174.74.184/
https://47.174.74.184:443/
   ProxyPass /47.142.209.118/
https://47.142.209.118:443/
  ProxyPassReverse /47.142.209.118/
https://47.142.209.118:443/
   ProxyPass /47.142.209.116/
https://47.142.209.116:443/
  ProxyPassReverse /47.142.209.116/
https://47.142.209.116:443/
   ProxyPass /prov/ https://47.174.74.184:8443/prov/
   ProxyPassReverse /prov/
https://47.174.74.184:8443/prov/
   AllowCONNECT 433
   <Proxy *>
        Order deny,allow
        Allow from all
   </Proxy>
         </IfModule>
          #End Proxy Config
          === "list_proxy_conf" completed successfully
```

9 Locate the proxy entry for the active unit used by the CS 2000 Session Server Manager. Refer to the following figure for assistance in locating this entry.

ProxyPass /10.65.99.67/ https://10.65.99.67:443/	Entry for physical unit 0
ProxyPassReverse /10.65.99.67/ https://10.65.99.67:443/	
ProxyPass /10.65.99.70/ https://10.65.99.70:443/	Entry for physical Unit 1
ProxyPassReverse /10.65.99.70/ https://10.65.99.70:443/	
ProxyPass /10.65.99.72/ https://10.65.99.72:443/	Entry for active unit
ProxyPassReverse /10.65.99.72/ https://10.65.99.72:443/	
*ProxyPass /**prov**/ https://10.67.99.72:8443/**prov**/*	Entry for active unit GUI
*ProxyPassReverse /**prov**/ https://10.67.99.72:8443/**prov**/*	

10 If necessary, record the label for the remote hostname/tag associated with the active unit.

ATTENTION

If necessary, see "Selecting and using tag names" (page 187) for more information about using remote tag names. The tag name shown must match the tag name used by the SIP Gateway application for the same node when you installed or upgraded it.

11 Exit the Apache Proxy Configuration level:

x

You are returned to the SPFS operating system.

12 Exit the Configuration level:

```
x
```

You are returned to the SPFS operating system.

13 Exit the CLI:

```
x
```

You are returned to the SPFS operating system.

14 If applicable, logout from the server.

15 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

Selecting and using tag names

Tag names for the active unit web proxy entries, must match the tag name entered when installing or upgrading the SIP Gateway application. Failure to use the same tag name will prevent access to the CS 2000 Session Server Manager after the SPFS web proxy services restart.

ATTENTION

If you are upgrading from SN08, or rolling back to SN08, the SPFS web proxy server must be using the prov tag name.

If the remote tag name for a node does not match that used during installation or upgrade of the SIP Gateway application, you must configure a new proxy entry using the correct remote tag name, then remove the obsolete proxy entry.

Reconfiguring the SST BIOS

Purpose of this procedure

Use the following procedure to make changes to the BIOS settings on the SST platform hardware, when you have replaced the SST chassis with a spare and the unit does not boot properly or if you want to verify that the BIOS is properly set up.

If you are changing any settings from their default, you may need to perform this procedure on both SST units. BIOS settings for both units must match.

Limitations and restrictions

Do not use this procedure to configure a new SST node installation.

ATTENTION

Do not use this procedure on an active SST unit.

Remove the RJ45 serial cable when this procedure is complete. Failure to remove the cable may cause software upgrade to fail.

Prerequisites

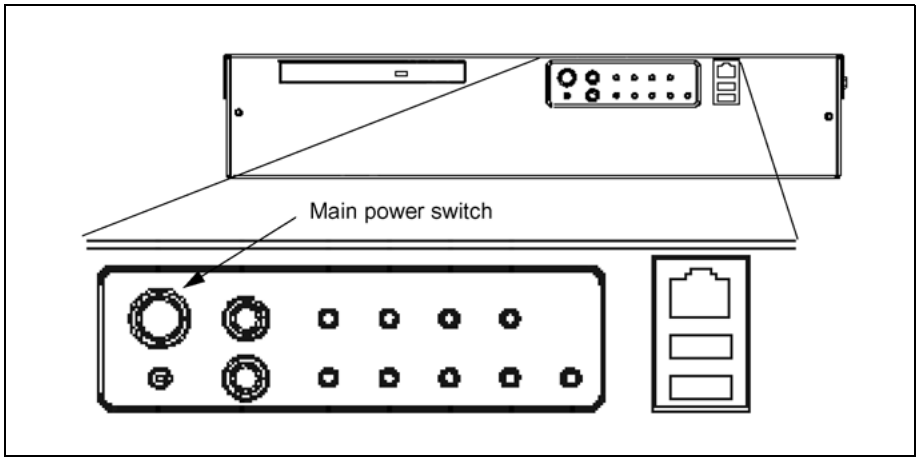
Verify that there are no active alarms on the active SST unit.

CAUTION

Performing this procedure on an SST node performing call processing temporarily affects fault-tolerant capability and overall system performance while the affected unit is offline.

Action

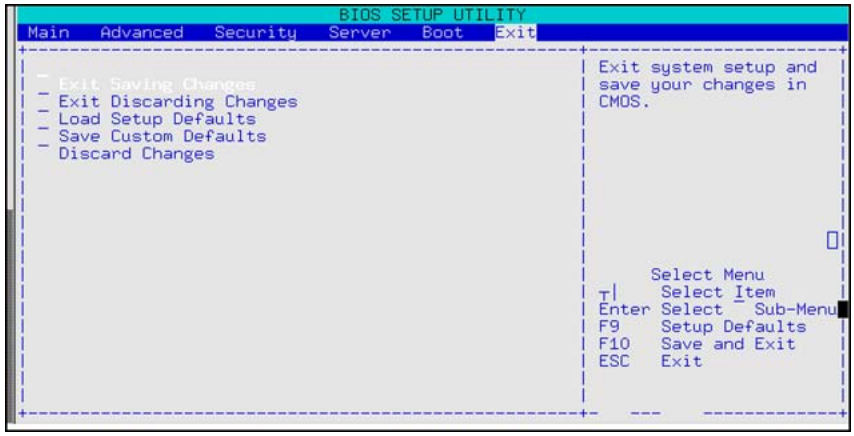
Step	Action
	At the Session Server console
1	If necessary, refer to procedure "Attaching a VGA monitor and keyboard console" (page 25) to ensure that you have a console interface connected to the rear of the SST you are reprovisioning. Your site may support other connection options.
2	If necessary, power on the SST using the main power switch located on the front panel, as shown in the following figure.



The BIOS information screen appears

3 At the BIOS information screen, press the **<F2>** key to enter the BIOS setup.

The main BIOS setup screen appears.



4 Use the right arrow key to move to the Server menu to validate (and change if necessary) the following entries:

Asset NMI on PERR: **Disabled**

Asset NMI on SERR: **Disabled**

FRB-2 Policy: **Retry 3 times**

POST Error Pause: **Disabled**

Boot Monitoring: **5 minutes**

Boot Monitoring Policy: **Always Reset**

5 Highlight the **Console Redirection item** and press **Enter** to validate (and change if necessary) the following entries:

BIOS Redirection Port: **Serial 2 (RJ45)**

ACPI Redirection Port: **Serial 2 (RJ45)**

Baud Rate: **9600**

Flow Control: **No flow control**

Terminal Type: **VT100+**

6 Press the **ESC** key to return to the Server menu, select the **Fault Resilient Booting** menu option and press **Enter**.

7 Validate (and change if necessary) the following entries:

Late POST timeout: **Disabled**

Fault Resilient Booting: **Reset**

8 Press the **ESC** key to return to the Server menu, then press the right arrow key to move to the Boot menu.

9 Select **Boot Device Priority** and press **Enter** to validate (and change if necessary) the following settings:

1st Boot Device: **ATAPI CD-ROM**

2nd Boot Device: **Hard Drive**

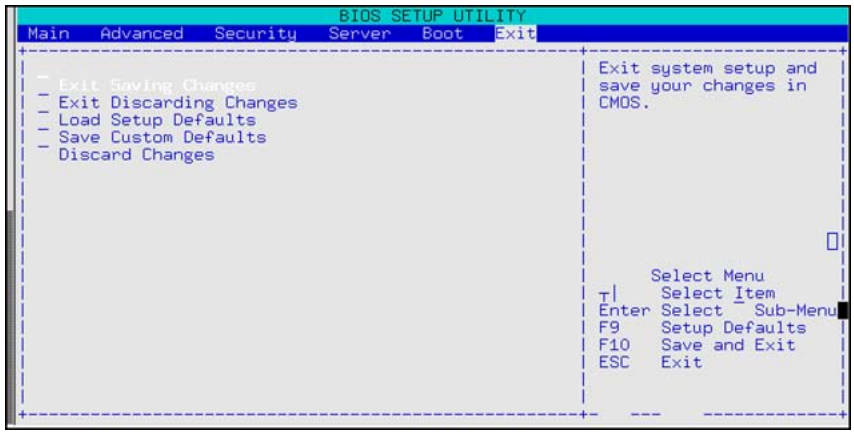
3rd/4th Boot Device: **Disabled**

10 Press the **ESC** key to return to the main menu.

11 Press the right arrow key to move to the **Exit** menu.

12 Highlight **Exit Saving Changes** and press **Enter**.

13 Type **`Yes`** in confirmation dialog box.



The SST unit resets and begins to boot.

14 Once the unit has rebooted, use procedure "Viewing the operational status of the NCGL platform" (page 146) to confirm that the rebooted unit has performed any necessary recoveries, returned to operational standby service and has generated no new alarms.

15 Remove the RJ45 serial cable connection from the unit. Failure to remove the cable may cause future software upgrades to fail.

—End—

Reprovisioning the NCGL platform software

Purpose of this procedure

Use this procedure when you need to reinstall the NCGL platform software from CD/DVD software disk because of a disk drive replacement where data has been lost or because of a software upgrade failure.

Limitations and restrictions

Do not use this procedure to configure a new unit.

If the node is in operation and performing call processing activities, only perform this procedure on the standby unit.

CAUTION
Possible service interruption
This procedure destroys all data on the affected unit's disk drives. Any critical data should be backed up.

Use care when executing this procedure. This procedure may cause the loss of customer data and causes all network configuration values to be reset to a default setting.

When using the **commish** tool to commission the NCGL platform, ensure that all values (other than hostname and IP address) entered match those on the other (mate) unit. Failure to do so may cause a service outage for SIP call traffic.

ATTENTION
Remove the RJ45 serial cable from the unit after completing this procedure. Failure to remove the cable may result in future software upgrade failures.

Prerequisites

Complete the procedure "Reconfiguring the SST BIOS" (page 188) to ensure that the Boot Device Priority is set so that the DVD/CD-ROM drive is accessed before the hard drive during boot-up.

Obtain the following values from the active unit using the commands provided. These values are required for the inactive unit being reprovisioned.

Note: Only the hostname and the IP address are unique to each unit.

- netmask:

  ```
  grep NETMASK /etc/sysconfig/network-scripts/ifcfg-eth0
  ```

- default gateway IP address:

```
grep GATEWAY /etc/sysconfig/network
```

- timezone:

  ```
  grep ZONE /etc/sysconfig/clock
  ```

- NTP server IP address:

  ```
  grep NTPSRVR /etc/sysconfig/ntp
  ```

- log host server IP address:

  ```
  grep loghost /etc/hosts
  ```

- network monitor IP address:

  ```
  grep MONITOR /etc/sysconfig/netnodes
  ```

- web proxy server IP address:

  ```
  grep WEBPROXY /etc/ sysconfig/netnodes
  ```

- SNMP trap destination IP address:

  ```
  grep SNMPDEST /etc/sysconfig/snmp
  ```

  Note: Ignore the port number as it is automatically assigned by the system.

- mate unit IP address:

  ```
  grep mateblade /etc/hosts
  ```

- active unit hostname:

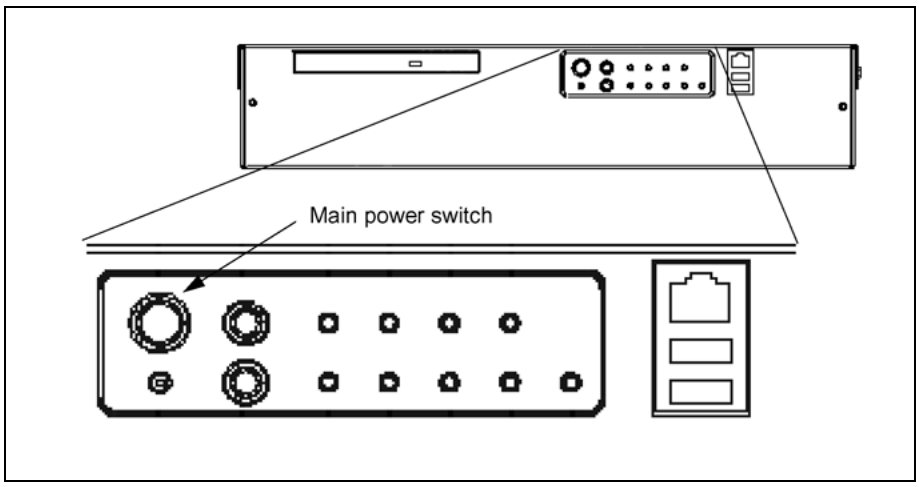
  ```
  hostname
  ```

  Note: Use a similar hostname for the inactive unit. For example, if the active unit hostname is LAB00_1, use LAB00_2 for the mate hostname.

Action

Step	Action
	At the Serial Console
1	If necessary, refer to procedure "Attaching a VT-100 console monitor to the RJ-45 serial port" (page 24) to ensure that you have a console interface connected to the rear of the unit you are reprovisioning. Your site may support other connection options. Do not use a VGA console to complete this procedure.
2	If the standby unit is still operating, shut it down using procedure "Halt (shutdown) a unit" in the *Session Server Trunks Security and Administration* (NN10346-611). This procedure does not power-off the unit.

3 If necessary, power-off the unit using the main power switch located on the front panel.



4 tdrtyPower-on the unit using the main power switch located on the front panel.

The BIOS information screen appears

5 Once the BIOS information screen appears, press the **F2** key when prompted.

6 Change the boot device priority by using the right arrow key to advance to the *Boot* menu.

7 Select **Boot Device Priority** and press **Enter**.

8 Navigate down to **Hard Drive** to change the boot priority. Change the boot priority to the following settings:

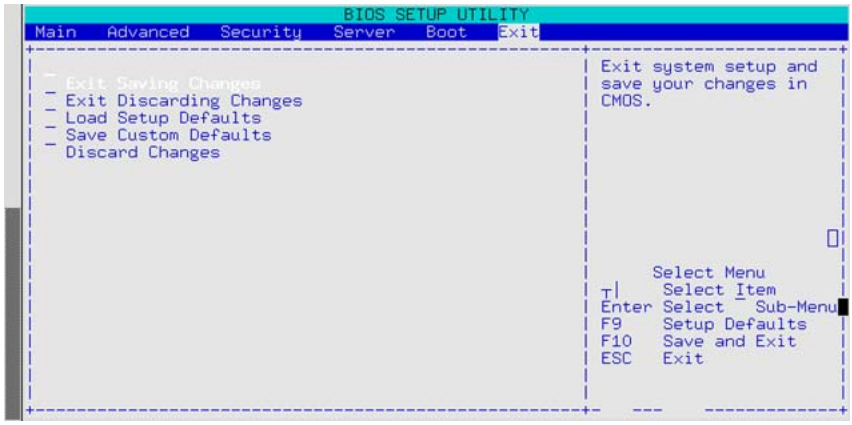
1st Boot Device: ATAPI CD-ROM (the DVD-Rom drive)

2nd Boot Device: Hard Drive

3rd/4th Boot Device: Disabled

9 Press **ESC** to return to the *Boot* menu, and then press the right arrow key to move to the *Exit* menu.

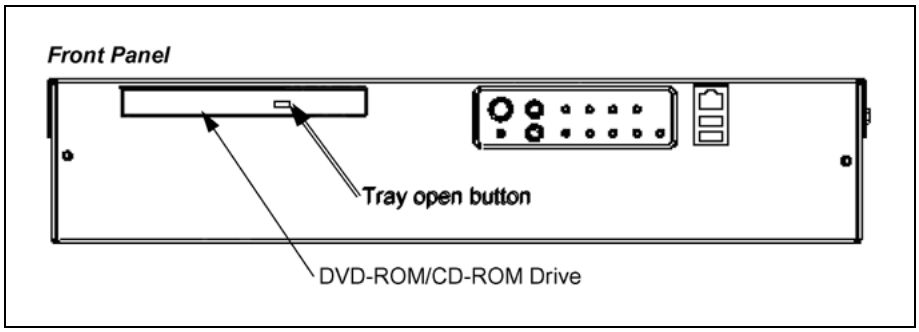
10 Highlight **Exit Saving Changes** and press **Enter**.



11 Type **Yes** in confirmation dialog box.

The unit resets and begins to boot.

12 Immediately press the tray open button on the DVD-ROM and insert the CD/DVD disk into the DVD-ROM drive.



13 At the boot prompt, you have 5 seconds to quickly type **NUKE** and press **Enter**.

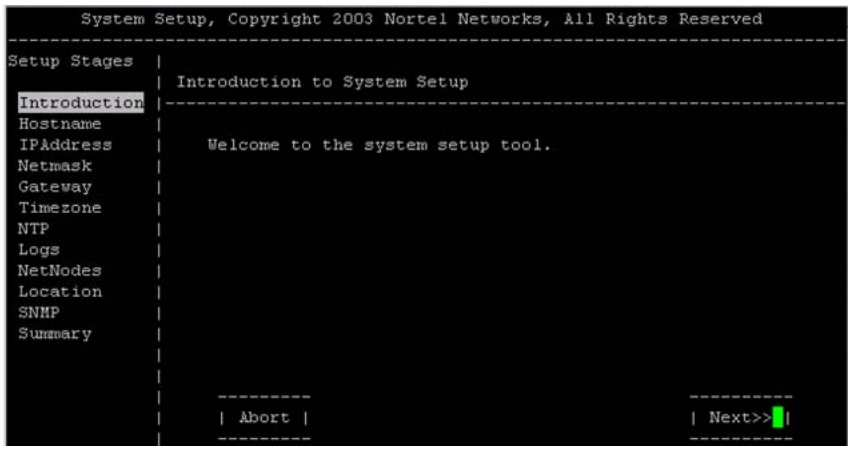
CAUTION
The NUKE command completely erases the drive and initiates a reboot from the CD/DVD disk.

Once the Boot prompt appears, only 5 seconds are given to type NUKE before the unit continues booting. If you miss the 5 second window, immediately power-off the unit using the power button on the front panel and return to Step 4.

14 Observe that after the NUKE command has erased the disk drive, the server reboots from the CD/DVD disk.

After several seconds, the NCGL load screen appears and the boot process continues.

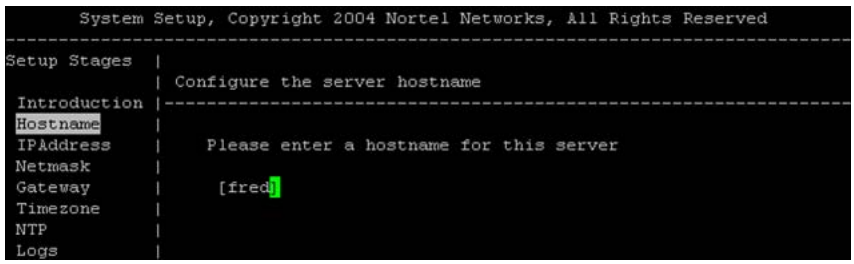
Once the unit completes the boot-up process, the NCGL system setup tool is displayed.



15 Position the cursor on the Next button and press **Enter**.

In general, use the **Tab** key to navigate between fields on the screen and use **Enter** to select a field or entry.

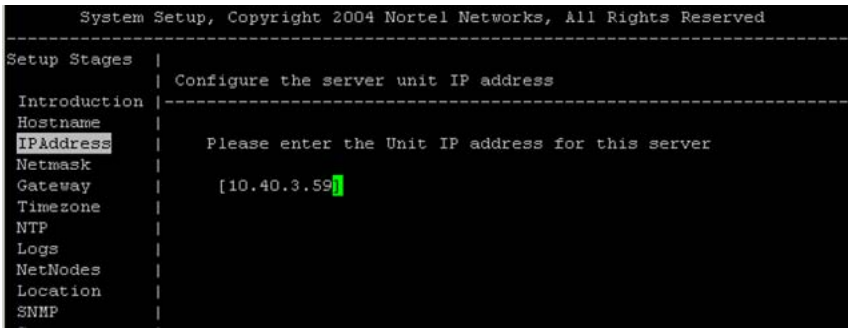
The server hostname screen appears.



16 If applicable, enter a hostname for this unit using up to 60 alphanumeric characters. Hyphens, underscores are allowed. Periods are not allowed.

17 Position the cursor on the **Next** button and press **Enter**.

The IP address configuration screen appears.



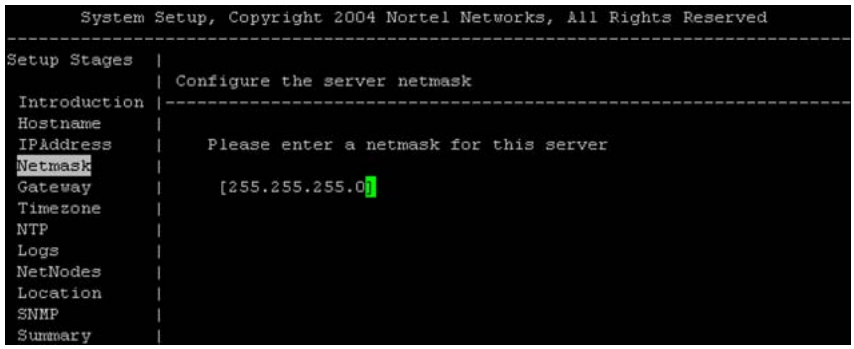
18 If applicable, enter an IP address for this unit in the following format:

```
10.40.102.112
```

See "SST configuration" (page 9) and contact your site Network Administrator to acquire the correct IP addresses used in this procedure.

19 Position the cursor on the **Next** button and press **Enter**.

The server netmask configuration screen appears.



20 If applicable, enter the netmask in the format:

```
255.255.255.0
```

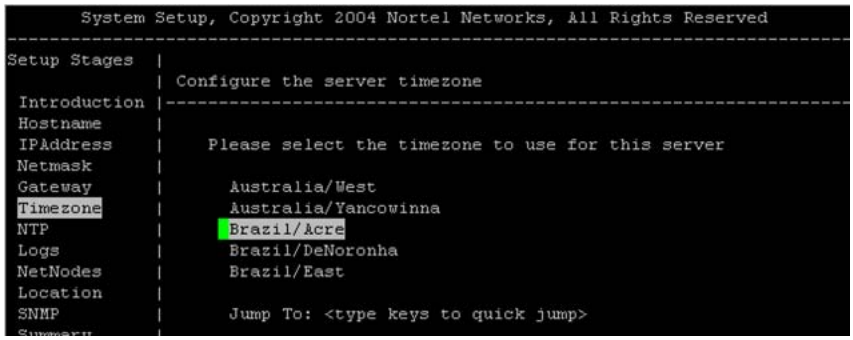
21 Position the cursor on the **Next** button and press **Enter**.

The server default gateway configuration screen appears.

22 If applicable, enter the IP address of the server default gateway.

23 Position the cursor on the **Next** button and press **Enter**.

The time zone configuration screen appears.

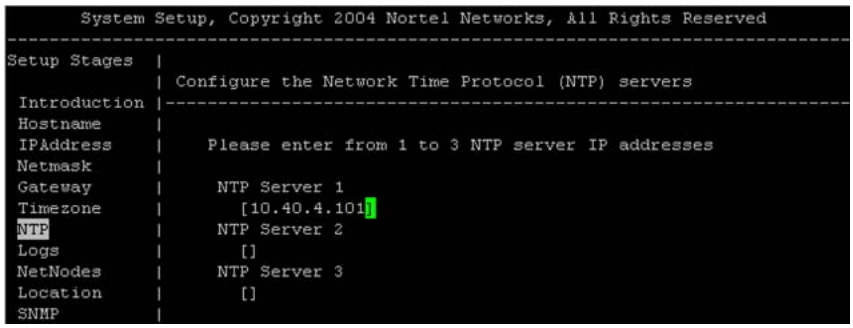


24 If applicable, use the up/down arrow keys to select the correct time zone, or type lower case characters on the keyboard to allow a quick jump to a time zone location in the list.

The quick jump is case sensitive.

25 Position the cursor on the **Next** button and press **Enter**.

The network time protocol (NTP) configuration screen appears.



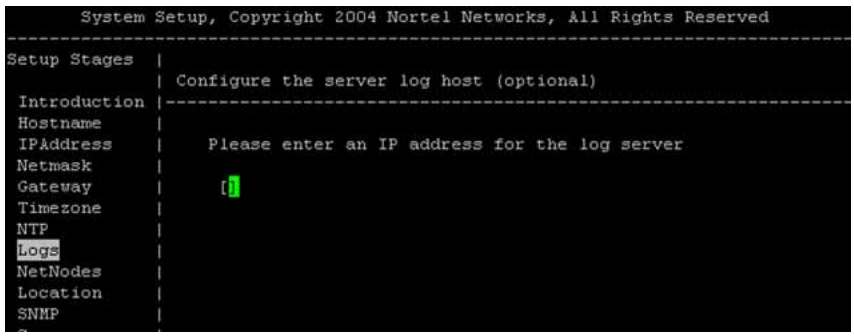
26 If applicable, enter the IP address of at least 1 (up to a maximum of 3) network time protocol servers in the following format:

```
10.40.102.112
```

To be consistent with other component implementations on the CS-LAN, the IP address of the SDM/ Core and Billing Manager should be used. The Core and Billing Manager are set up to communicate to the central Stratum-1 NTP server.

27 Position the cursor on the **Next** button and press **Enter**.

The log server configuration screen appears.



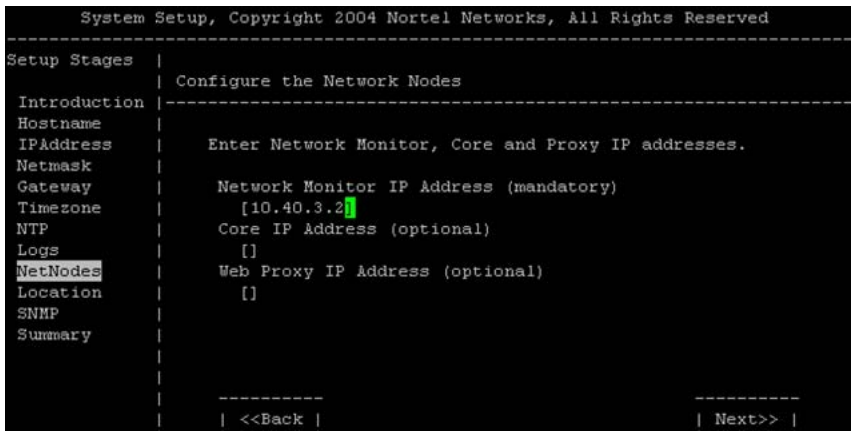
28 Enter the IP address of the log server in the following format:

```
192.168.102.112
```

This should be the IP address of the CS 2000 Management Tools server or another log aggregate server used in your network for collecting logs.

29 Position the cursor on the **Next** button and press **Enter**.

The Network Nodes page is displayed.



30 Use the following sub-steps to complete the Network Nodes screen:

a. For networks using sites using a CS-LAN with VRRP running, the Network Monitor should be the VRRP IP address (the default gateway). Consult your site network engineering guidelines to determine the correct IP address of this gateway, then enter the Network Monitor IP address in the following format:

```
10.40.102.112
```

b. Do not enter any address values for the Core IP addresses field. This field must remain blank.

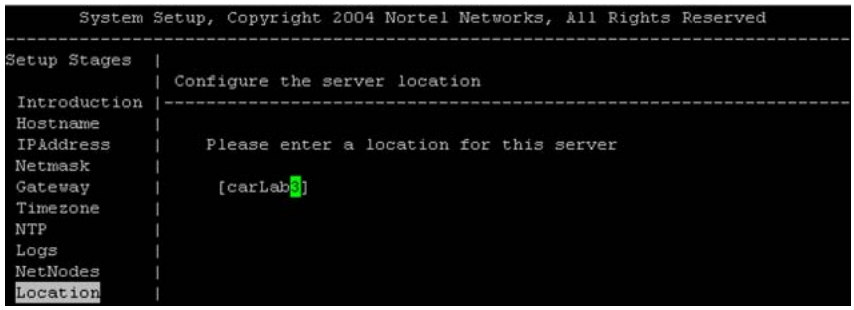
c. Enter the IP address of the SPFS server for the Web Proxy IP address in the following format:

```
10.40.102.112
```

Use the IP address of the SPFS platform residing on the CS 2000 Management Tools server.

31 Position the cursor on the **Next** button and press **Enter**.

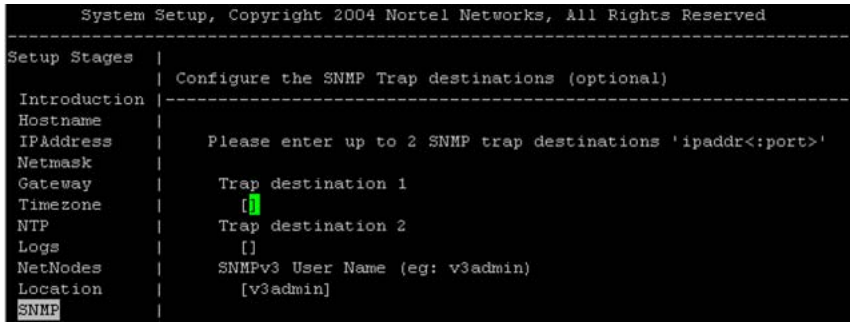
The server location page is displayed.



32 If applicable, enter a location identifier for the physical location.

33 Position the cursor on the **Next** button and press **Enter**.

The optional SNMP trap destinations page is displayed.



34 If applicable, enter the IP address of the IEMS server for Trap destination 1 in the following format:

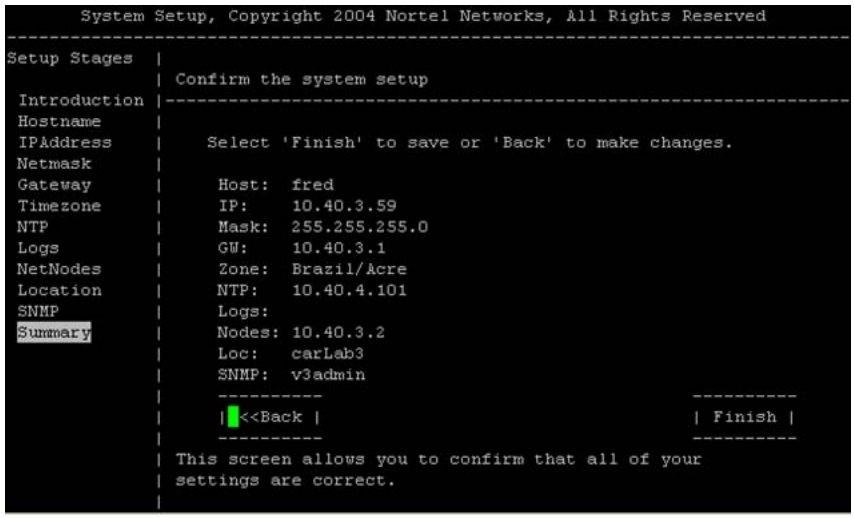
```
10.40.102.112
```

Use the IP address of the IEMS application residing on the CS 2000 Management Tools server.

Do not enter values for the Trap destination2 and SNMPv3 User Name fields.

35 Position the cursor on the **Next** button and press **Enter**.

36 Verify that all of the commish settings made for this unit match those of the mate unit.

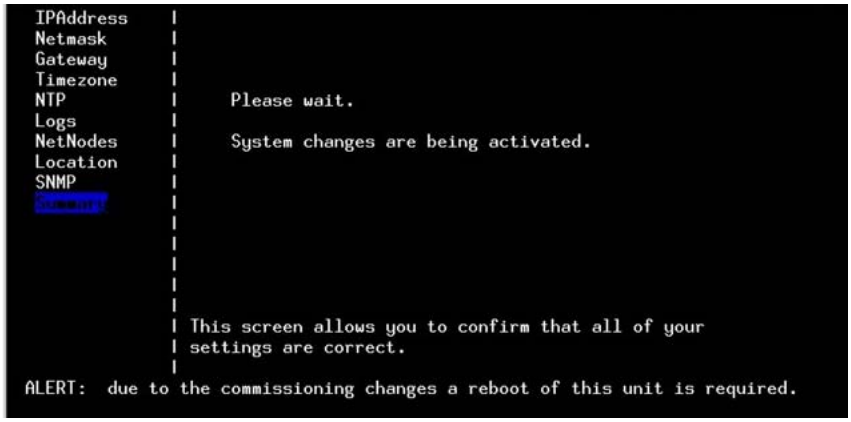


37 Eject the CD/DVD disk from the DVD drive. You must eject the disk before finishing with the commish tool to ensure that the unit boots from the hard drive and not the DVD drive.

38 Position the cursor on the **Finish** button and press **Enter**.

The system configures itself based upon the supplied settings.

After this procedure is completed, the unit automatically reboots. Allow the unit to boot normally.



39 Remove the RJ45 serial cable from the unit. Failure to remove the cable may result in future software upgrade failure.

40 You have completed this procedure. If applicable, return to the higher level task or procedure that directed you to this procedure.

—End—

Modifying NCGL platform provisioning

Purpose of this procedure

Use this procedure when you need to modify the NGCL provisioning values that were set up during initial commissioning activities. Provisioning values that can be changed using this procedure include:

- change the IP address of the proxy server (default gateway)
- change the IP address or netmask
- change the hostname
- change the time zone setting
- change the IP addresses of the network time protocol servers
- change the IP address of the log server to spool log files to
- change the SPFS web proxy server address
- change the IP addresses to allow access by the IEMS

Limitations and restrictions

ATTENTION

This procedure must be performed on both units; however, because a reboot and SwAct of the units is required in order for changes made to take effect, you can only perform this procedure on the standby unit.

Remove the RJ45 serial cable from each unit when this procedure is complete. Failure to remove the cable may result in future software upgrade failures.

CAUTION

Possible service interruption

Failure to following this procedure properly may cause a service outage for SIP call traffic.

Prerequisites

Before performing this procedure, the unit must first be jammed.

If necessary, refer to procedure"Attaching a VT-100 console monitor to the RJ-45 serial port" (page 24) to connect a console interface to the rear of the unit for which you are modifying provisioning.

Action

Step	Action

At a NCGL command line interface (CLI)

1 Log onto the standby unit.

2 At the prompt change to the root user:

```
su - root
```

3 Start the platform commissioning tool:

```
commish
```

After a few seconds the Introduction screen is displayed.

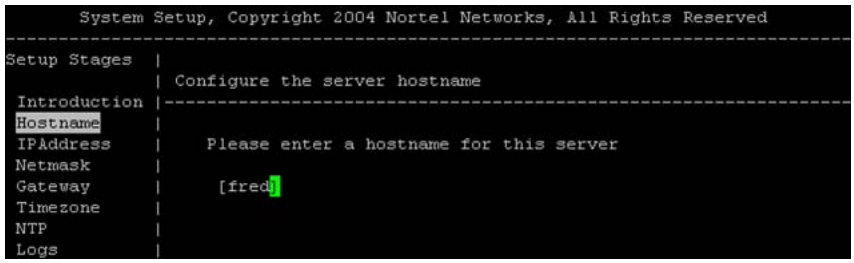
If the commish tool does not start and you receive the following message, them unjam and swact the units.

```
Commissioning start:
    Local unit 0 is active, enabled.
    Mate unit 1 is standby, enabled.
Aborted: This unit is active. Recommissioning cannot
be performed on the active unit. When appropriate,
switch unit activity and try again.
```

4 Position the cursor on the Next button and press **Enter**.

In general, use the **Tab** key to navigate between fields on the screen and use **Enter** to select a field or entry.

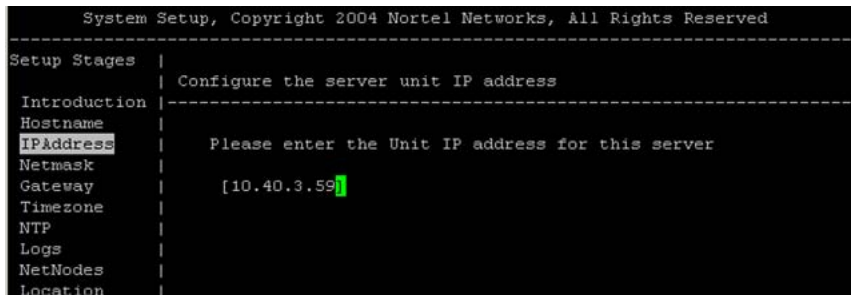
The server hostname screen appears.



5 If applicable, enter a hostname for this unit using up to 60 alphanumeric characters. Hyphens, underscores are allowed.

6 Position the cursor on the **Next** button and press **Enter**.

The IP address configuration screen appears.



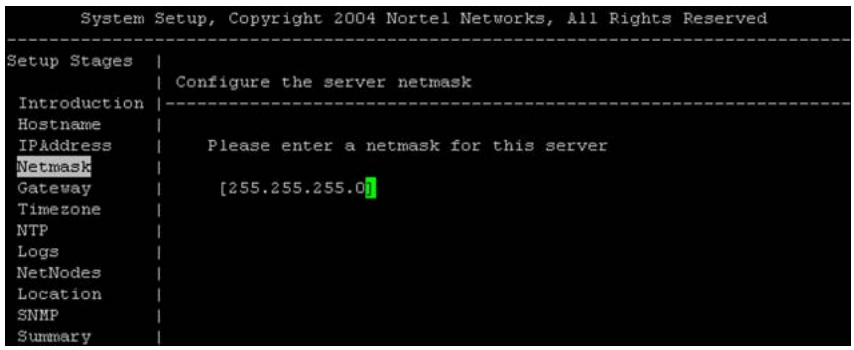
7 If applicable, enter an IP address for this in the following format:

192.168.102.112

See "SST configuration" (page 9) and contact your site Network Administrator to acquire the correct IP addresses used in this procedure.

8 Position the cursor on the **Next** button and press **Enter**.

The server netmask configuration screen appears.



9 If applicable, enter the netmask in the format:

255.255.255.0

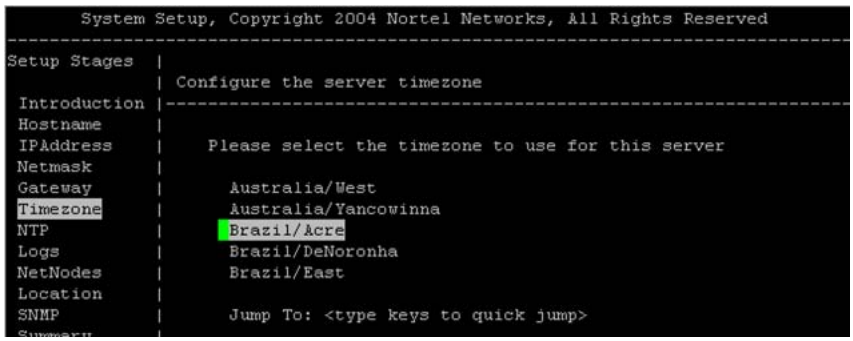
10 Position the cursor on the **Next** button and press **Enter**.

The server default gateway configuration screen appears.

11 If applicable, enter the IP address of the server default gateway.

12 Position the cursor on the **Next** button and press **Enter**.

The time zone configuration screen appears.

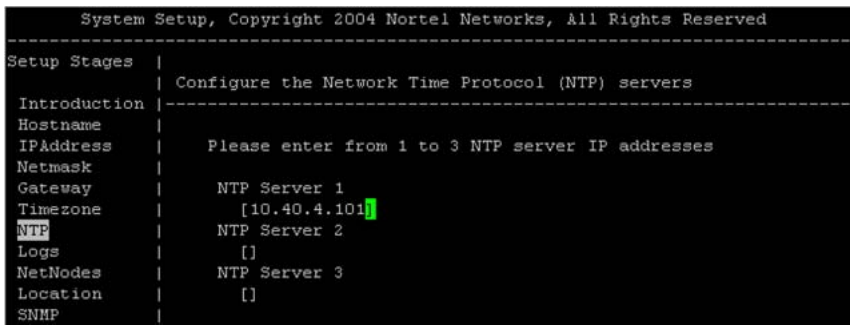


13 If applicable, use the up/down arrow keys to select the correct time zone, or type lower case characters on the keyboard to allow a quick jump to a time zone location in the list.

The quick jump is case sensitive.

14 Position the cursor on the **Next** button and press **Enter**.

The network time protocol (NTP) configuration screen appears.



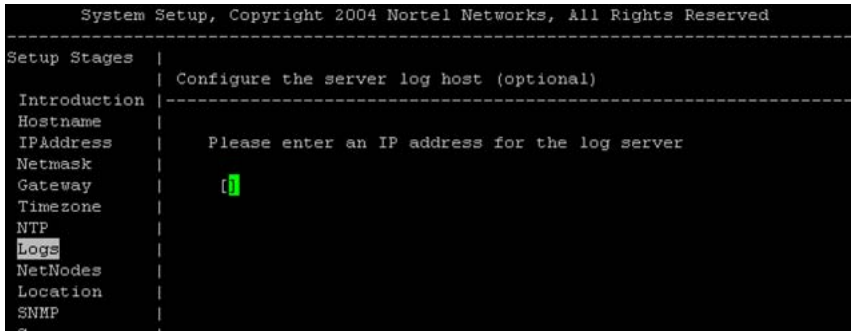
15 If applicable, enter the IP address of at least 1 (up to a maximum of 3) network time protocol servers in the following format:

```
192.168.102.112
```

To be consistent with other component implementations on the CS-LAN, use the IP address of the SDM/ Core and Billing Manager. The SDM/ Core and Billing Manager are set up to communicate to the central Stratum-1 NTP server.

16 Position the cursor on the **Next** button and press **Enter**.

The log server configuration screen appears.



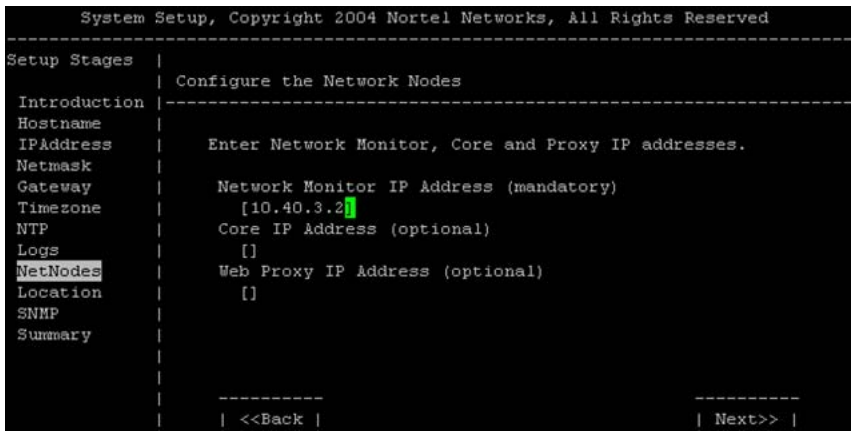
17 Enter the IP address of the log server in the following format:

```
192.168.102.112
```

This should be the IP address of the CS 2000 Management Tools server or it may be another log aggregate server used in your network for collecting logs.

18 Position the cursor on the **Next** button and press **Enter**.

The Network Nodes page is displayed.



19 Use the following sub-steps to complete the Network Nodes screen:

a. For networks using sites using a CS-LAN with VRRP running, the Network Monitor should be the VRRP IP address (the default gateway). Consult your site network engineering guidelines to determine the correct IP address of this gateway, then enter the Network Monitor IP address in the following format:

```
192.168.102.112
```

b. Do not enter any address values for the Core IP addresses field. This field must remain blank.

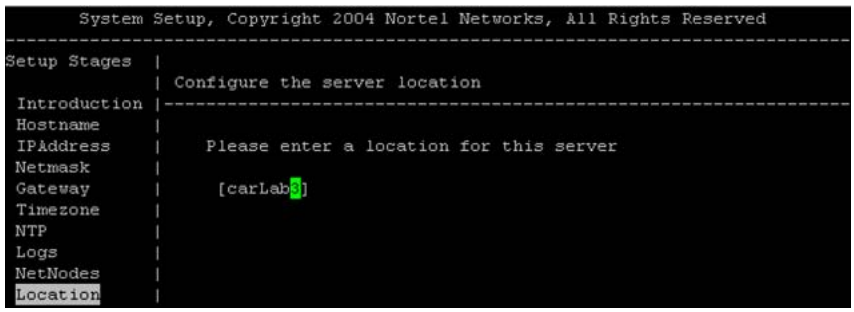
c. Enter the IP address of the SPFS server for the Web Proxy IP address in the following format:

```
192.168.102.112
```

Use the IP address of the SPFS platform residing on the CS 2000 Management Tools server.

20 Position the cursor on the **Next** button and press **Enter**.

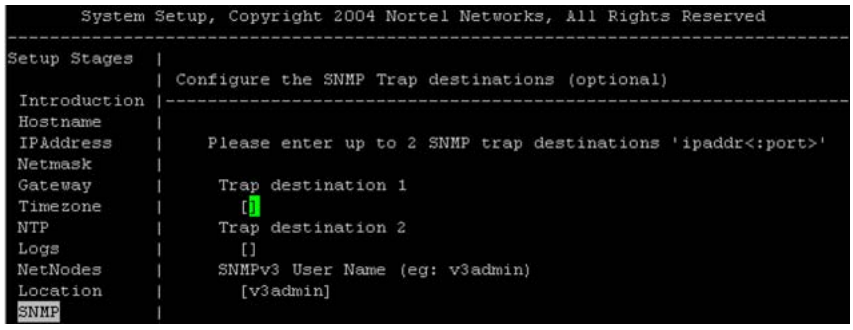
The server location page is displayed.



21 If applicable, enter a location identifier for the physical location.

22 Position the cursor on the **Next** button and press **Enter**.

The optional SNMP trap destinations page is displayed.



23 If applicable, enter the IP address of the IEMS server for Trap destination 1 in the following format:

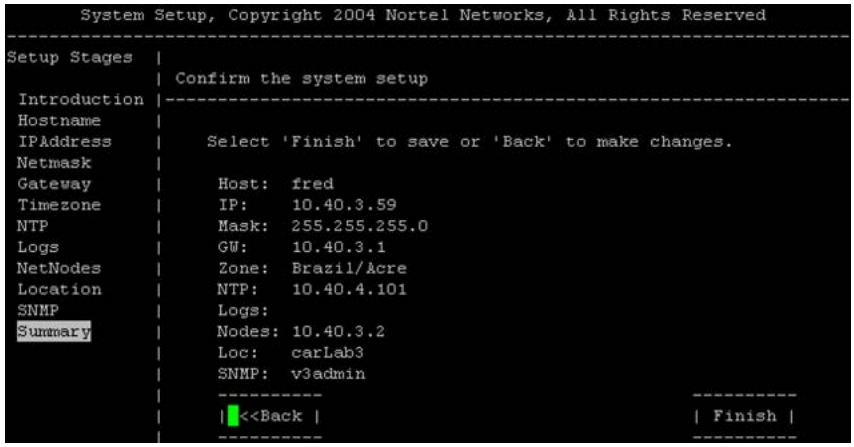
```
192.168.102.112
```

Use the IP address of the IEMS application residing on the CS 2000 Management Tools server.

Do not enter values for the Trap destination2 and SNMPv3 User Name fields.

24 Position the cursor on the **Next** button and press **Enter**.

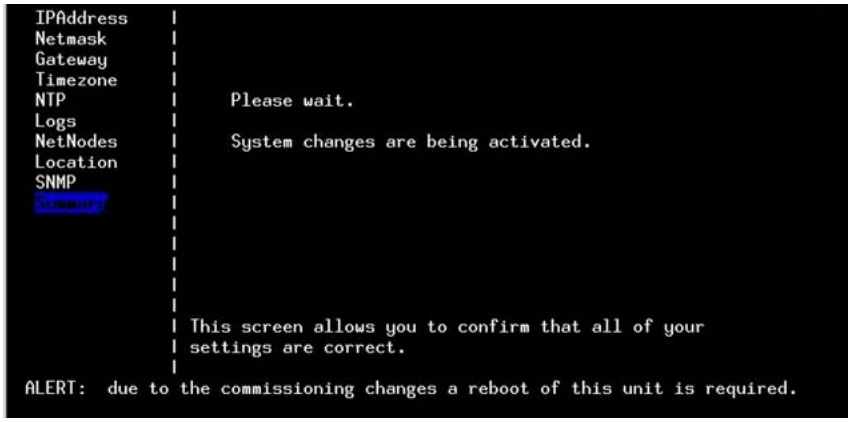
The summary screen is displayed



25 Position the cursor on the **Finish** button and press **Enter**.

The system configures itself based upon the supplied settings.

After this procedure is completed, the unit may automatically reboot. Allow the unit to boot normally.



26 After the unit has rebooted, verify the unit is unjammed or unjam it now.

27 SwAct the units.

28 Repeat this procedure on the other, now in standby, unit.

29 Use the procedure "Viewing the operational status of the NCGL platform" (page 146) to verify that both units are in operational service and that no new alarms have been raised.

30 Remove the RJ45 serial cable from the unit. Failure to remove the cable may cause future software upgrades to fail.

—End—

Starting filesystem monitoring

Purpose of this procedure

Use this procedure to start (enable) monitoring of disk and filesystem usage. Monitoring usage means that the NCGL operating system raises a critical, major, or minor alarm when thresholds are crossed. This procedure must be performed on both of the SST units in the node.

ATTENTION

Nortel Networks recommends monitoring all filesystems.

Limitations and restrictions

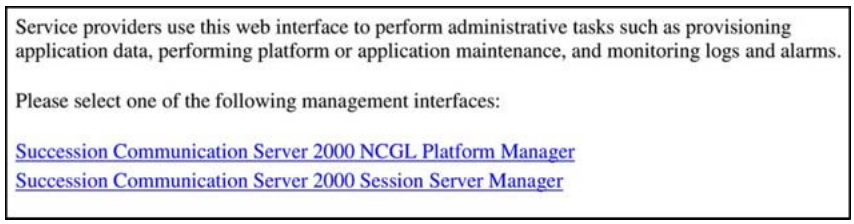
There are no limitations for performing this procedure

Prerequisites

There are no prerequisites for this procedure.

Action

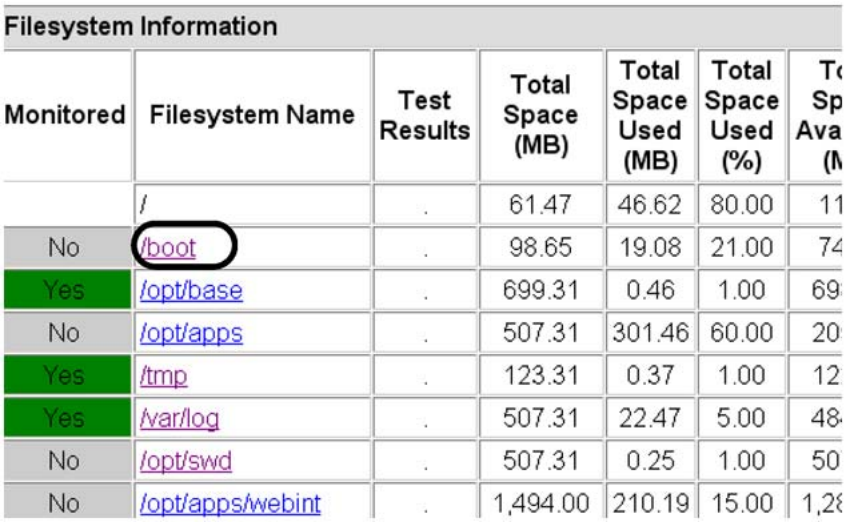
Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



2 Click the **Disk Services** link.

The Disk Services page is displayed.

3 Filesystems that are not monitored are indicated with a 'No' in the *Monitored* column of the *Filesystem Information* panel. To begin monitoring a filesystem, click the filesystem link for which you want to enable monitoring.



Filesystem Information

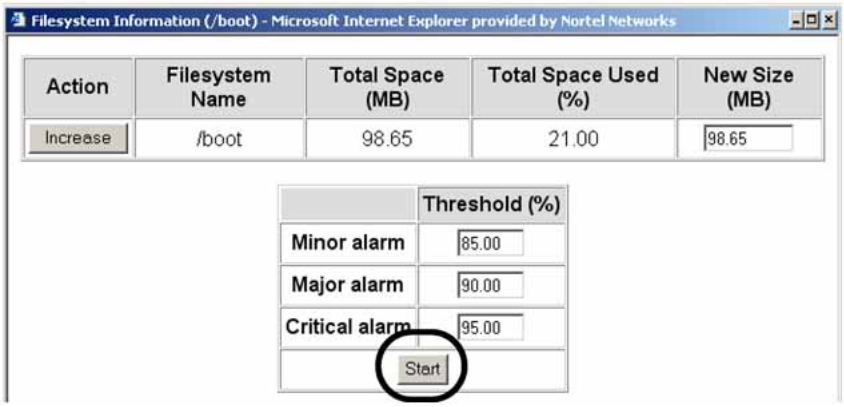
Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	To Sp Ava (M
	/	.	61.47	46.62	80.00	11
No	/boot	.	98.65	19.08	21.00	74
Yes	/opt/base	.	699.31	0.46	1.00	69
No	/opt/apps	.	507.31	301.46	60.00	20
Yes	/tmp	.	123.31	0.37	1.00	12
Yes	/var/log	.	507.31	22.47	5.00	48
No	/opt/swd	.	507.31	0.25	1.00	50
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,2

A filesystem information window appears, showing the current threshold levels along with other filesystem statistics.

4 If you want to start filesystem monitoring using the existing settings, click the **Start** button.

or

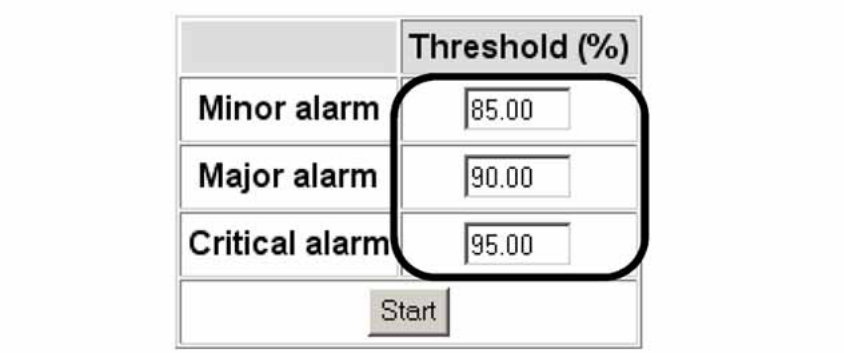
If you would like to make adjustments to the alarm threshold levels, continue with 5.



5 Adjust the monitoring thresholds for the filesystem by entering a new threshold value for one or more of the alarm severity types. When you are finished then click the **Start** button.

ATTENTION

Ensure that you enter the highest threshold value for the critical alarm and the lowest value or the minor alarm.



6 Repeat this procedure for the same filesystem on the second (mate) SST unit.

—End—

Stopping filesystem monitoring

Purpose of this procedure

Use this procedure to stop (disable) monitoring of disk and filesystem usage. This procedure must be performed on both SST units in the node.

Limitations and restrictions

ATTENTION

Nortel Networks recommends monitoring all filesystems. Use this procedure only when necessary.

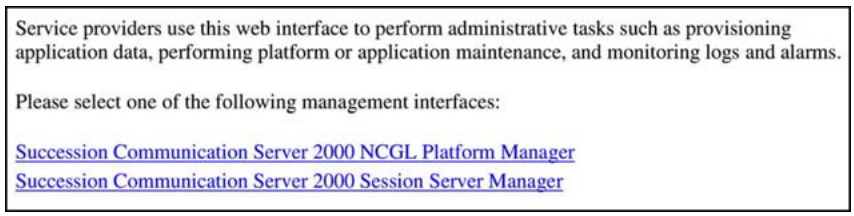
Do not leave monitoring disabled any longer than necessary.

Prerequisites

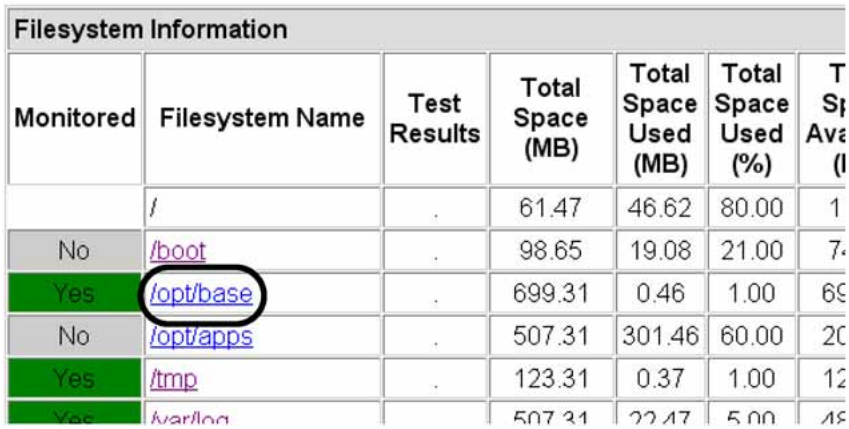
There are no prerequisites for this procedure.

Action

Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



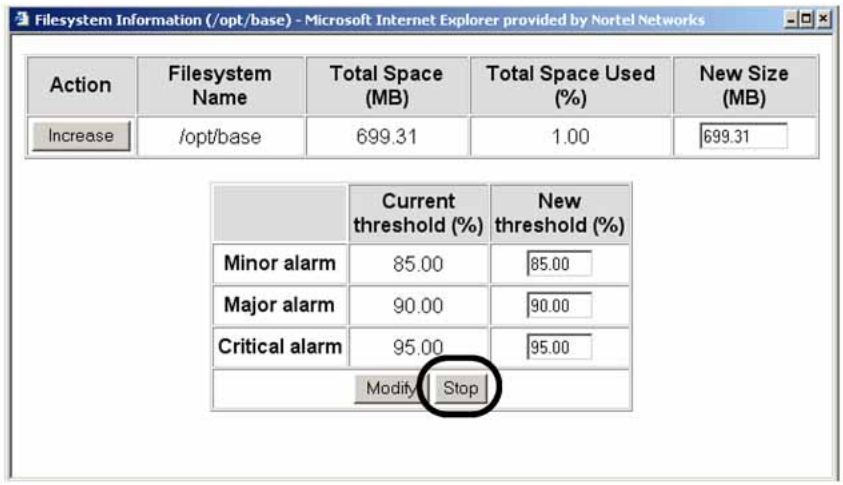
2	Click the **Disk Services** link. *The Disk Services page is displayed.*
3	Click the filesystem link for the filesystem you want to stop monitoring.



A filesystem information window appears, showing the current threshold levels along with other filesystem statistics.

4 To stop filesystem monitoring, click the **Stop** button.

ATTENTION
Nortel Networks recommends monitoring all filesystems. Do not leave monitoring disabled any longer than necessary.



5 Repeat this procedure for the same filesystem on the second (mate) SST unit.

—End—

Modifying filesystem monitoring thresholds

Purpose of this procedure

Use this procedure to modify the thresholds for monitoring disk and filesystem usage. SST has the ability to raise critical, major, or minor alarms when specified disk resource usage thresholds are crossed. This procedure must be performed on both of the SST units in the node.

ATTENTION

Nortel Networks recommends monitoring all filesystems.

Limitations and restrictions

It is not recommended to set the alarm thresholds lower than their default settings, unless recommended by Nortel support personnel. Doing so may produce additional alarm and log activity.

Prerequisites

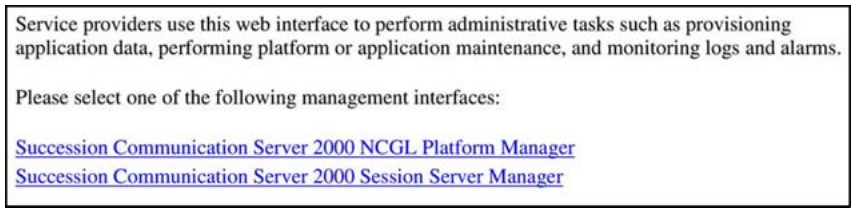
There are no prerequisites for this procedure.

Action

Step	Action

At the CS 2000 Session Server Launch Point

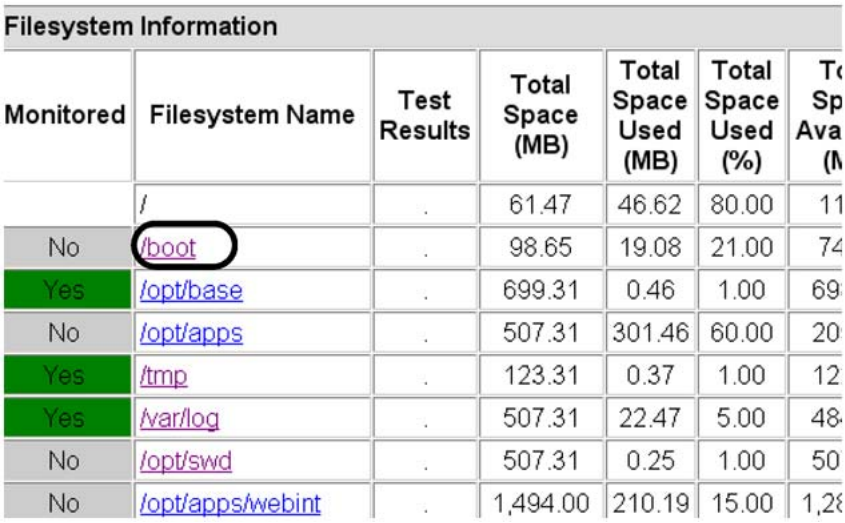
1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



2 Click the **Disk Services** link.

The Disk Services page is displayed.

3 Filesystems that are monitored are indicated with a 'Yes' in the *Monitored* column of the *Filesystem Information* panel. To modify settings for a monitored filesystem, click the filesystem link for the filesystem you want to modify monitored settings for.



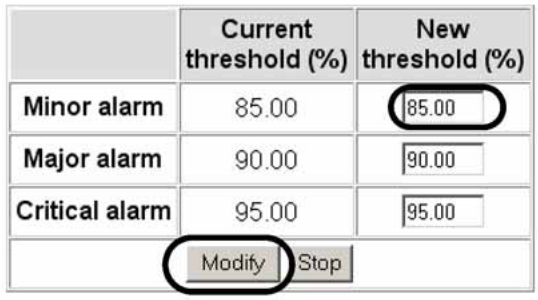
Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	To Sp Ava (M
	/	.	61.47	46.62	80.00	11
No	/boot	.	98.65	19.08	21.00	74
Yes	/opt/base	.	699.31	0.46	1.00	69
No	/opt/apps	.	507.31	301.46	60.00	20
Yes	/tmp	.	123.31	0.37	1.00	12
Yes	/var/log	.	507.31	22.47	5.00	48
No	/opt/swd	.	507.31	0.25	1.00	50
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,2

A filesystem information window appears, showing the current threshold levels along with other filesystem statistics.

4 Enter a new threshold value for the filesystem monitor, for each of the alarm severity types, then click the **Modify** button.

ATTENTION
Ensure that you enter the highest threshold value for the critical alarm and the lowest value for the minor alarm.



	Current threshold (%)	New threshold (%)
Minor alarm	85.00	85.00
Major alarm	90.00	90.00
Critical alarm	95.00	95.00
	Modify Stop	

5 Repeat this procedure for the same filesystem on the second (mate) SST unit.

—End—

Increasing filesystem size

Purpose of this procedure

This procedure is used to increase the size (in MB) of an existing filesystem on the SST hard drives. This procedure must be performed on both of the SST units in the node.

Limitations and restrictions

Perform this procedure at the direction of Nortel Networks support personnel.

Due to overhead that the operating system requires, the new size of the filesystem is slightly larger than the value entered.

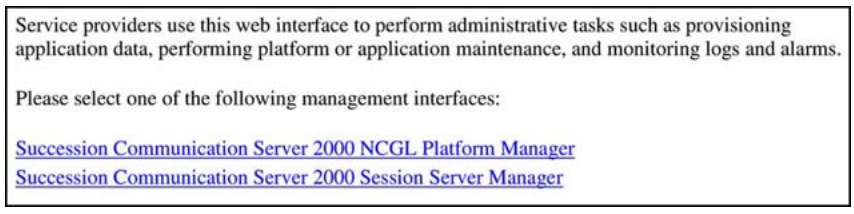
You cannot reduce the size of a filesystem. You must first remove the filesystem completely using procedure "Removing a filesystem" (page 225), then recreate the filesystem, using a smaller amount of disk space, using procedure "Creating a filesystem" (page 220).

Prerequisites

There are no prerequisites for this procedure.

Action

Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



2	Click the **Disk Services** link. *The Disk Services page is displayed.*
3	Make a note of the current filesystem size, then click the filesystem link for the filesystem that you want to increase in size.

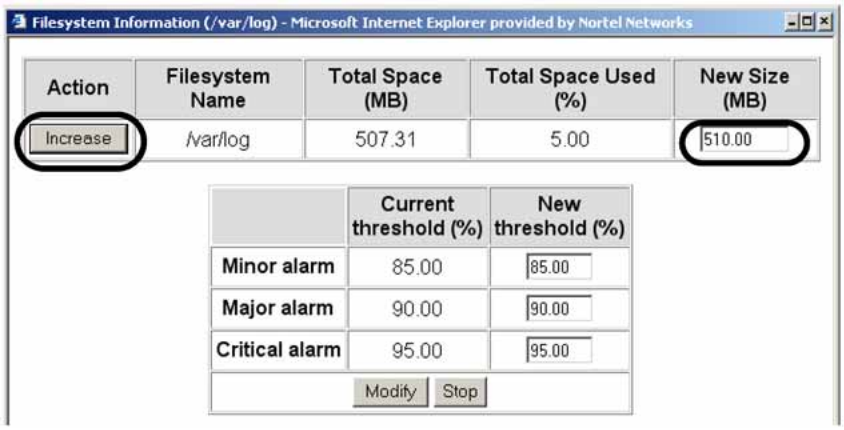
Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	To Sp Ava (M
	/	.	61.47	46.62	80.00	11
No	/boot	.	98.65	19.08	21.00	74
Yes	/opt/base	.	699.31	0.46	1.00	69
No	/opt/apps	.	507.31	301.46	60.00	20
Yes	/tmp	.	123.31	0.37	1.00	12
Yes	/var/log	.	507.31	22.47	5.00	48
No	/opt/swd	.	507.31	0.25	1.00	50
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,28

A filesystem information window appears, showing the current threshold levels along with other filesystem statistics.

4 Enter a new value for the filesystem size in the **New Size** field then click the **Increase** button.

Enter a value that is larger than the value shown in the Total Space (MB) field.



5 Verify that the increase is indicated in the Total Space (MB) column of the *Filesystem Information* panel.

Due to overhead that the operating system requires, the new size of the filesystem is slightly larger than the value entered.

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	Total Space Available (MB)
	/	.	61.47	46.81	81.00	11.48
No	/boot	.	98.65	19.08	21.00	74.48
Yes	/opt/base	.	699.31	0.46	1.00	698.85
No	/opt/apps	.	507.31	301.46	60.00	205.85
Yes	/tmp	.	123.31	0.37	1.00	122.94
Yes	/var/log	.	539.31	24.51	5.00	514.80
No	/opt/swd	.	507.31	0.25	1.00	507.06

6 Repeat this procedure on the second (mate) SST unit.

—End—

Creating a filesystem

Purpose of this procedure

This procedure is used to add a new filesystem to the SST hard drives. This procedure must be performed on both of the SST units in the node.

Limitations and restrictions

The following limitations apply to creating new filesystems:

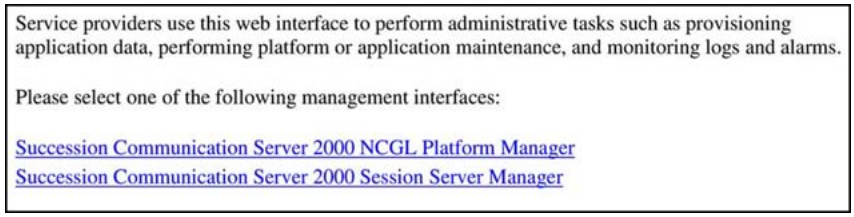
- Perform this procedure at the direction of Nortel Networks support personnel.
- The minimum size for a new filesystem is 27 (MB).
- Due to overhead that the operating system requires, the size of the new filesystem is slightly larger than the value entered.
- New filesystem names must be unique from existing filesystem names currently in the system.

Prerequisites

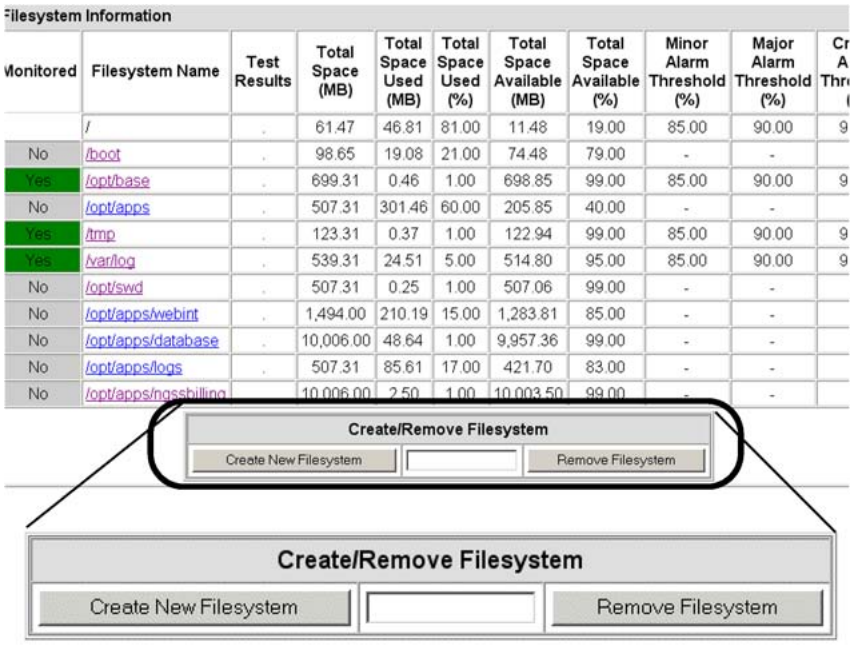
There are no prerequisites for this procedure.

Action

Step	Action
	At the CS 2000 Session Server Launch Point
1	Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



2	Click the **Disk Services** link. *The Disk Services page is displayed.*
3	Scroll to the *Create/Remove Filesystem* section.



4 Type a name for the new filesystem in the blank field and click the **Create New Filesystem** button to open the Set Size window.

The name entered for the new filesystem must be fully qualified from the root level (/) and must begin with a forward slash (/) character.

ATTENTION

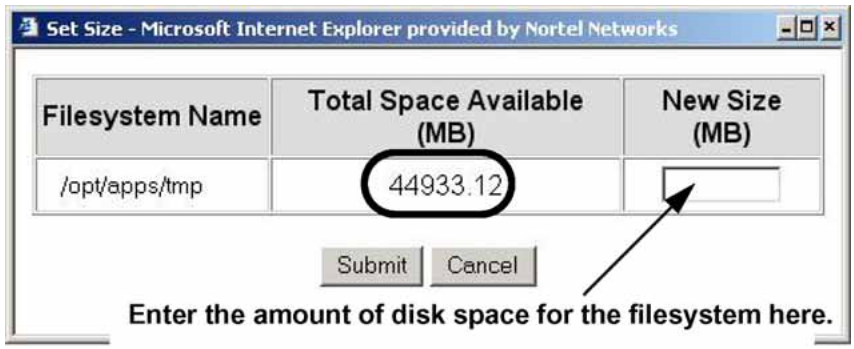
Use only the following characters when naming the filesystem:

- 0-9
- a-z
- A-Z
- / + .- (slash, plus sign, period and dash; use of the underscore character "_" and $ are not supported)

New filesystem names must be unique from existing filesystem names currently in the system.

5 Enter the size of the filesystem to create in the New Size field then click the **Submit** button.

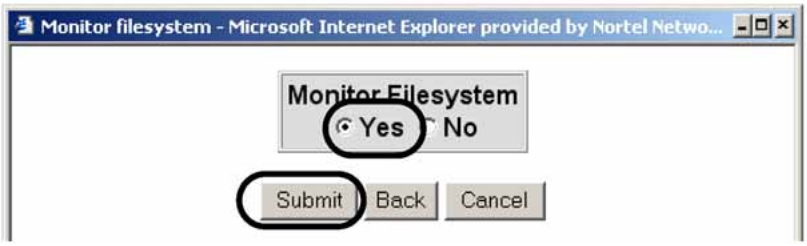
The numeric value must be at least 27 MB and no more than the total space (MB) available. If you enter a value that is not in an acceptable range for the system, an error message is generated and you are prompted to enter a minimum value.



6 To enable disk space monitoring for this filesystem, click the **Yes** radio button and click **Submit**.

ATTENTION

Nortel Networks recommends monitoring for all filesystems.

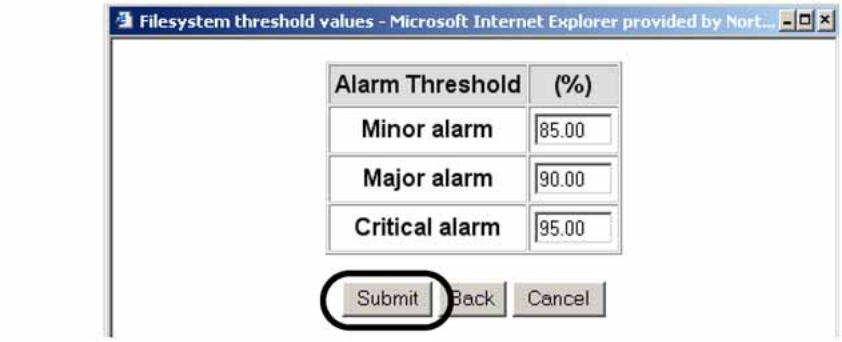


7 If desired, change the alarm threshold values, then click **Submit**.

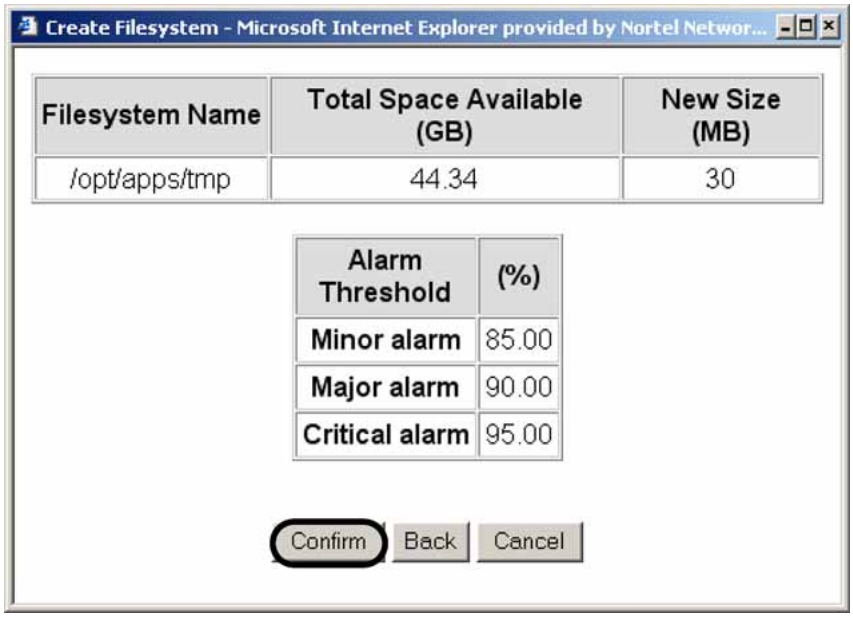
ATTENTION

Ensure that you enter the highest threshold value for the critical alarm and the lowest value or the minor alarm.

It is not recommended to set the alarm thresholds lower than their default settings, unless recommended by Nortel support personnel. Doing so may produce additional alarm and log activity.



8 Review the provisioning data for the new filesystem and click **Confirm** to create the new filesystem, or click **Back** to make changes.



9 When the system indicates that the filesystem was successfully created, click **OK**.

You are returned to the Filesystem Information view.

10 Confirm that the new file system shows up in the *Filesystem Information* view. If you need to make changes to the filesystem, refer to the appropriate procedure in this NTP for instructions.

Yes	/tmp	.	123.31	0.37	1.00	122.94	99.00
Yes	/var/log	.	539.31	24.67	5.00	514.64	95.00
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,283.81	85.00
No	/opt/apps/database	.	10,006.00	48.64	1.00	9,957.36	99.00
No	/opt/apps/logs	.	507.31	85.61	17.00	421.70	83.00
No	/opt/apps/ngssbilling	.	10,006.00	2.50	1.00	10,003.50	99.00
Yes	/opt/apps/tmp	-	27.31	0.05	1.00	27.27	99.00

11 Repeat this procedure for the other (mate) SST unit, using the same values and settings as you did for the first unit.

—End—

Removing a filesystem

Purpose of this procedure

This procedure is used to remove an entire filesystem from the SST hard drives. This procedure must be performed on both of the SST units in the node.

Limitations and restrictions

Deleting the following filesystems is not allowed.

- / (root)
- /boot
- all filesystems prefixed by /opt

CAUTION
Removing filesystems permanently destroys all data on that filesystem. Since such data cannot be recovered, ensure that you have made a backup of any important data.

Prerequisites

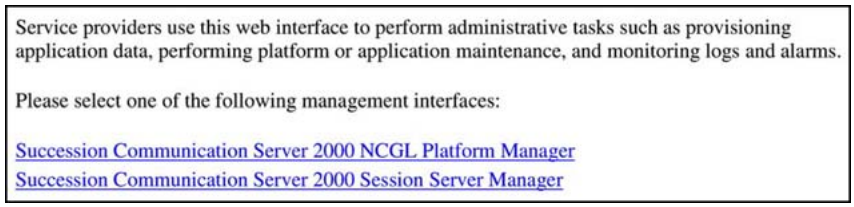
For information about backing up filesystems, refer to *Session Server Trunks Security and Administration* (NN10346-611).

Action

Step	Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



2 Click the **Disk Services** link.

The Disk Services page is displayed.

3 Locate the name of the filesystem that you want to remove in the *Filesystems Information* view.

Monitored	Filesystem Name	Test Results	Total Space (MB)	Space Used (MB)	Space Used (%)	Space Available (MB)	Space Availabl (%)
	/	.	61.47	46.99	81.00	11.30	19.00
No	/boot	.	98.65	19.08	21.00	74.48	79.00
Yes	/opt/base	.	699.31	0.48	1.00	698.83	99.00
No	/opt/apps	.	507.31	301.46	60.00	205.85	40.00
Yes	/tmp	.	123.31	0.37	1.00	122.94	99.00
Yes	/var/log	.	539.31	24.67	5.00	514.64	95.00
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,283.81	85.00
No	/opt/apps/database	.	10,006.00	48.64	1.00	9,957.36	99.00
No	/opt/apps/logs	.	507.31	85.61	17.00	421.70	83.00
No	/opt/apps/ngssbilling	.	10,006.00	2.50	1.00	10,003.50	99.00
Yes	/opt/apps/tmp	-	27.31	0.05	1.00	27.27	99.00

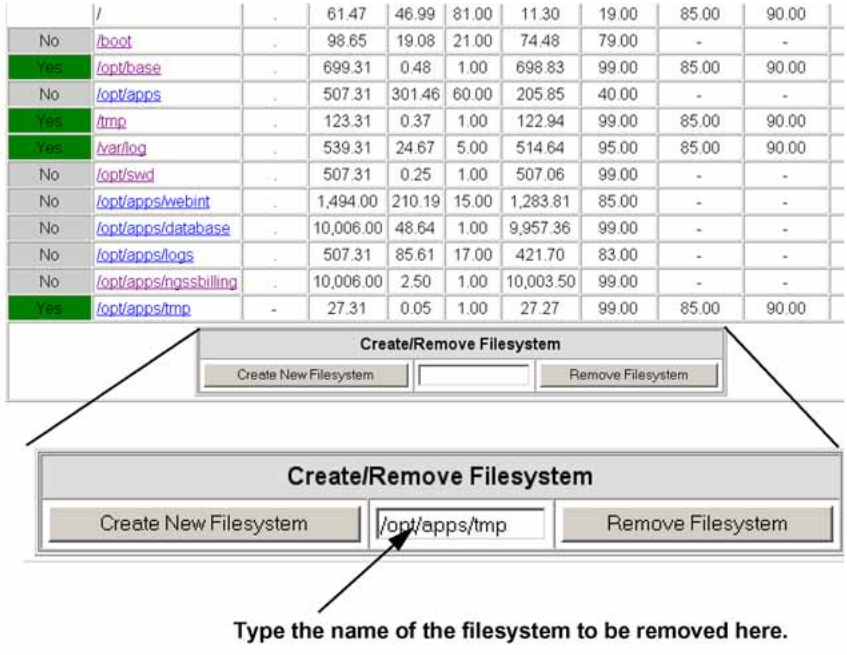
Create/Remove Filesystem

Create New Filesystem | | Remove File

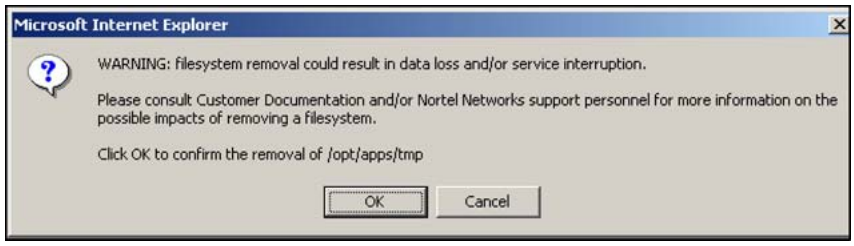
4 Type the name of the filesystem in the blank field of the *Create/Remove Filesystem* panel, then click the **Remove Filesystem** button

ATTENTION

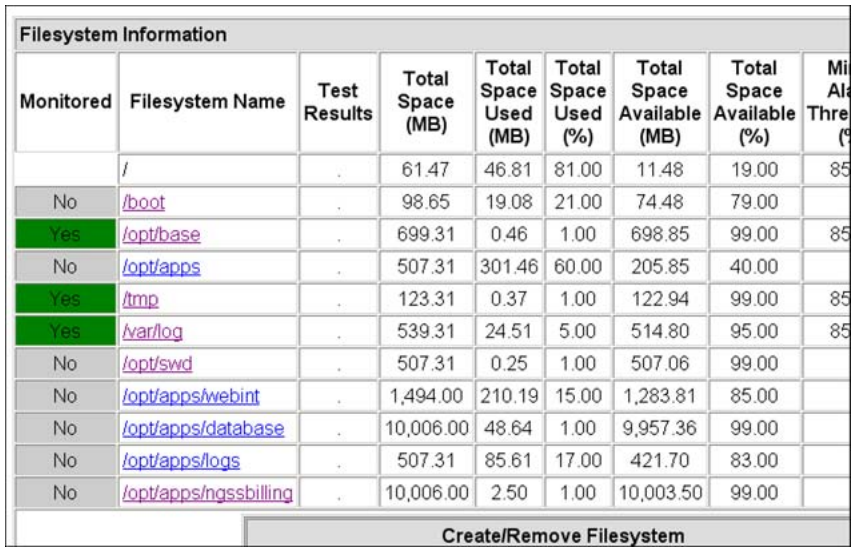
Deletion of the / (root) and /boot filesystems is not allowed.



5 Confirm that you want to remove the filesystem by clicking **OK**.



6 Confirm that the file system has been deleted from the *Filesystem Information* view.



Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	Total Space Available (MB)	Total Space Available (%)	Mi Al Thre (%
	/	.	61.47	46.81	81.00	11.48	19.00	85
No	/boot	.	98.65	19.08	21.00	74.48	79.00	
Yes	/opt/base	.	699.31	0.46	1.00	698.85	99.00	85
No	/opt/apps	.	507.31	301.46	60.00	205.85	40.00	
Yes	/tmp	.	123.31	0.37	1.00	122.94	99.00	85
Yes	/var/log	.	539.31	24.51	5.00	514.80	95.00	85
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00	
No	/opt/apps/webint	.	1,494.00	210.19	15.00	1,283.81	85.00	
No	/opt/apps/database	.	10,006.00	48.64	1.00	9,957.36	99.00	
No	/opt/apps/logs	.	507.31	85.61	17.00	421.70	83.00	
No	/opt/apps/ngssbilling	.	10,006.00	2.50	1.00	10,003.50	99.00	

Create/Remove Filesystem

7 Repeat this procedure for the other (mate) SST unit, using the same values and settings as you did for the first unit.

—End—

Carrier VoIP

Session Server Trunks Configuration Management

Publication: NN10338-511
Document status: Standard
Document version: 04.03
Document date: 20 October 2006

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

The information contained in this document is sourced in Canada, the United States of America, and the United Kingdom.