Session Server Configuration Management

What’s new in the (I)SN08 release?

The following new features and activities are covered in this NTP for the (i)SN08 release:

- Feature A00006893: This feature provides TLS security on the signaling paths (but not the call content) between the Session Server-SIP Gateway application and a similarly configured remote SIP application server or call server.
- Feature A00008383: Support for Multiple HTTPS connections to the Session Server through SSPFS. This feature provides support for multiple proxy https connections from IEMS/SSPFS and allows multiple Session Server nodes to reside on the CS-LAN.
- Support for two Session Server nodes. A CS 2000 can support two Sesion Server nodes, four physical units, in this release. This feature also allows an increase to parameter maxCallLegs from

40 000 to 50 000. Refer to Configure SIP Gateway application parameters on page 44. Refer to the following table.

Capacity increase

	SN07	SN08
Number of Session Server nodes supported on a CS 2000	1	2
Maximum DPT ports per Session Server node	40 000 (UDP) or 40 000 (TCP)	50 000 (UDP) or 40 000 (TCP)
Maximum DPT ports per CS 2000	40 000 (UDP) or 40 000 (TCP)	100 000 (UDP) or 40 000 (TCP)
Call capacity per Session Server pair in BHHCA	900 000 (UDP) or 500 000 (TCP)	900 000 (UDP) or 500 000 (TCP)
Call capacity per CS 2000 in BHHCA	900 000 (UDP) or 500 000 (TCP)	1 800 000 (UDP) or 500 000 (TCP)

Note: The maximum DPT ports equals the maximum number of simultaneous sessions.

Configuration management strategy

The purpose of this NTP is to provide a means for the customer to perform configuration management activities on the Session Server including changing existing configuration settings on a Session Server that has been installed and commissioned into an existing CS 2000 Network.

The purpose of this NTP is not for providing initial installation and commissioning of a Session Server platform or its applications. For initial installation of a Session Server into a network, consult your Nortel service representative in acquiring the appropriate Installation Methods (IMs) for the Session Server component.

General configuration limitations and restrictions

The following general limitations and restrictions apply when performing configuration management of the Session Server for any solution.

- Neither of the Session Server’s two GUIs (the CS 2000 Session Server Manager and the CS 2000 NCGL Platform Manager) support being accessed over a NAT'd connection. Only SSPFS 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 web client GUIs, allow the operation to complete before performing other actions.

Tools and utilities

Re-provisioning of the Session Server or changing of the Session Server’s 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 described in this NTP:

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

Client web browser requirements

For provisioning and maintaining the Session Server 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 Session Server GUIs and CLIs

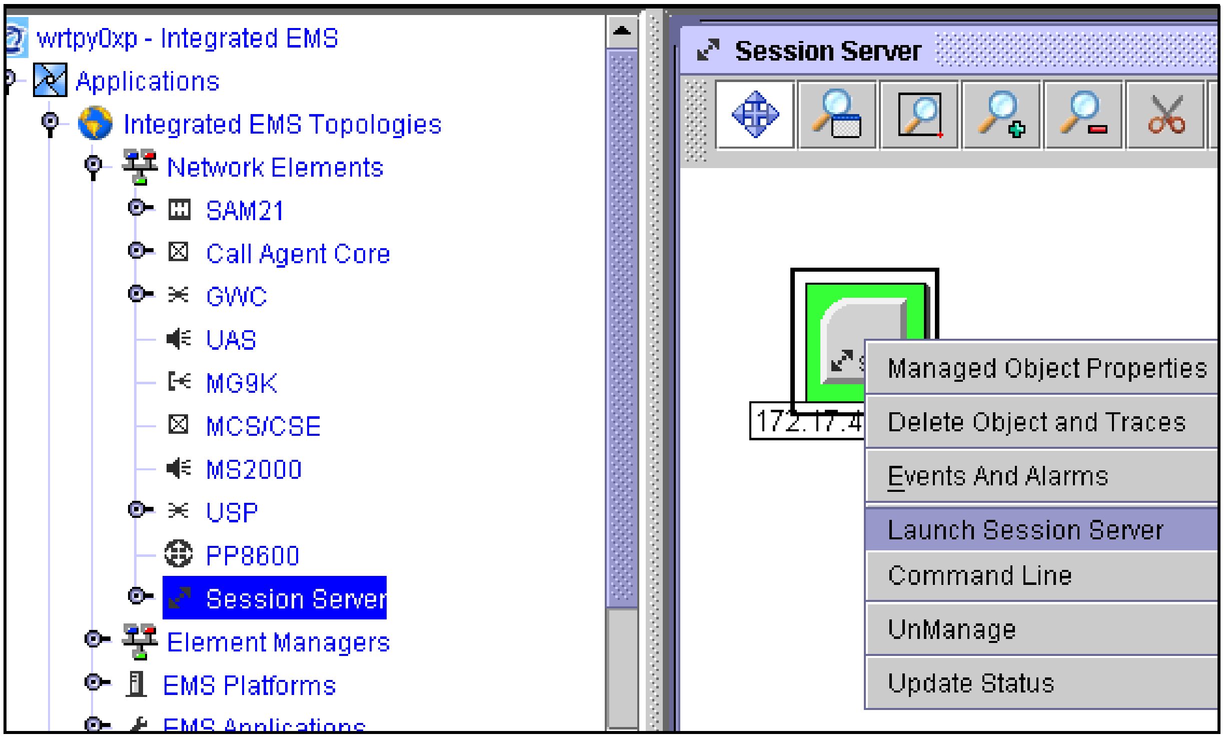
The Session Server can be configured to be accessed from the Integrated Element Manager System (Integrated EMS) between the customer operation LAN and the CS 2000 call server LAN. It can also be configured without the Integrated EMS because the Session Server functions as its own element manager. This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

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

There are three primary methods for accessing Session Server user interfaces:

- All GUI and CLI interfaces to the Session Server GUI can be accessed by selecting and right-clicking on the active Session Server element from the Integrated EMS expanded Network Elements view, as shown below.

Accessing Session Server GUIs or CLI from the Integrated EMS



For more information, refer to procedure *Access the CS 2000 Session Server GUIs from the Integrated EMS*, found in the Session Server Security and Administration NTP, NN10346-611. For more information about using the Integrated EMS service, refer to the Integrated EMS Basics NTP, NN10329-111.

- All GUI interfaces to the Session Server can be accessed from a remote system known to the proxy server (running on CS 2000 Management Tools server) on the CS-LAN.
- For commissioning purposes, the CLI interface can be accessed through a secure shell (SSH) connection from a remote client to the Session Server by way of SSH/telnet access through the SSPFS server.

  The CLI can also be accessed using a console connected to the rear of the Session Server active unit. In some cases, this connection is wired to a terminal box. Refer to section Attach a VGA monitor and keyboard console on page 18 for more information about using this method.

ATTENTION
For all methods of GUI access, 1st party cookies (cookies that only get sent back to the originating server) must be enabled on the client system web browser to enable logging onto the Session Server; however, 3rd party cookies (cookies that can be read by servers other than the originating server) can be disabled.

ATTENTION
For all methods of GUI access, only HTTPS (HyperText Transport Protocol Secure) access is allowed. For security reasons, HTTP (HyperText Transport Protocol) access is not supported on the Session Server.

ATTENTION
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 SSPFS server’s hostname/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.

Session Server configuration

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

- Session Server NCGL Platform commissioning
- Session Server SIP Gateway Application software installation
- Session Server SIP Gateway Application provisioning

Configuring multiple Session Server nodes in the call server network

In SN08, one or more Session Server node hardware (SAM-XTS) units are installed in either the SAMF or Call Control frames (CCF). On the CCF frame (NTRX51TA), a Session Server node (made up of two hardware units) is usually mounted below the STORM units. On the SAMF frame (NTRX51HA), up to two Session Server nodes (up to 4 hardware units) are mounted at the top of the frame, starting below the BIP power distribution unit.

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

Overview of CS 2000 XA-Core and Compact Call Agent Table Provisioning

There are several important core tables that are provisioned on the CS 2000 XA-Core or the CS 2000 Compact Call Agent for the Session Server to enable processing of SIP calls by the Session Server. These include:

- Table SERVRINV stores provisioned data for gateway controllers including SIP-T and VRDN GWCs used by Session Server.
- 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 Dynamic Packet Trunks (DPTs). Because Session Server SIP trunks are 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 Session Server SIP trunks, table DPTRKMEM provides a means to associate trunk group CLLIs with ranges of external trunk names (EXTRKNM).

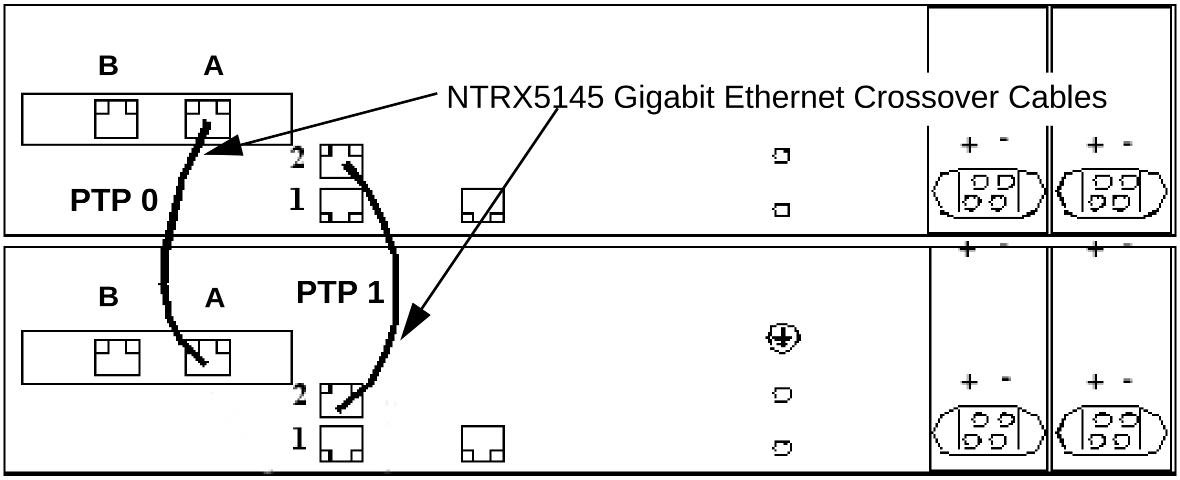
For more information about provisioning these core tables, refer to the CS 2000 Configuration Management NTP applicable to your solution.

Connecting Session Server ethernet ports to the call server network

Each of the Session Server 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 Session Server units



Notes about ethernet ports:

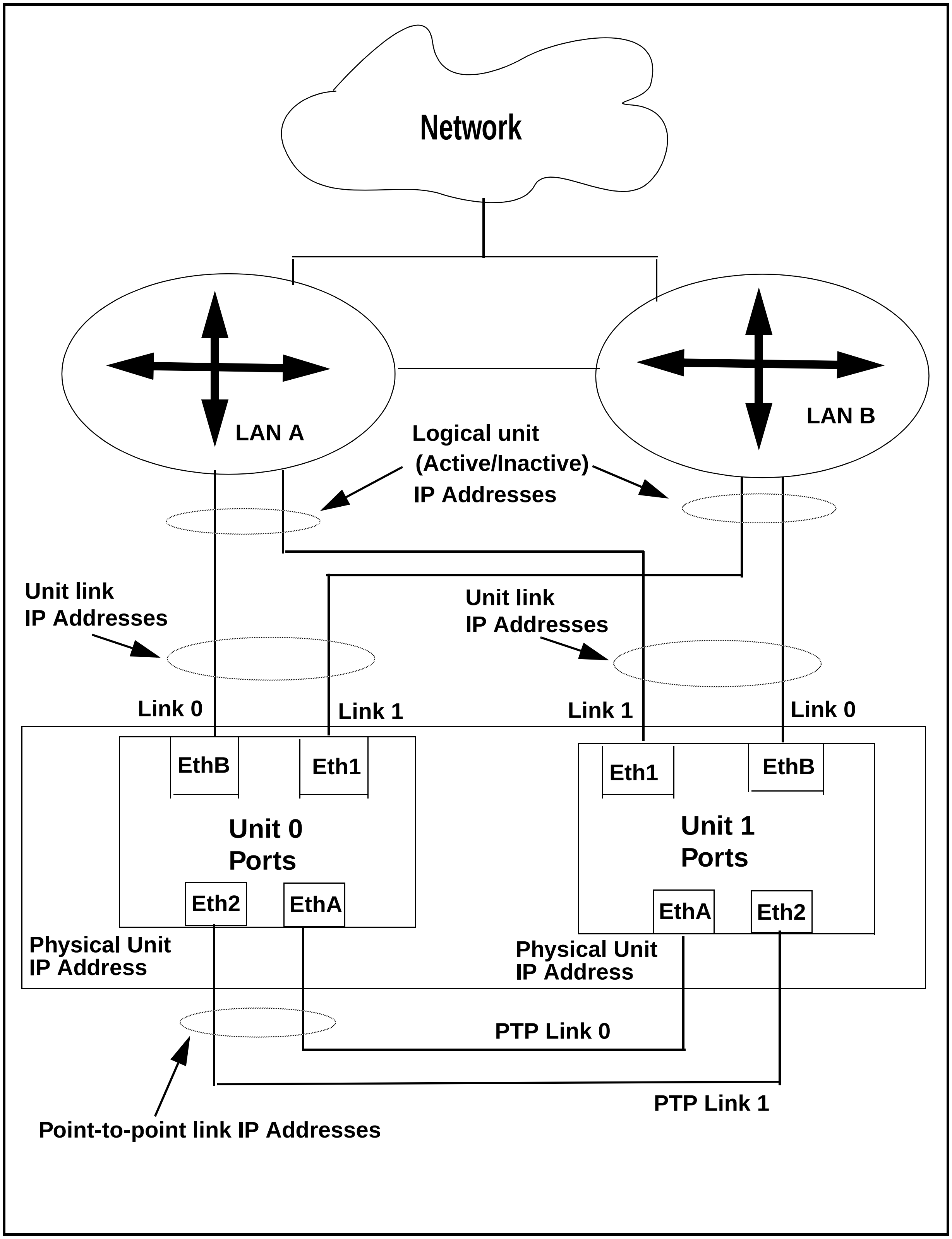
Ports 1 and B (both sets) go to CS-LAN Switch

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

Mapping IP addresses and links to physical ethernet ports

The following figure shows the port and link configuration for both the Session Server units. Port ethB of each unit is connected directly to a LAN switch, while port eth1 is connected to the redundant 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 Session Server ethernet links and ports to IP addresses



Understanding Session Server 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 Call Server (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 by the user during the commissioning process for that unit as determined by requirements at the customer site with assistance from the IP solution Network Engineering Guidelines. The rest of the IP addresses are generated 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 a Session Server node

Session Server IP addresses	Example unit IP address scheme	Datafilled or generated by:	Description
Active unit	172.16.16.72[1]	system	Logical unit
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[2]	system	Local point to point link
Mate PTP link 1	192.168.1.2	system	Mate point to point link

[1] The active node’s last set of digits must be the highest address and must be divisible by 8.

[2] 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.

Procedures for managing Session Server GUI access using IEMS

Most configuration activities for setting up the Session Server GUIs and CLI to be accessible from the Integrated EMS are performed using the Integrated EMS Configuration Management NTP, NN10330-511. Use the following list of procedures to configure the Integrated EMS and Session Server to allow Session Server GUI and CLI access from Integrated EMS.

Procedure
Adding a Session Server found in the Integrated EMS Configuration Management NTP, NN10330-511
Modify NCGL platform provisioning on page 205

Adding DPT trunk group connections handled by Session Server

Adding new SIP trunk groups to a local Call Server network involves configuration activities on a range of components (elements) in the network.

New DPT (SIP) trunk datafill must be added to Core table SIPLINK and the DPT entry RTS'd from the Core DPTTRM map level to facilitate the link names being transferred from table SIPLINK. Refer to section *Troubleshooting SIP-T trunk group link status on the Core* in the Session Server Fault Management NTP, 10332-911, 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 Session Server while the Session Server is in service. If additional DPT GWCs are required to handle increased call volume, they can be introduced without any impact to call processing. The in-service addition of trunk groups and DPT GWCs made available to the Session Server can be accomplished because the Session Server uses a simple, round-robin scheme to distribute incoming calls across all in-service DPT GWCs. Consult the Configuration NTP applicable to your solution for information and end-to-end instructions for adding new DPT trunk groups for your network.

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
Add/manage telephony profiles on page 62
Configure Remote SIP Servers on page 21
Add/Manage Access Link Maps on page 67

Modifying SIP (DPT) trunk group connections handled by Session Server

Use the following procedures to modify the number of trunk groups that can process calls on the Session Server.

Procedure
Modify DPT trunk group connections supported by the SIP Gateway application on page 172

Increasing the number of calls allowed through Session Server

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 Session Server provisioning.

Use the following procedures to increase the number of simultaneous calls that can be handled by the Session Server.

Procedure
Modify Session Server maximum DPT call limits on page 173

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 Session Server. 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/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 Session Server 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 Session Server.
- 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
Configure SIP Gateway application parameters on page 44 Configure Remote SIP Servers on page 21

Procedure
Add/manage SIP server IP address access control lists on page 52
Add/Manage SIP-T GWCs on page 56

Procedures for creating and modifying NCGL filesystems

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

Procedure
Start filesystem monitoring on page 215
Stop filesystem monitoring on page 219
Modify filesystem monitoring thresholds on page 222
Remove a filesystem on page 225
Increase filesystem size on page 229
Create a filesystem on page 233

Procedures for performing Session Server platform re-commissioning

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

Procedure
Modify NCGL platform provisioning on page 205
Reprovision the Session Server NCGL platform software on page 193
Reconfigure the Session Server BIOS on page 189
Add a Session Server node to the SSPFS server web proxy on page 175

Procedures for managing SIP Gateway Application software

Refer to the Session Server Upgrades NTP, NN10349-461, for detailed information about reinstalling the SIP Gateway application as part of a maintenance release or major release upgrade activity.

Procedures for 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 Session Server unit.

Procedure
Lock the SIP Gateway application on page 160
Unlock the SIP Gateway application on page 163
Suspend the SIP Gateway application on page 166
Unsuspend the SIP Gateway application on page 169

Procedures for reconfiguring the SIP Gateway Application software

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

ATTENTION

When possible, only perform service affecting procedures on the standby Session Server 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	Complete procedure Configure SIP Gateway application parameters on page 44.
2	Complete procedure Configure Remote SIP Servers on page 21.
3	Complete procedure Add/manage SIP server IP address access control lists on page 52.
4	Complete procedure Add/Manage SIP-T GWCs on page 56.

Step	Procedure
5	Complete procedure Add/manage telephony profiles on page 62.
6	Complete procedure Add/manage NOAs, NPIs and Phone Context maps on page 73.
7	Complete procedure Add/Manage Access Link Maps on page 67.
8	Complete procedure Add/Manage SIP base protocols on page 86.
9	Complete procedure Add/Manage ISUP to SIP mapping on page 91.
10	Complete procedure Add/Manage SIP to ISUP mapping on page 102.
11	Complete procedure Add/Manage SIP Redirection mapping on page 110.
12	Complete procedure Add/Manage ISUP variant mappings on page 117.
13	Complete procedure Manage TLS security parameters on page 130.

Procedures for monitoring the Session Server 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 Session Server platforms.

Procedure
View the operational status of the SIP Gateway application on page 136
View the operational status of a Session Server NCGL platform on page 141

Attach 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 a Session Server 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.

> **ATTENTION**
>
> 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.

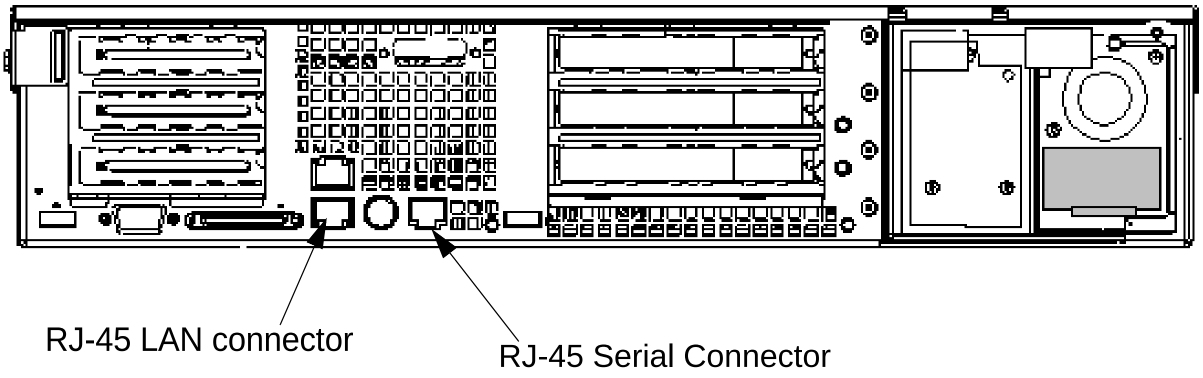
Use this procedure when the Session Server platform NCGL is not fully configured.

At the rear of the Session Server chassis.

1 Attach the VT100+ terminal to the serial port using the diagram shown below

> ***Note:*** Ensure that the Session Server 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.

Rear view of Session Server chassis



2 The procedure is complete.

Attach a VGA monitor and keyboard console

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

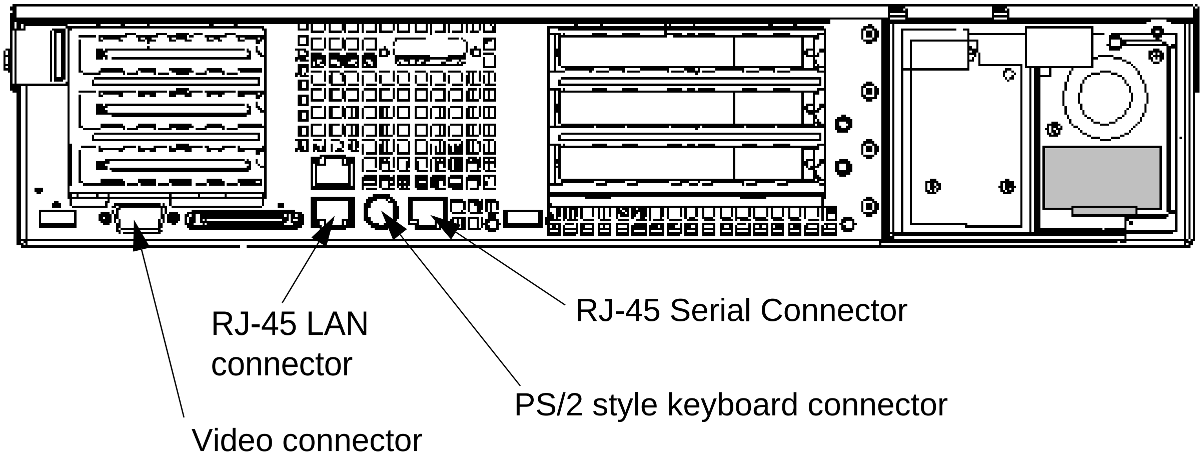
> **ATTENTION**
> You cannot use this method to fully commission a Session Server unit. Instead, use method Attach a VT-100 console monitor to the RJ-45 serial port on page 16.

At the rear of the Session Server chassis.

1 Plug in a PS/2 style keyboard and VGA monitor into the rear of the Session Server chassis using the diagram shown below.

Note: Optionally use a dongle (Y cable) to connect both keyboard and mouse to the same PS/2 mouse/keyboard port.

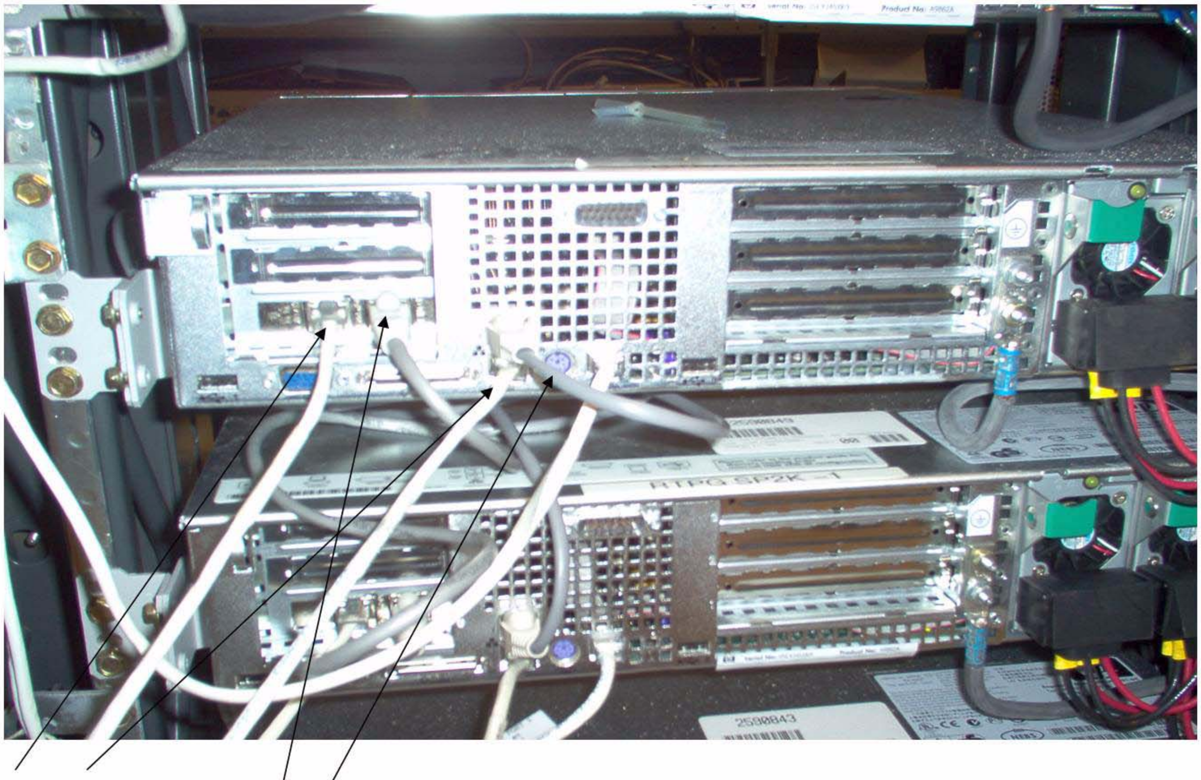
Rear view of Session Server chassis



2 The procedure is complete.

Checking ethernet cabling at the rear of the Session Server units

Each Session Server is 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.



Ethernet Connectivity interface to the CS LAN

Cross-over Cable for Point-to-point connectivity between two units in the same node.

Individual procedures

Although many of the modular procedures found in this NTP can be executed on their own to complete some tasks, most must be executed as part of a higher level activity, where performing a series of multiple tasks or procedures is required. Therefore, it is recommended that you refer to the high level activity, found in the overview section of this NTP, for complete instructions for performing high level tasks.

Configure 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 Session Server communicates with a remote SIP server or any remote SIP device (such as other CS 2000 Call Servers or a Multimedia Communication Server (MCS) using the session initiation protocol. Session Server 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 adding a new SIP server associated with a new trunk group, first refer to section Adding DPT trunk group connections handled by Session Server on page 11 to ensure that all prerequisite activities have been completed.

When modifying GWC and IP address datafill for existing remote SIP servers, GWC names and IP addresses cannot be re-used.

For sites that enable optional access control lists (ACL), 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.

Prerequisites

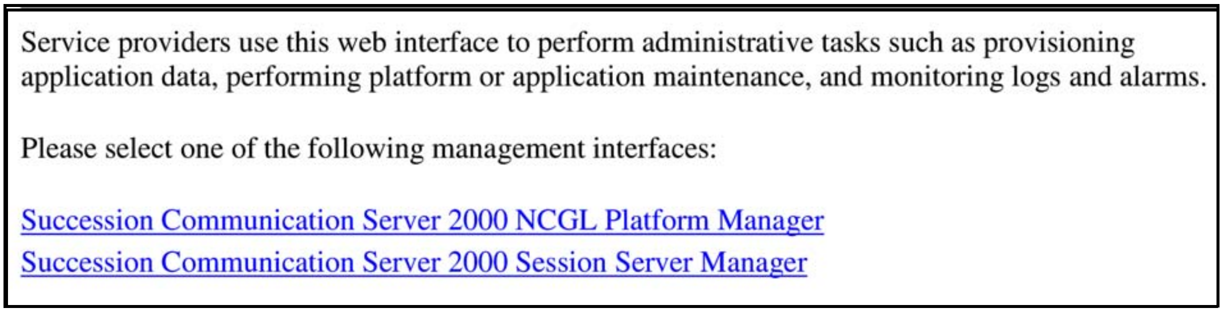
This procedure must be completed before procedure Add/Manage Access Link Maps on page 67 is completed.

Review section Recommended provisioning information for various configurations on page 36 for details regarding completing datafill activities applicable to your configuration and Carrier VoIP software release.

Action

At the CS 2000 Session Server Launch Point

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

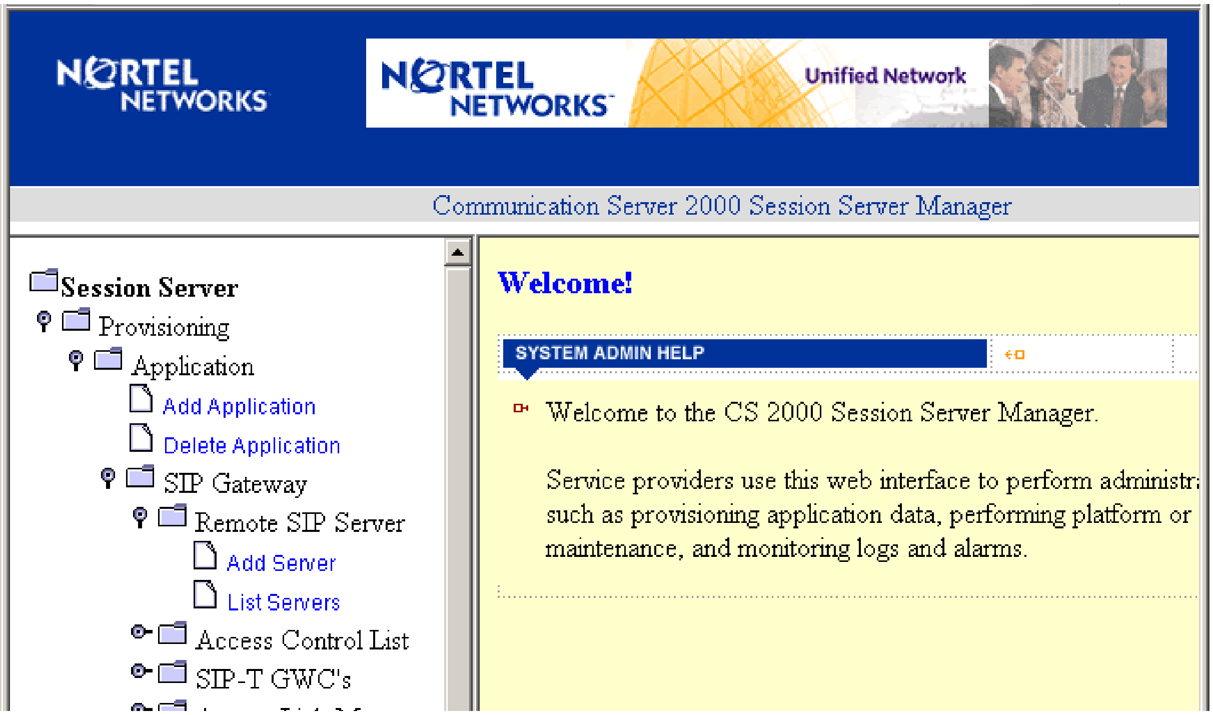


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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



Welcome to the CS 2000 Session Server Manager.

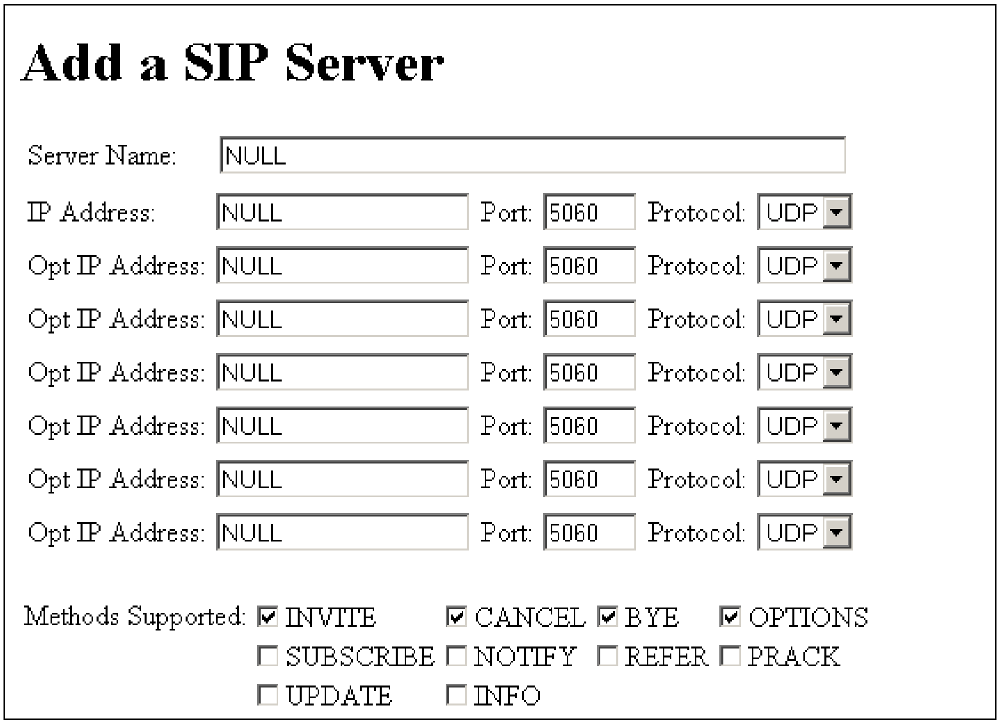
Service providers use this web interface to perform administr such as provisioning application data, performing platform or maintenance, and monitoring logs and alarms.

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.



Add a SIP Server

Server Name: NULL

IP Address: NULL	Port: 5060	Protocol: UDP
Opt IP Address: NULL	Port: 5060	Protocol: UDP
Opt IP Address: NULL	Port: 5060	Protocol: UDP
Opt IP Address: NULL	Port: 5060	Protocol: UDP
Opt IP Address: NULL	Port: 5060	Protocol: UDP
Opt IP Address: NULL	Port: 5060	Protocol: UDP
Opt IP Address: NULL	Port: 5060	Protocol: UDP

Methods Supported: ☑ INVITE ☑ CANCEL ☑ BYE ☑ OPTIONS
□ SUBSCRIBE □ NOTIFY □ REFER □ PRACK
□ UPDATE □ INFO

5 Datafill each field using Table of recommended or default Remote SIP Server provisioning parameters on page 27. Default and recommended values are indicated in this table where appropriate. Also, review section Recommended provisioning information for various configurations on page 36 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 64 alphanumeric characters, with hyphens, underscores and periods allowed)
- IP Address (Use the default Port number and Protocol values; do not use 0.0.0.0)

  Note: In a loop-around configuration, the *IP Address* field for the Remote SIP server representing the Session Server should be datafilled with the active IP address of the Session Server 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)
- APN Information (select an APN representation from the drop-down menu; other fields can be left NULL)
- 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)

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

6 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.

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

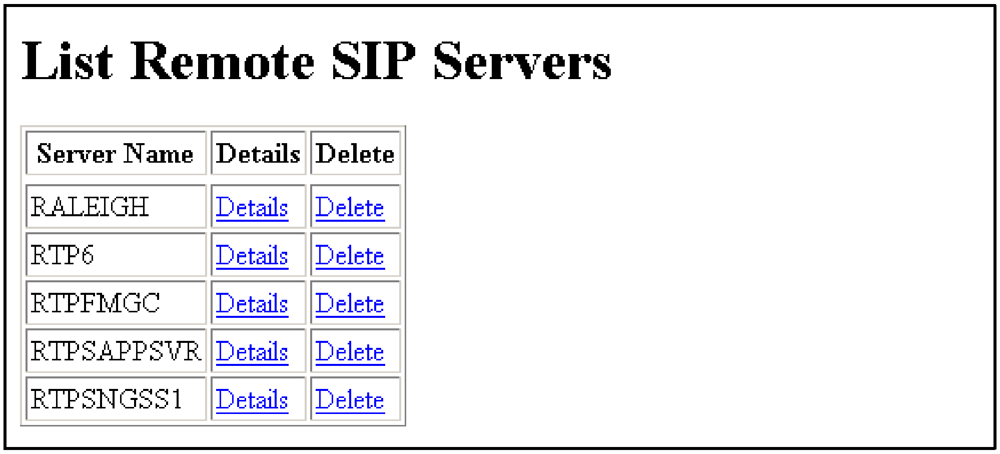
8 Use the following table to determine your next step:

If	Do
you want to add additional 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

If	Do
you want to delete an existing Remote SIP Server	skip to step 14
you are done with this procedure	skip to step 18

9 Click **List Servers**.

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

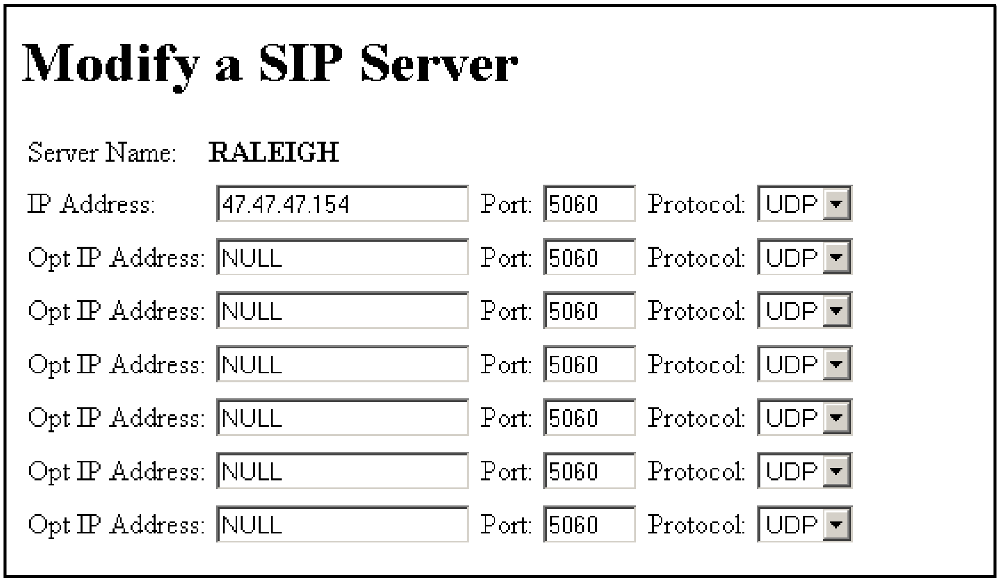


List Remote SIP Servers

Server Name	Details	Delete
RALEIGH	Details	Delete
RTP6	Details	Delete
RTPFMGC	Details	Delete
RTPSAPPSVR	Details	Delete
RTPSNGSS1	Details	Delete

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

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



Modify a SIP Server

Server Name: RALEIGH

IP Address:	47.47.47.154	Port:	5060	Protocol:	UDP
Opt IP Address:	NULL	Port:	5060	Protocol:	UDP
Opt IP Address:	NULL	Port:	5060	Protocol:	UDP
Opt IP Address:	NULL	Port:	5060	Protocol:	UDP
Opt IP Address:	NULL	Port:	5060	Protocol:	UDP
Opt IP Address:	NULL	Port:	5060	Protocol:	UDP
Opt IP Address:	NULL	Port:	5060	Protocol:	UDP

11 Refer to Table of recommended or default Remote SIP Server provisioning parameters on page 27 to assist with parameters.

12 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.

Note: 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.

13 Return to step 3 if you want to make other changes to other Remote SIP Servers, otherwise continue with step 18.

14 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.

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

Note: 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>?
```

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

17 Return to step 3 if you want to make other changes to other Remote SIP Servers, otherwise continue with step 18.

18 The procedure is complete.

Table of 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, refer to the following tables:

- Recommended provisioning information for various configurations on page 36
- Backward compatibility configuration information for VRDN configurations on page 40

Field	Description	Default Value or Range	Recommended Value
Server Name:	Character string name for the remote SIP server, up to 64 alphanumeric characters, with hyphens, underscores and periods allowed.	N/A	Use DNS naming conventions when naming your server.
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. ***Note:*** If used for loop-around calls, the IP address for the active Session Server 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.	Refer to section Recommended provisioning information for various configurations on page 36.
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.	Refer to section Recommended provisioning information for various configurations on page 36.

Field	Description	Default Value or Range	Recommended Value
Server Methods Supported	Contains the following: • Invite • Cancel • Bye • Options • Subscribe • Notify • Refer • Prack • Update • Info	All False; check the box to make it true (supported)	Refer to section Recommended provisioning information for various configurations on page 36.
URI Parameters Supported • CIC • RN • NPDI • Phone-Context	Click the check boxes for parameters that are supported. • CIC - this parameter carries Carrier Identification Parameter from SIP to ISUP and vice-versa. • RN - Redirect Number is used in LNP scenarios • NPDI - indicates the number in the Request-URL is ported • Phone-Context - indicates the context of the called party number in the Request-URL	All False; check the box to make it true (supported)	Refer to section Recommended provisioning information for various configurations on page 36.

Field	Description	Default Value or Range	Recommended Value
SIP Headers Supported	Click appropriate headers that are supported by remote server: • Content-Disposition • Remote-Party-ID • P-Asserted-ID • P-Preferred-ID • Privacy • Reason • Replaces • Referred-By • Originating Dial Plan ID • Billing Number • Rate Plan • Terminating Dial Plan ID • Diversion	All False; check a box to make the header true (supported)	Refer to section Recommended provisioning information for various configurations on page 36.
ISUP to SIP Cause Map	Contains the name of the mapping table for ISUP Release Cause to SIP response code.	unselected	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.	unselected	Select a preferred map from the list or use DEFAULT
SIP Redirection Map	Contains the name of the mapping table for redirection mapping.	unselected	Select a preferred map from the list or use DEFAULT
ISUP Variant to SIP Version Mapping	Contains the name of the mapping table for ISUP Variant to SIP Version Mapping.	unselected	Select a preferred map from the list or use DEFAULT

Field	Description	Default Value or Range	Recommended Value
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.	unselected	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	The priority range is 123; ordered as listed.	Refer to section Recommended provisioning information for various configurations on page 36.
APN Representation	Use defaults unless otherwise specified • APN Representation • APN Prefix • Phone Context for APN	N/A or blank field	Refer to section Recommended provisioning information for various configurations on page 36.
BCI Data	• Interworking Indication	• Interworking Encountered • Interworking Not Encountered	Refer to section Recommended provisioning information for various configurations on page 36
	• ISUP / BICC Indicator	• ISUP Not Used All the Way • ISUP Not Used All the Way	
	• ISDN Access Indicator	• Terminating Assess Not ISDN • Terminating Assess Not ISDN	

Field	Description	Default Value or Range	Recommended Value
FCI Data	• Domestic/International Call Indication	• Treat as Domestic Call • Treat as International Call	Refer to section Recommended provisioning information for various configurations on page 36
	• Interworking Indicator	• Interworking Encountered • No Interworking Encountered	
	• ISDN User Part Indicator	• ISUP Not Used All the Way • ISUP Used All the Way	
	• ISUP/BICC Preference Indicator	• ISUP/BICC Not Required • ISUP/BICC Required All the Way	
	• ISDN Access Indicator	• Originating Access is Not ISDN • Originating Access is ISDN	
SIP Header Format	Supports the following form of SIP headers: • Compact • Long	Compact	Use the default
Options for Heartbeat	Indicates if SIP Options method is used to determine accessibility of the SIP server.	Yes	Use the default

Field	Description	Default Value or Range	Recommended Value
Telephony Profile Support	An indication of whether or not the Session Server sends the X-Nortel_profile header to this remote SIP Server. ***Note:*** Datafill with “No” when the Remote SIP Server does not support receiving the X-Nortel_Profile header in the SIP message.	Yes	Use the default
Use Info for Long Call Audit	Long call audit provisioning.	No	Use the default
Map Non-Screened RPI To Calling #	Whether or not to include RPI header for clg number when building outgoing INVITEs	No	Use the default
Accept Early SDP	Determines if Early Session Description Protocol is allowed.	Yes	Refer to section Recommended provisioning information for various configurations on page 36.
Accept Invite Without SDP	Indicates whether or not 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
E.164 Format Allowed	Indicates if E.164 format is supported. ***Note:*** To derive ETSI ISUP messages utilizing SIP instead of SIP-T, value must be set to No.	No	Refer to section Recommended provisioning information for various configurations on page 36.

Field	Description	Default Value or Range	Recommended Value
Enforce CODEC-Compatibility	Indicates whether support for other codec is provided. If Yes, then at least one of the codec fields must be set to yes in the Config Data web page. Refer to procedure Configure SIP Gateway application parameters on page 44.	No	Refer to section Recommended provisioning information for various configurations on page 36.
Accepts Encapsulated ISUP	Indicates whether to perform ISUP encapsulation or not. **Note:** In order 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	Refer to section Recommended provisioning information for various configurations on page 36.
Conn Mode Allowed	Use default unless otherwise specified	No	No
OCN Allowed	Use default unless otherwise specified	No	No
Country Code Support	Indicates if country code screening is supported. If yes a country code must be datafilled.	No	Refer to section Recommended provisioning information for various configurations on page 36.
Country Code	Indicates if Country Code is supported. If supported, then datafill 3 digit Country Code if Country Code Support is set to Yes.	field is blank if Country Code Support = No	Refer to section Recommended provisioning information for various configurations on page 36.
Prefix Digit Used	Use default unless otherwise specified	No	No
Prefix Digit for Int	Use default unless otherwise specified	default is for field to be blank	Use 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.	7	Use the default

Field	Description	Default Value or Range	Recommended Value
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	There is no default.	Refer to section Recommended provisioning information for various configurations on page 36.
Agent Representation	Indicates agent supported ISUP, PRI or Line.	ISUP	Refer to section Recommended provisioning information for various configurations on page 36.
"unknown" header	Indicates the String to use when Presentation indication is Unknown	default is for field to be blank	Use default unless otherwise specified
"anonymous" header	Indicates the String to use when Presentation indication is restricted	default is for field to be blank	Use default unless otherwise specified

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 specific requirements. The different configurations documented include:

- Session Server-to-Session Server
- Session Server-to-SN07/SN08 VRDN
- Session Server-to-MCS

Use following table, which captures the provisioning information for the above specific configurations used in SN08 when using Table of recommended or default Remote SIP Server provisioning parameters on page 27 to provision your Session Server.

Note: Refer to the Footnotes section at the end of this table for footnote details.

Field	Session Server - MCS	Session Server - SN07/SN08 VRDN	Session Server-Session Server
IP Address	x.x.x.x	x.x.x.x	x.x.x.x
Port	5060	5060	5060 or 5061[1]
Protocol	UDP	UDP	UDP, TCP or TLS
Optional IP (1-6)	none	none	none
Methods:	INVITE, CANCEL, BYE, OPTIONS, PRACK	INVITE, CANCEL, BYE, OPTIONS, SUBSCRIBE, NOTIFY, PRACK, INFO	INVITE, CANCEL, BYE, OPTIONS, SUBSCRIBE, NOTIFY, PRACK, INFO, UPDATE[2], REFER
URI Parameters Supported	none	cic	all
SIP Headers supported	Content-Disposition, one of Remote-Party-ID or P-Asserted-ID/ Privacy	Content-Disposition, one of Remote-Party-ID or P-Asserted-ID/ Privacy, Diversion	Content-Disposition, one of Remote-Party-ID or P-Asserted-ID/ Privacy, Reason, Replaces, Referred-By, Diversion

Field	Session Server - MCS	Session Server - SN07/SN08 VRDN	Session Server-Session Server
ISUP to SIP Cause Map[3]	Default	Default	Default
SIP to ISUP Cause Map[4]	Default	Default	Default
SIP Redirection Map[5]	Default	Default	Default
ISUP Variant to SIP Version Map[6]	Default	Default[7]	Default
NOA/NPI to Phone Context Map:	Default	Default	Default[8]
SIP Cause Precedence Priority	Default (OR) Encap: Third Retry: Second CauseCode: First	Default	Any
APN Representation	Not Applicable	Not Applicable	Applicable[9]
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
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 nonISDN	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN

Field	Session Server - MCS	Session Server - SN07/SN08 VRDN	Session Server-Session Server
SIP Header format	Compact or Long	Compact or Long	Compact or Long
Options for Heartbeat	Yes	Yes	Yes
Telephony Profile	Yes	Yes	Yes Or No
Use Info for Long Call Audit	Yes	Yes	Yes Or No
Map non-screened RPI to Calling #	Yes	Yes	Yes
Accepts Early SDP[10]	No	Yes	Yes Or No
Accept Invite without SDP	Yes	Yes	Yes
E.164 Format Allowed[11]	No	No	Yes[12]
Enforce Code-Compatibility[13]	No	No	Yes Or No[14]
Accepts Encapsulated ISUP	No	Yes	Yes Or No[15]
Conn Mode Allowed	Use default unless otherwise specified	No	No
OCN Allowed	Use default unless otherwise specified	No	No
CountryCode Support[16]	No	No	Yes Or No
Prefix Digit Used	Use default unless otherwise specified	No	No
Prefix Digit for Int	Use default unless otherwise specified	Use default unless otherwise specified	Use default unless otherwise specified
Hop-Counter	2[17]	7	7

Field	Session Server - MCS	Session Server - SN07/SN08 VRDN	Session Server-Session Server
Out of Band DTMF	vnd.nortelnetworks.digits	telephone-event	telephone-event
Agent	ISUP	ISUP	ISUP
Unknown Header	Any String	Any String	Any String
Anonymous Header	Any String	Any String	Any String
Footnotes			

1. 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 Session Server units. The default protocol port for TCP and UDP is 5060. The default protocol port for TLS is 5061.
2. Either all the nodes in a SIP call should support UPDATE, or none of them should, otherwise, undesired behavior may occur.
3. A custom ISUP - SIP cause map can be added by clicking on the "ISUP and SIP Mappings" tab and adding a new mapping under the "ISUP to SIP Map".
4. A custom SIP - ISUP cause map can be added by clicking on the "SIP and ISUP Mappings" tab and adding a new mapping under the "SIP to ISUP Map".
5. A custom SIP Redirection Map can be added by clicking on the "ISUP and SIP Mappings" tab and a new mapping under the "SIP Redirection".
6. This maps the ISUP Protocol/Version/Variant to the SIP base and Version fields. See FN section for instructions on how to add a new mapping. Refer to table Protocols, versions and variants used for VRDN communication on page 129 for different protocol variants that are required for communicating with VRDN configurations. For all other configurations, base/version entries are configurable.
7. When interworking with VRDN, add an entry with base/version of gr394/gr394 for any external protocol (such as Q764, NULL, NULL, gr394, gr394).
8. 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.
9. This value is used to set up handling of the Action Point Number (APN) for Private Numbering Plan-type calls. There are three different types that can be selected from the pull-down menu:
    1. Use Prefix ---> requires datafill of the Prefix field
    2. Use Prefix and Phone Context --> requires datafill of both Prefix and Phone-Context fields
    3. Phone Context Only --> requires datafill of the Phone Context Field.
10. 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'.
11. Setting this field to 'Y' requires datafilling the Country Code Supported filed to 'Y' and entry of valid Country Code in the provided field.
12. Setting this field 'Y' requires datafill of Country Code Supported to be set to 'Y' along with an entry of a valid Country Code in the provided field.
13. Setting this field to 'Y' requires selection of at least one applicable codec in the 'Config Data' section.
14. Setting this field to 'Y' requires selection of at least one applicable codec in the 'Config Data' section

15. 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 a Session Server-to-Session Server configuration.
16. This field must be set to ‘Y’ and a valid Country code datafilled, if the ‘E.164 Allowed’ field is set to ‘Y’
17. This value 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. Refer to the MCS SIP Application Module NTP, NN10029-111, for assistance with determining the Hop Count value set on the MCS.

Backward compatibility configuration information for VRDN configurations

The remote SIP server configuration page allows the craftsperson to provision a number of fields on a per customer specific requirements. The different configurations discussed include:

- Session Server - SN06.2 VRDN
- Session Server - SN06 VRDN

Use following table, which captures the provisioning information for the above specific configurations used in SN08 when using Table of recommended or default Remote SIP Server provisioning parameters on page 27 to provision your Session Server.

> ***Note:*** Refer to the Footnotes section at the end of this table for footnote details.

Field	Session Server - SN06.2 VRDN	Session Server - SN06 VRDN
IP Address	x.x.x.x	x.x.x.x
Port	5060	5060
Protocol	UDP	UDP
Optional IP (1-7)	none	none
Methods:	INVITE, CANCEL, BYE, OPTIONS, SUBSCRIBE, NOTIFY, PRACK, INFO	INVITE, CANCEL, BYE, OPTIONS, PRACK, INFO
URI Parameters Supported	cic	none

Field	Session Server - SN06.2 VRDN	Session Server - SN06 VRDN
SIP Headers supported	One of Remote-Party-ID or P-Asserted-ID/Privacy, Diversion	Remote-Party-ID
ISUP to SIP Cause Map[1]	Default	Default
SIP to ISUP Cause Map[2]	Default	Default
SIP Redirection Map[3]	Default	Default
ISUP Variant to SIP Version Map[4]	Default[5]	Default[6]
NOA/NPI to Phone Context Map:	None	None
SIP Cause Precedence Priority[7]	Default	Default
APN Information	Not Applicable	Not Applicable
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
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 nonISDN	Treat as National Call (D) Interworking Encountered (F) ISUP Not Used All the Way (HG) ISUP Not required (I) Originating Access nonISDN
SIP Header format	Compact or Long	Compact or Long
Options for Heartbeat	yes	yes
Telephony Profile	yes	yes
Use Info for Long Call Audit	yes	yes

Field	Session Server - SN06.2 VRDN	Session Server - SN06 VRDN
Map non-screened RPI to Calling#	yes	yes
Accepts Early SDP	yes	yes
Accept Invite without SDP	yes	yes
E.164 Format Allowed[8]	no	no
Enforce Code-Compatibility[9]	no	no
Accepts Encapsulated ISUP	yes	yes
CountryCode[10] Support	no	no
Hop-Counter	7	7
Out of Band DTMF	telephone-event	Not Applicable
Agent	ISUP	ISUP
Unknown Header	any string	any string
Anonymous Header	any string	any string
Footnotes:		

1. A custom ISUP - SIP cause map can be added by clicking on the “ISUP and SIP Mappings” tab and adding a new mapping under “ISUP to SIP Map”.
2. A custom SIP - ISUP cause map can be added by clicking on the “SIP and ISUP Mappings” tab and adding a new mapping under “SIP to ISUP Map”.
3. A custom SIP Redirection Map can be added by clicking on the “ISUP and SIP Mappings” tab and a new mapping under “SIP Redirection”.
4. This maps an ISUP Protocol/Version/Variant to the SIP base and Version fields. Refer to table Protocols, versions and variants used for VRDN communication on page 129 for different protocol variants that are required for communicating with VRDN configurations. For all other configurations, base and version entries are configurable.
5. When interworking with VRDN, add an entry with the base/version of gr394/gr394 for any external protocol (such as Q764, NULL, NULL, gr394, gr394).
6. When interworking with VRDN, add an entry with the base/version of gr394/gr394 for any external protocol (such as Q764, NULL, NULL, gr394, gr394).
7. You can change the precedence setting for testing purposes and select a different precedence for different interworkings.
8. Setting this field to ‘Y’ requires datafill of the “Country Code Supported” field to be set to ‘Y’ along with entry of a valid Country Code in the provided field.

9. Setting this field to ‘Y’ requires selection of at least one applicable codec in the “Config Data” section.
10. This field must be set to ‘Y’ and a valid Country code datafilled, if the ‘E.164 Allowed’ field is set to ‘Y’

Configure 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).

- localTCPport
- localUDPport
- supportedExtensionList
- MaxSipMsgSize
- SubsAutoRefresh
- MaxSubscription
- ProvisionalTimer
- enableOnBoardBilling
- maxCallLegs
- generalLingerTimer
- inviteLingerTimer
- retransmissionT1
- retransmissionT2
- retransmissionT4

The mgcHostName parameter should be datafilled to match parameter HOST_MGCNAME in table OFCENG in the CS 2000.

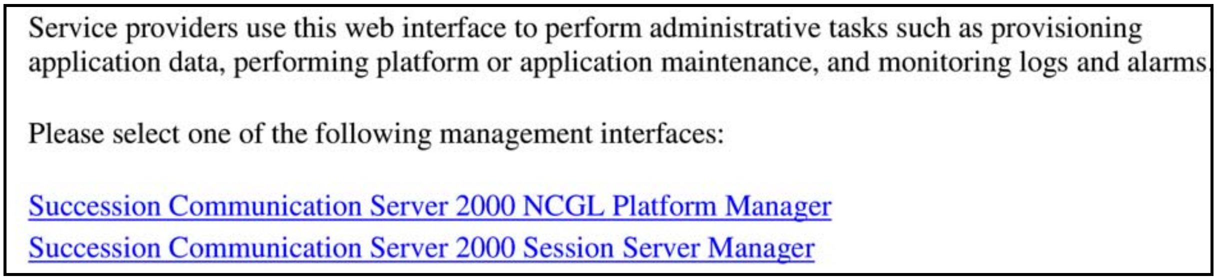
Prerequisites

There are no prerequisites for performing this procedure.

Action

At the CS 2000 Session Server Launch Point

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

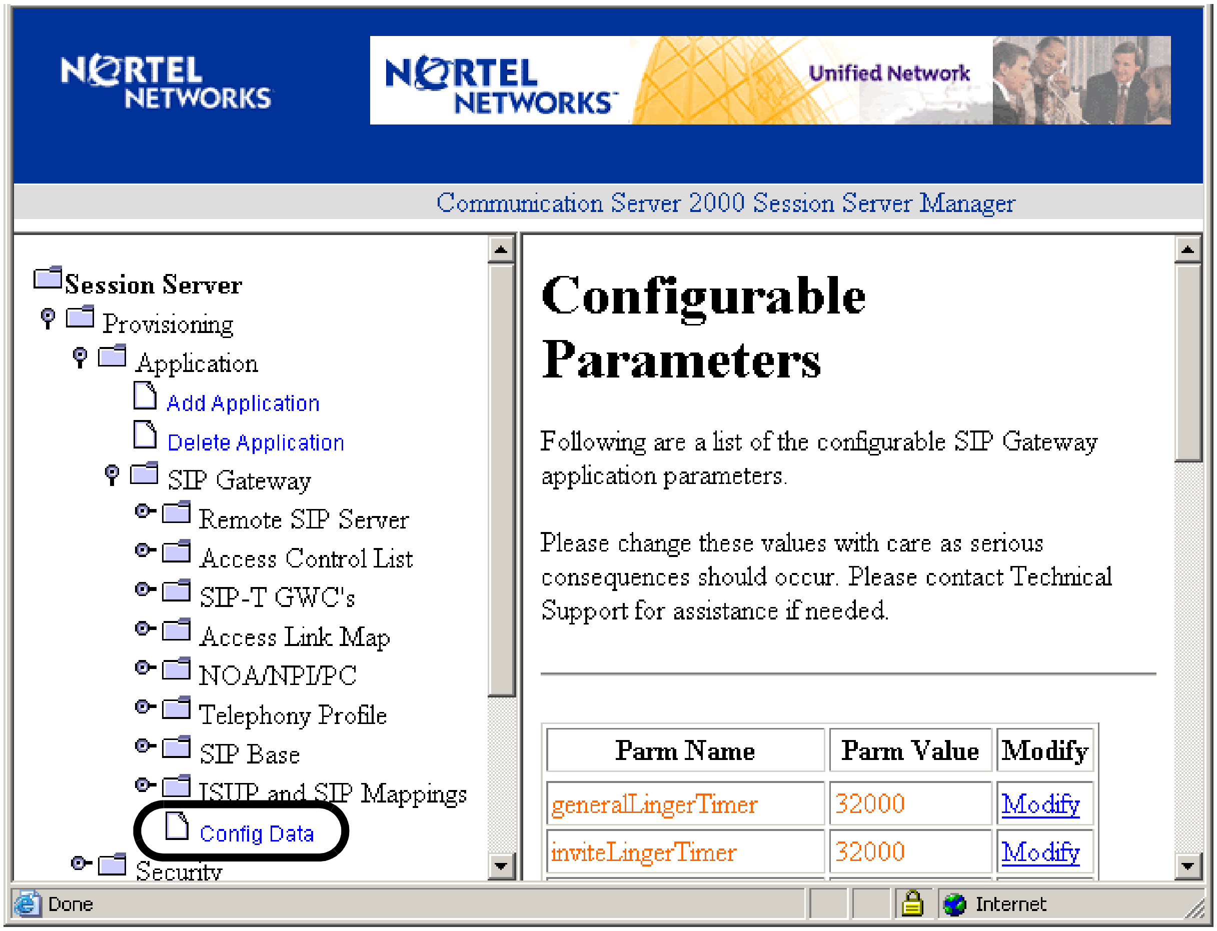


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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



Configurable Parameters

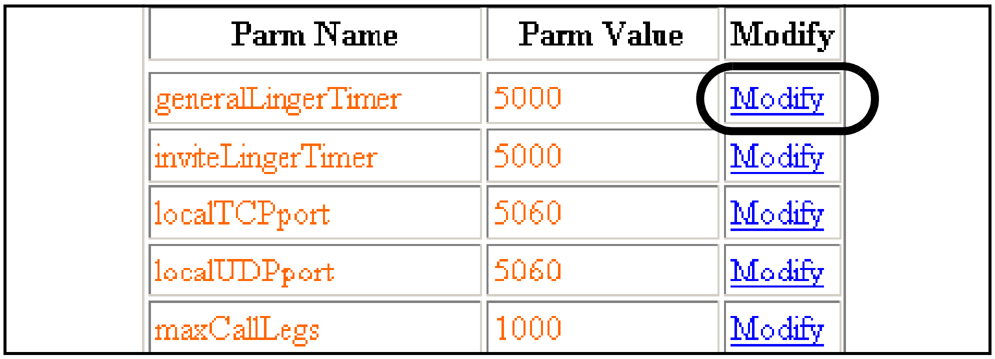
Following are a list of the configurable SIP Gateway application parameters.

Please change these values with care as serious consequences should occur. Please contact Technical Support for assistance if needed.

Parm Name	Parm Value	Modify
generalLingerTimer	32000	Modify
inviteLingerTimer	32000	Modify

The Configurable Parameters page opens in the right side frame.

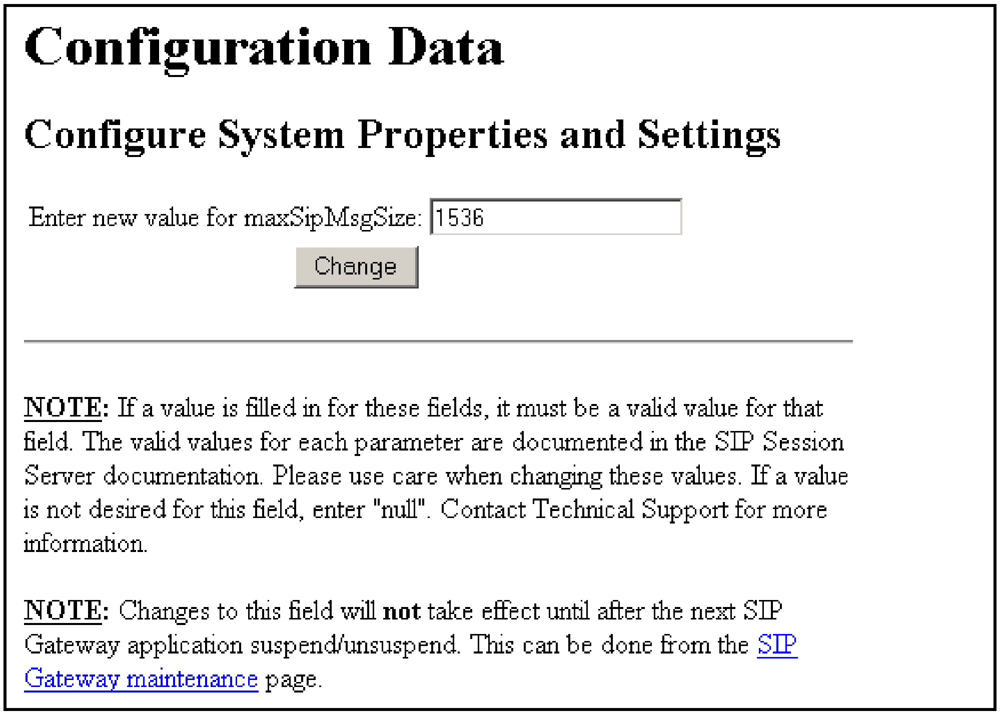
3 Click the **Modify** link to the right of the Parm Value to change.



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 on page 47 for a reference to the valid range and type of values for each parm value.



Configuration Data

Configure System Properties and Settings

Enter new value for maxSipMsgSize: 1536

NOTE: If a value is filled in for these fields, it must be a valid value for that field. The valid values for each parameter are documented in the SIP Session Server documentation. Please use care when changing these values. If a value is not desired for this field, enter "null". Contact Technical Support for more information.

NOTE: Changes to this field will **not** take effect until after the next SIP Gateway application suspend/unsuspend. This can be done from the SIP Gateway maintenance page.

5 If applicable, in the order listed, execute procedures Suspend the SIP Gateway application on page 166 and Unsuspend the SIP Gateway application on page 169 to force any new parameter values to take effect.

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

shown in orange in the GUI take effect after call processing is suspended and unsuspend.

6 The procedure is complete.

Additional Information

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

Note 1: Enforcement of all field values and ranges is handled by the database.

Note 2: 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

generalLingerTimer	After the Session Server sends a final response, it cannot be sure that the client gateway device has received the response message. The Session Server 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 Session Server 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.	Range = 1024 to 65534
		Default = 5060[1]

localUDPport	The local UDP port on which the SIP Stack listens.	Range = 1024 to 65534
		Default = 5060[2]

Parameter Name	Description	Recommended Value and Range

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

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 2000.
		Range = 200 to 4000
		Default = 1536

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 should match the value in field maxCallLegs.
		Range = 0 to 100000
		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)

Parameter Name	Description	Recommended Value and Range

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)

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 Session Server 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

Parameter Name	Description	Recommended Value and Range

codecG729Allowed
codecPCMUAllowed
codecPCMAAllowed
	These 3 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 Configure Remote SIP Servers on page 21.	Default = N[3]
		Default = N[4]
		Default = N[5]

enableOnBoardBilling	Create IPDR billing records and save to Session Server. Not supported in SN08.	Default = N[6]
enableAccessControlList[7]	Enables the capability to configure a valid range of IP addresses and netmasks that SIP servers may use to contact the Session Server SIP Gateway Application. Refer to procedure Add/manage SIP server IP address access control lists on page 52.	Default = N
mgcHostName	The FQDN (fully-qualified domain name) network name of the Session Server node. mgc_hostname can be up to 64 alphanumeric characters, with hyphens, underscores and periods allowed. ***Note:*** 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 the Session Server Security and Administration NTP, NN10346-611 for procedures on generating security certificates.	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
Footnotes:		

1.This can be configured for Session Server to Session Server calls.
2.This can be configured for Session Server to Session Server calls.
3.This must be set if ‘codec-enforcement’ is turned on for the server.
4.This must be set if ‘codec-enforcement’ is turned on for the server.
5.This must be set if ‘codec-enforcement’ is turned on for the server.
6.Billing is customer specific.
7.If this value is set to “Yes”, ensure ALL the IP Addresses the Session Server communicates with are listed in the Access Control List as shown in procedure Add/manage SIP server IP address access control lists on page 52. (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.

Add/manage 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 Session Server 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.

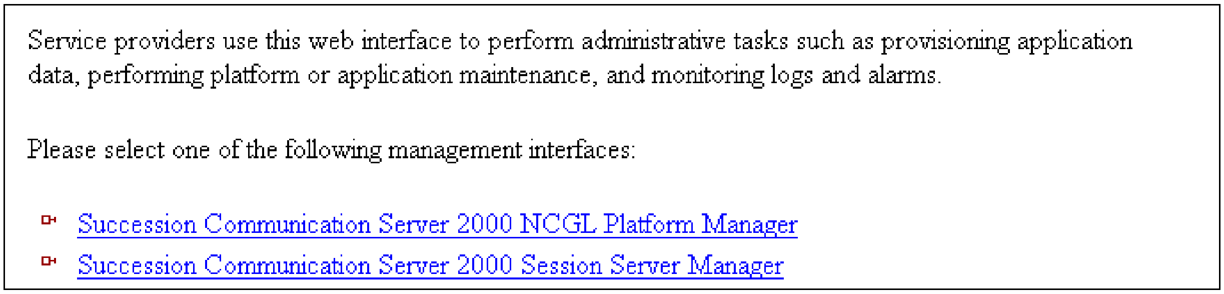
Prerequisites

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 Configure SIP Gateway application parameters on page 44.

Action

At the CS 2000 Session Server Launch Point

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

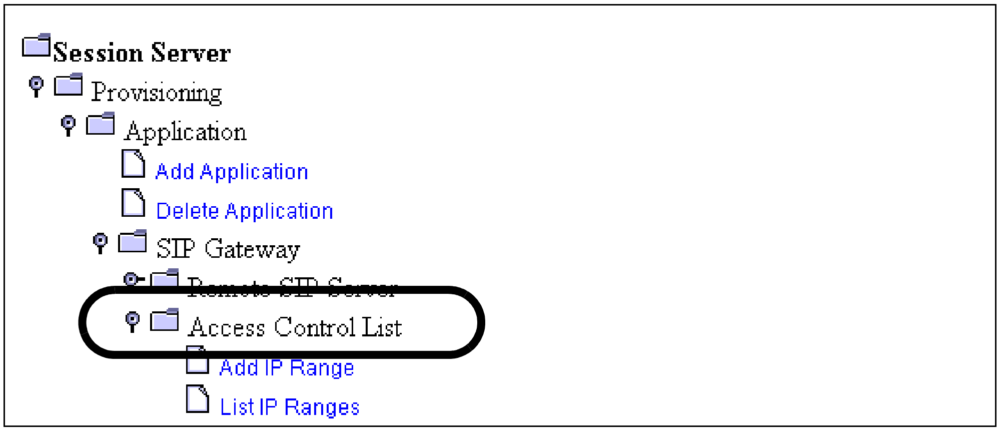


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

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

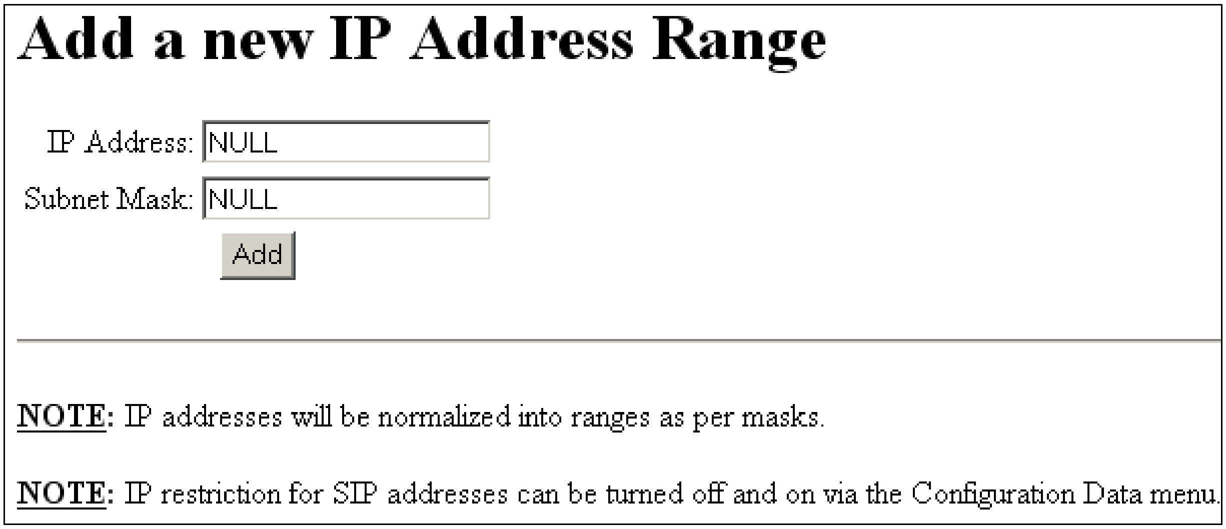


3 Use the following table to determine your next step:

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 9

If	Do
you are done with this procedure	step 13

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



Add a new IP Address Range

IP Address: NULL

Subnet Mask: NULL

NOTE: IP addresses will be normalized into ranges as per masks.

NOTE: IP restriction for SIP addresses can be turned off and on via the Configuration Data 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 commnuicating 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:

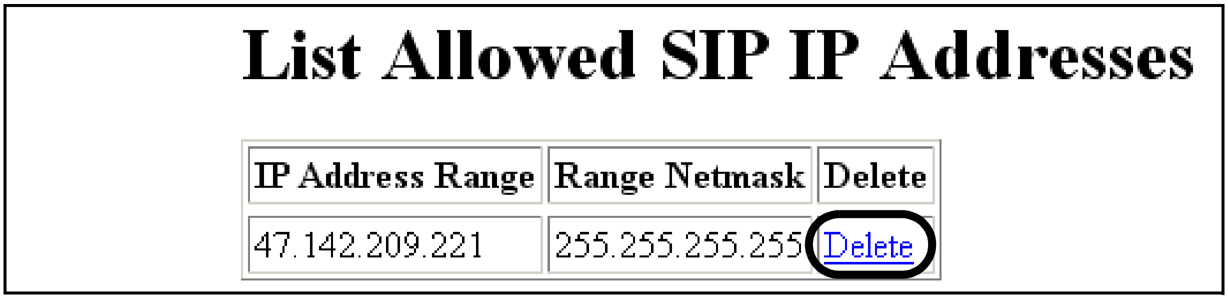
If	Do
you want to add additional IP address ranges	return to step 4
you want to view a list of existing Access Control Lists	skip to step 8
you want to delete a range IP addresses	skip to step 9
you are done with this procedure	skip to step 13

8 If you want to view a list of existing Access Control Lists, click the **List IP ranges** link. Otherwise skip to step 12.

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 step 12.

A page listing currently allowed IP ranges is presented.



List Allowed SIP IP Addresses

IP Address Range	Range Netmask	Delete
47.142.209.221	255.255.255.255	Delete

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

> ***Note:*** 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 The procedure is complete. Remember to set parameter enableAccessControlList to Yes in the Config Data.

Add/Manage 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.

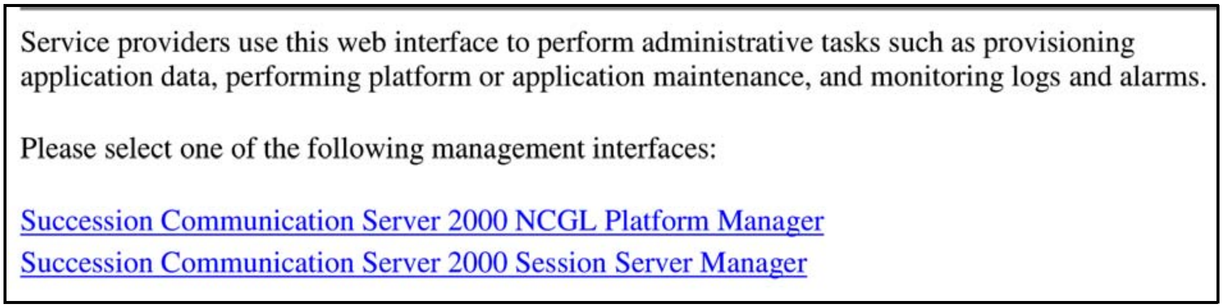
Prerequisites

SIP-T GWCs must be provisioned in the GWC Manager database. Refer to procedures in the GWC Configuration Management NTP, NN10205-511, to determine if SIP-T GWC types have already been provisioned.

Action

At the CS 2000 Session Server Launch Point

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

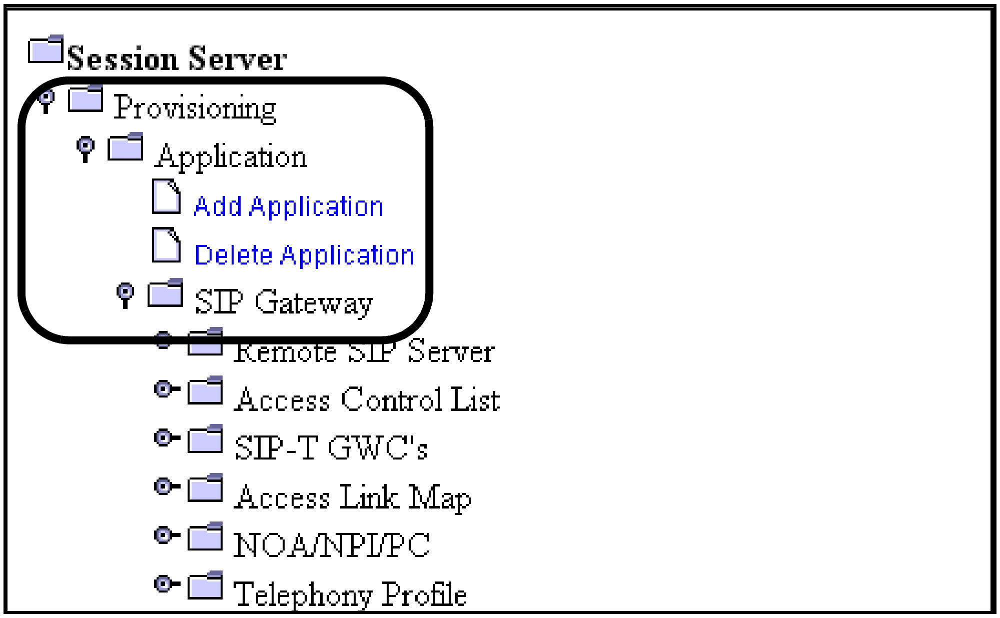


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

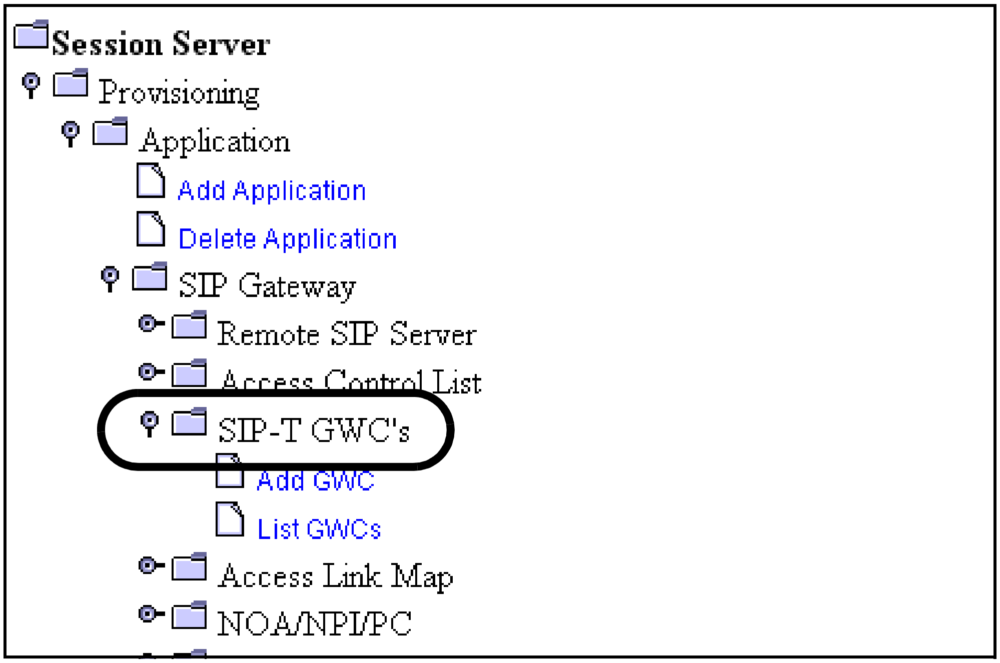
Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

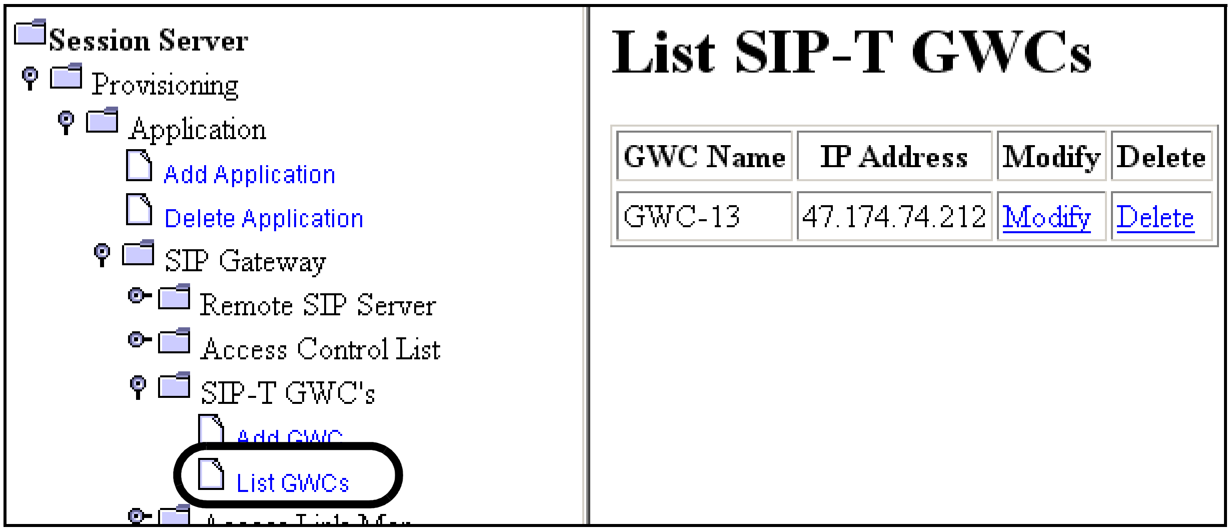
2 At the Session Server folder, click the **Provisioning folder,** then the **Application** folder and finally the **SIP Gateway** folder.



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.



List SIP-T GWCs

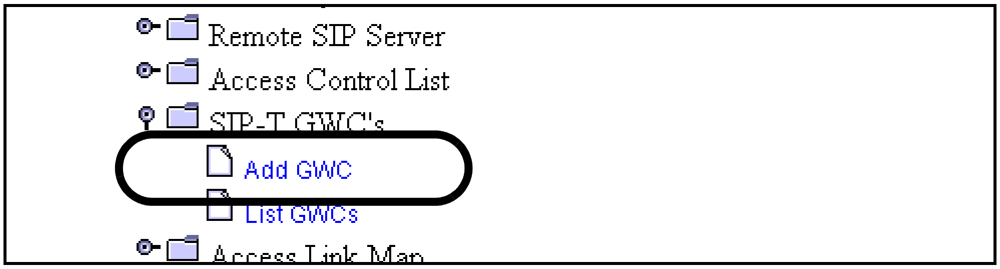
GWC Name	IP Address	Modify	Delete
GWC-13	47.174.74.212	Modify	Delete

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 13
you are done making changes	step 17

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

> ***Note:*** If no SIP-T GWCs are available for use, you must add them into the GWC Manager database. Refer to procedure *Add and configure a GWC node*, found in the GWC Configuration Management NTP, NN10205-511.

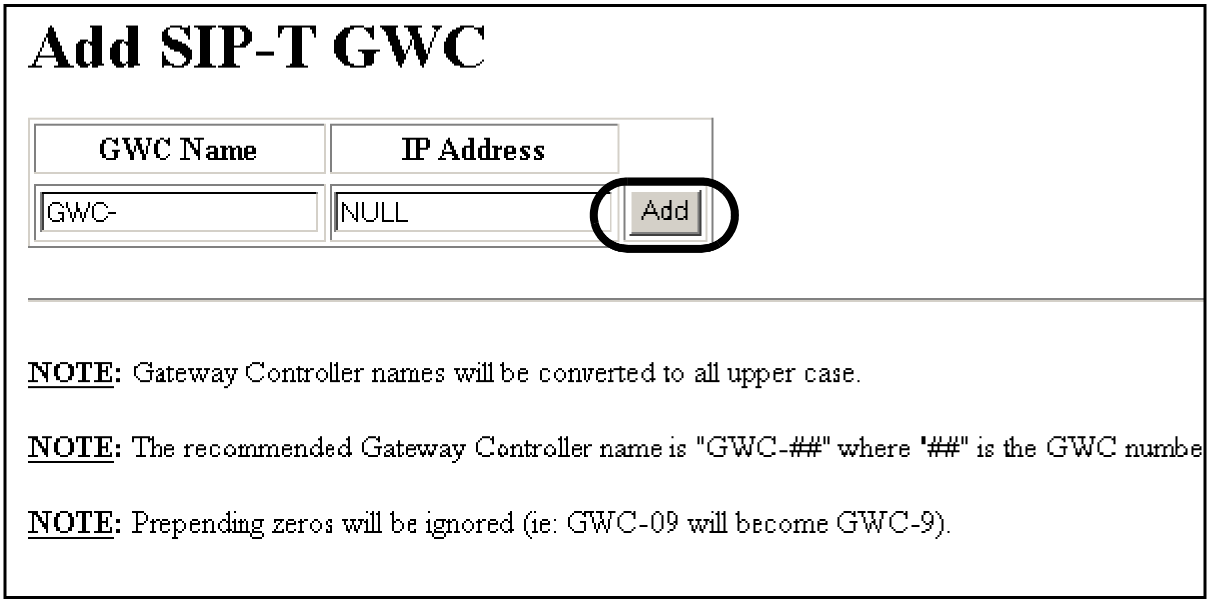


7 Datafill the GWC name and IP address of the active GWC unit in the GWC node, then click the **Add** button.

> **ATTENTION**
> GWC names and GWC IP addresses cannot be reused.

Note: 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 *View GWC node characteristics*, found in the GWC Configuration Management NTP, NN10205-511.



Add SIP-T GWC

GWC Name	IP Address	
GWC-	NULL	Add

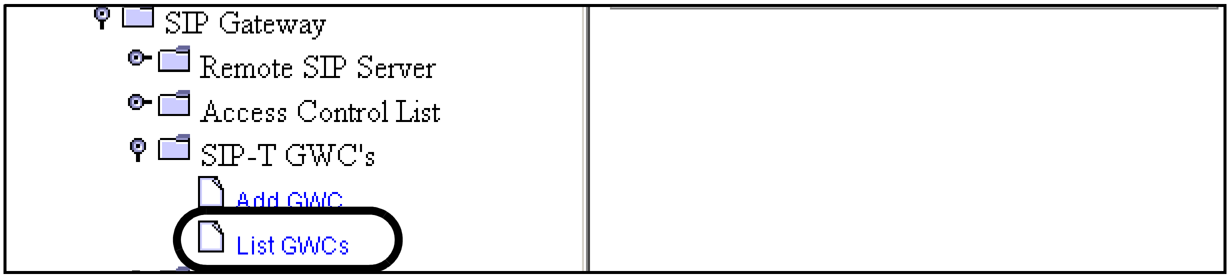
NOTE: Gateway Controller names will be converted to all upper case.

NOTE: The recommended Gateway Controller name is "GWC-##" where "##" is the GWC numbe

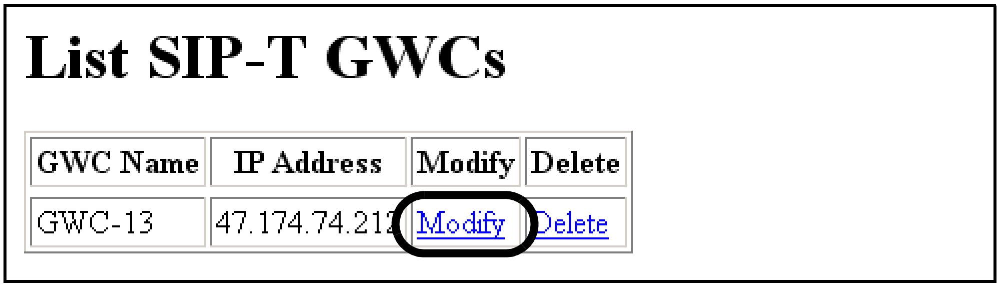
NOTE: Prepending zeros will be ignored (ie: GWC-09 will become GWC-9).

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.

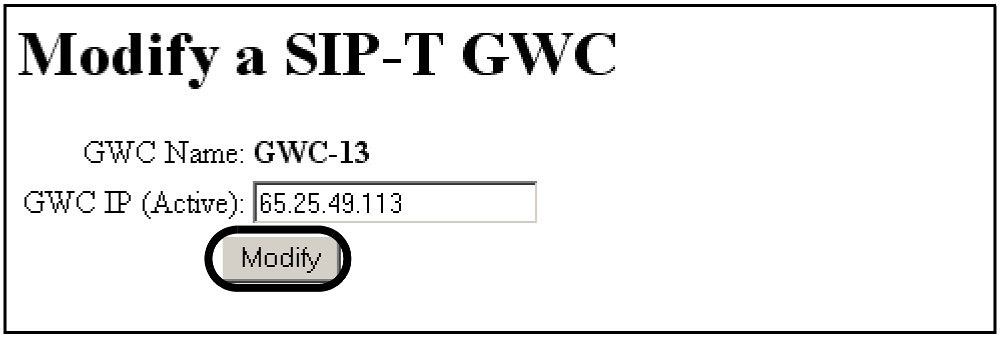


List SIP-T GWCs

GWC Name	IP Address	Modify	Delete
GWC-13	47.174.74.212	Modify	Delete

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.

> ***Note:*** 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 procedure *View GWC node characteristics*, found in the GWC Configuration Management NTP, NN10205-511.



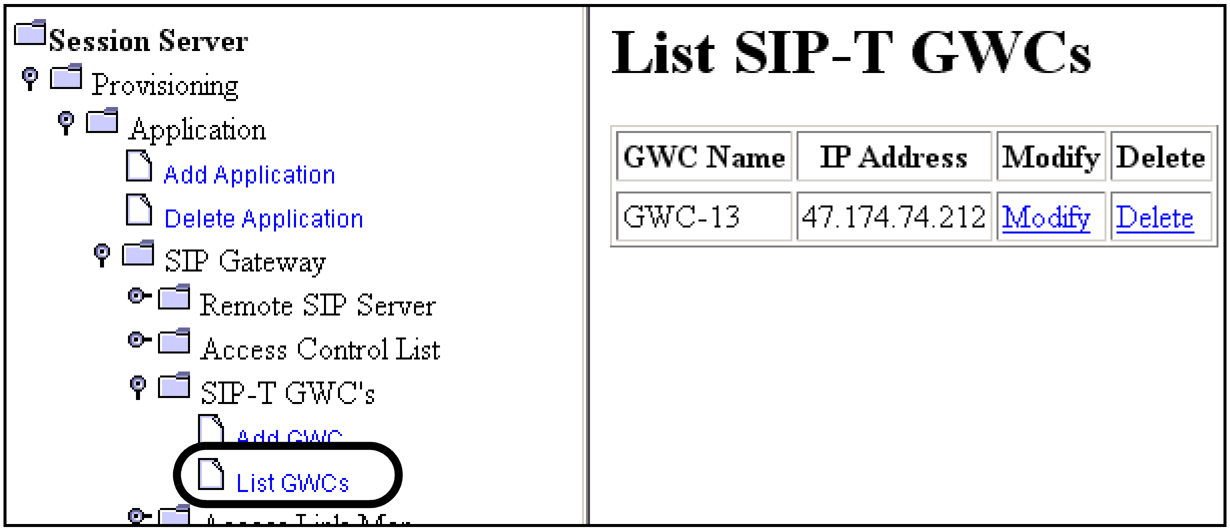
Modify a SIP-T GWC

GWC Name: **GWC-13**

GWC IP (Active): 65.25.49.113

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

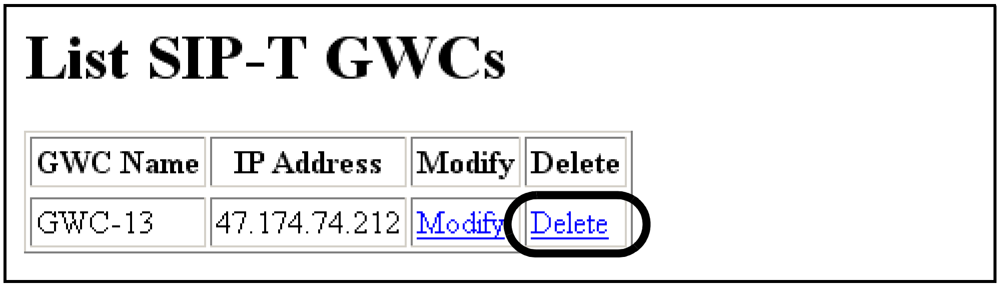
13 Click **List GWCs** to list all SIP-T GWCs existing in the SIP Gateway application database.



List SIP-T GWCs

GWC Name	IP Address	Modify	Delete
GWC-13	47.174.74.212	Modify	Delete

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



List SIP-T GWCs

GWC Name	IP Address	Modify	Delete
GWC-13	47.174.74.212	Modify	Delete

> ***Note:*** 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 13, otherwise return to step 5.

17 The procedure is complete.

Add/manage 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 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 section Adding DPT trunk group connections handled by Session Server on page 11 to ensure that all prerequisite activities have been completed.

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

- In the case where you are interconnecting a Session Server 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 Session Servers (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 Add/Manage Access Link Maps on page 67.

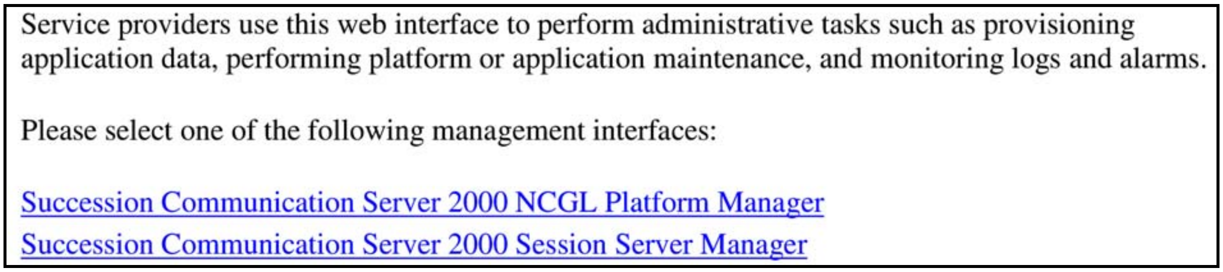
Prerequisites

This procedure must be completed before procedure Add/Manage Access Link Maps on page 67 is completed.

Action

At the CS 2000 Session Server Launch Point

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

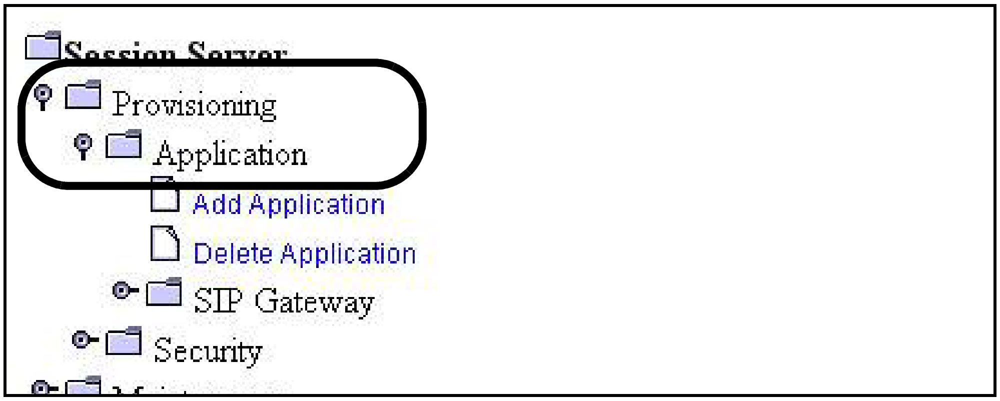


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

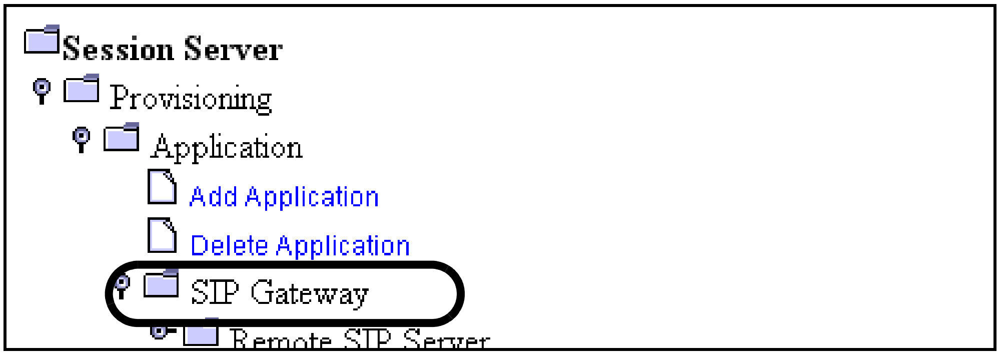
Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

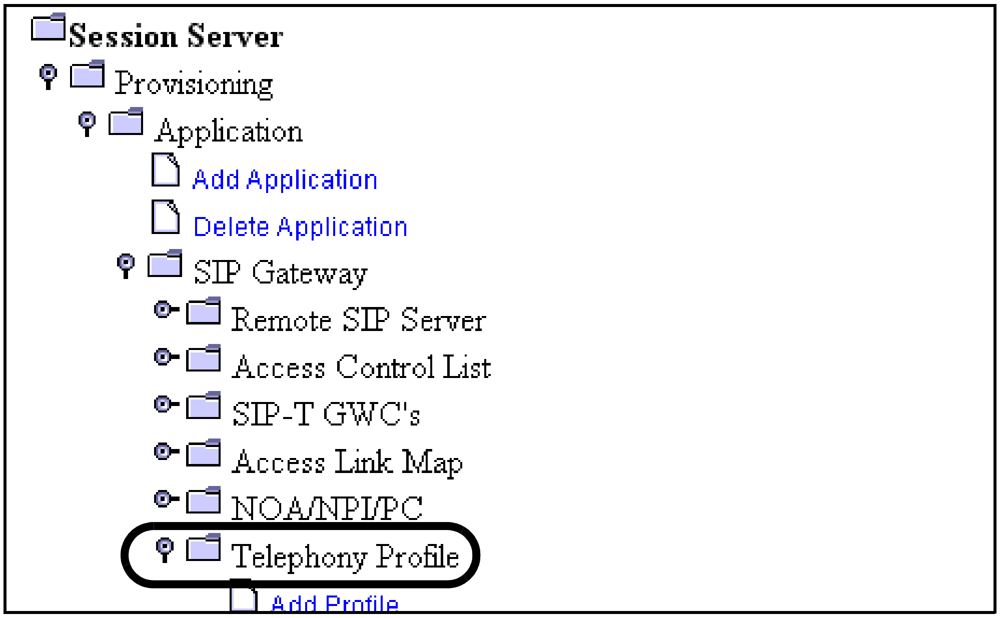
2 At the Session Server folder, click the **Provisioning folder,** then the **Application** folder.



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



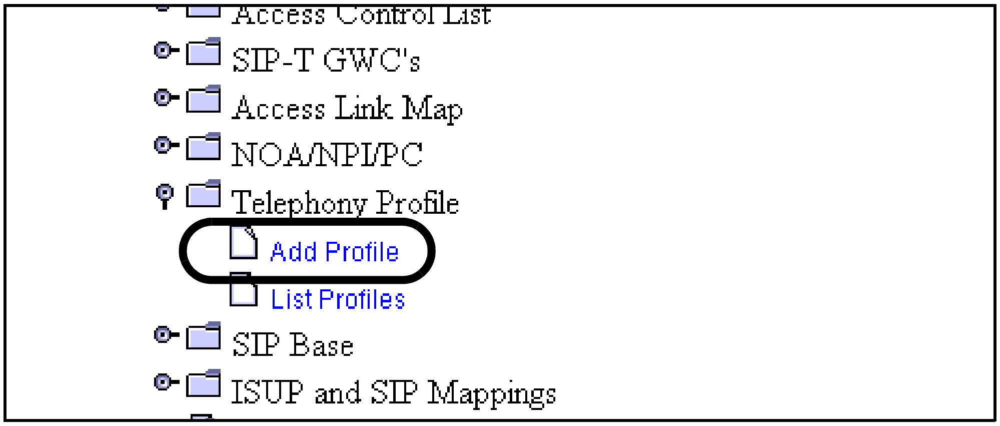
4 Click on the Telephony Profile link to open it.



5 Use the following table to determine your next step:

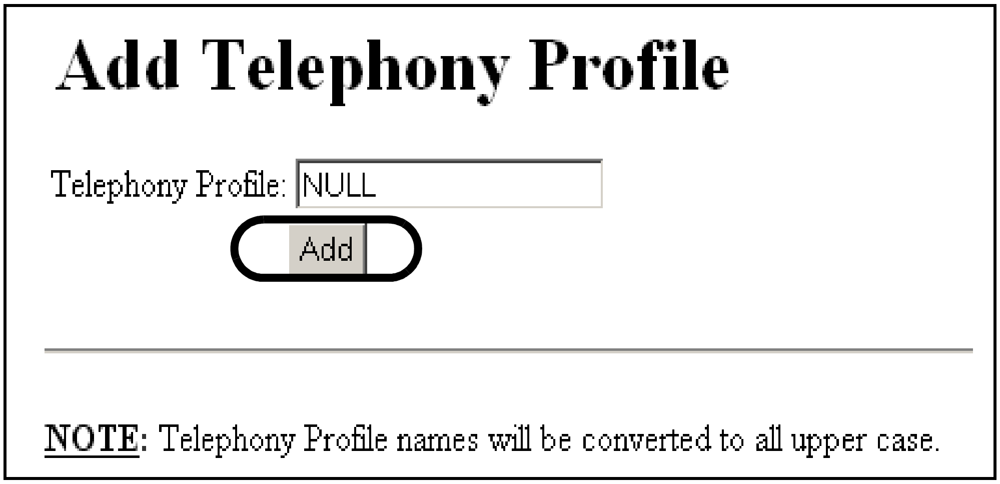
If	Do
you are adding a Telephony profile to the SIP GW Application database	step 6
you are listing or deleting a Telephony profile from the SIP GW Application database	step 9
you are done making changes to telephony profiles	step 14

6 Click the **Add Profile** link.



7 Enter a telephony profile name up to 32 alphanumeric characters, then click the **Add** button.

> ***Note:*** Telephony profile names should start with TP. To avoid confusion, do not use the same name for trunk names, telephony profile names and SIP link names.



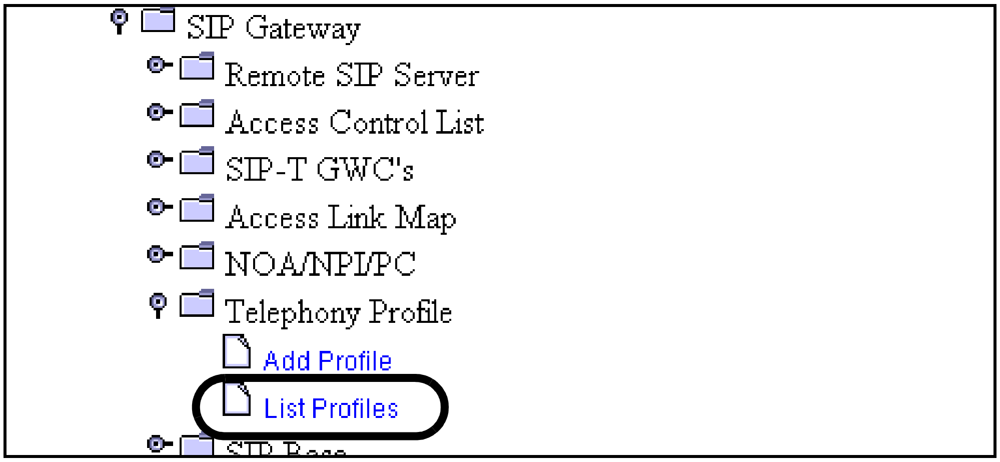
Add Telephony Profile

Telephony Profile: NULL

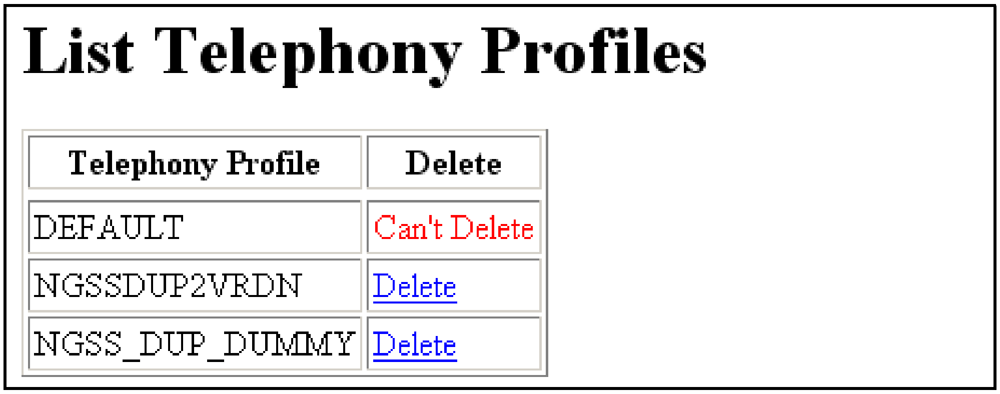
NOTE: Telephony Profile names will be converted to all upper case.

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.

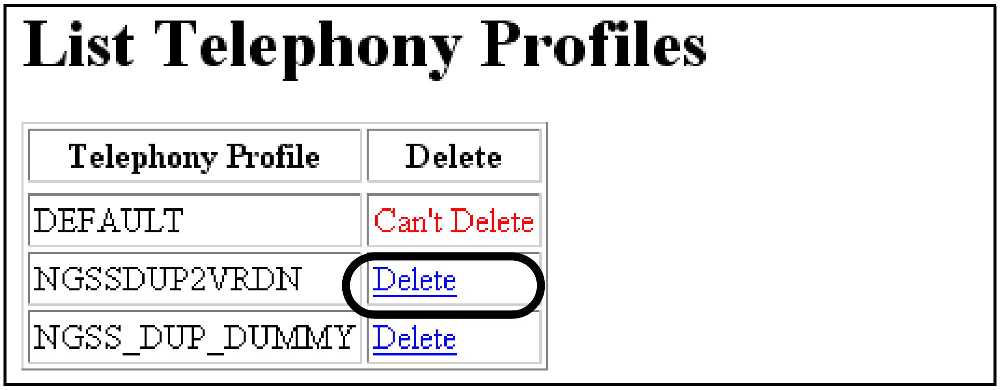


List Telephony Profiles

Telephony Profile	Delete
DEFAULT	Can't Delete
NGSSDUP2VRDN	Delete
NGSS_DUP_DUMMY	Delete

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 5.

Note: You cannot delete the default telephony profile.



List Telephony Profiles

Telephony Profile	Delete
DEFAULT	Can't Delete
NGSSDUP2VRDN	Delete
NGSS_DUP_DUMMY	Delete

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 step 5 if you are done deleting profiles.

14 The procedure is complete.

Add/Manage 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 Session Server nodes, link names should not be duplicated between Session Server nodes (in the access link mappings tables), otherwise undesireable behavior may result.

Prerequisites

If adding a new link map for use with a new trunk group, first refer to section Adding DPT trunk group connections handled by Session Server on page 11 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:

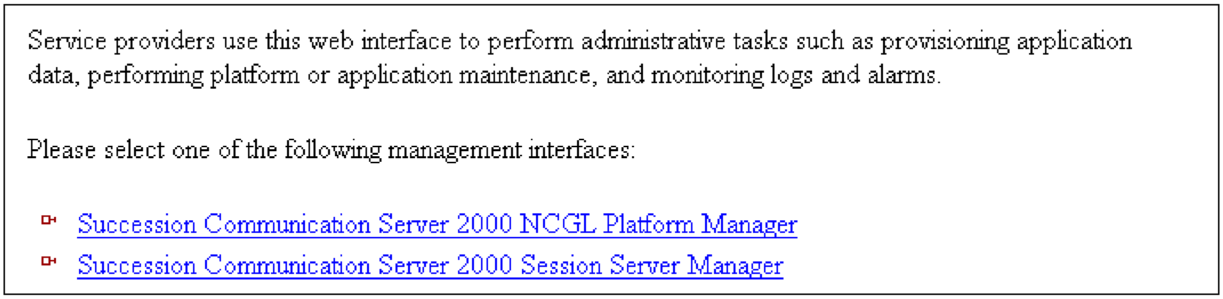
- Refer to Nortel Installation Method Session Server Commissioning, IM 24-0122, for instructions to ensure that core table SIPLINK is properly datafilled. Table SIPLINK provides link names needed to complete this procedure.

- Use procedure Add/manage telephony profiles on page 62 to ensure that a telephony profile is available.
- Use procedure Configure Remote SIP Servers on page 21 to ensure that a remote SIP servers is available.

Action

At the CS 2000 Session Server Launch Point

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

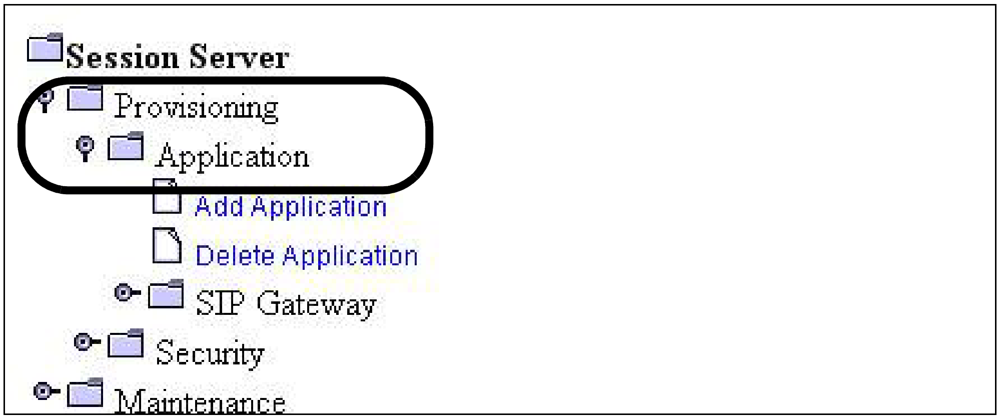


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

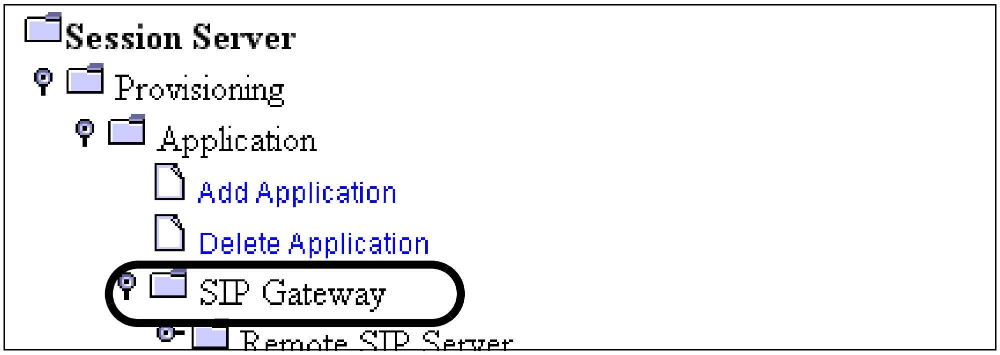
Please select one of the following management interfaces:

- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

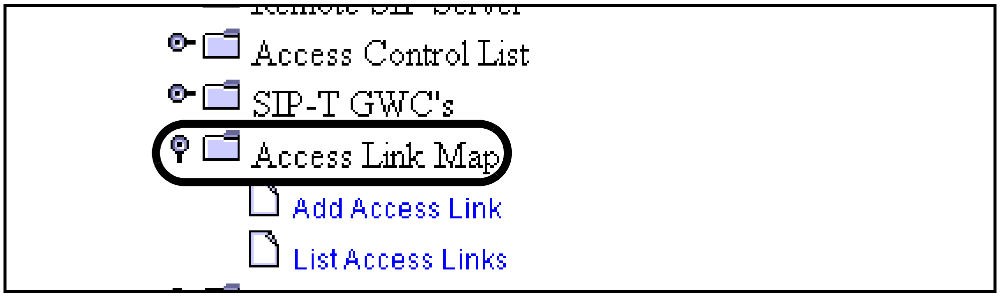
2 At the Session Server folder, click the **Provisioning folder,** then the **Application** folder.



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



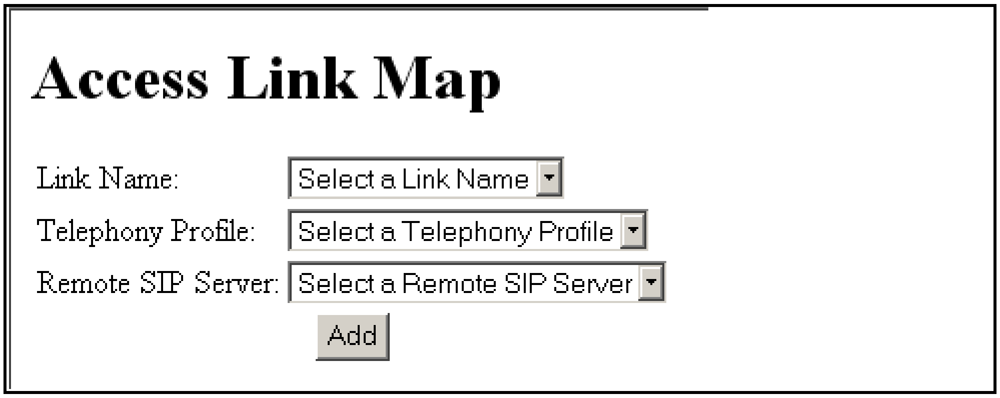
4 Click on the **Access Link Map** link to open it.



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 10
you are done making changes to Access Link maps	step 14

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



Access Link Map

Link Name: Select a Link Name

Telephony Profile: Select a Telephony Profile

Remote SIP Server: Select a Remote SIP Server

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

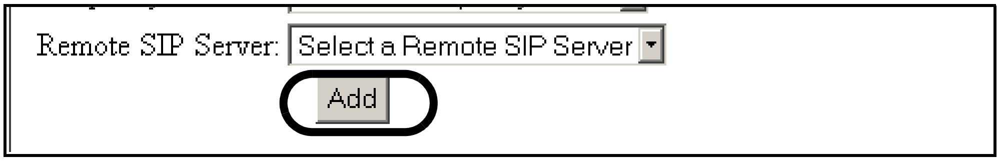
- Select a link name from the drop down menu.

  Note 1: 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 Add/Manage SIP-T GWCs on page 56, the Session Server sends an *mtc_discovery* message to the associated SIP-T GWC. The associated SIP-T GWC then responds with information about available link names.

  Note 2: Do not select a Link Name that is used by another Session Server node, otherwise undesireable behavior may result.

- Select a telephony profile from the drop down menu. Refer to procedure Add/manage telephony profiles on page 62 if a telephony profile is unavailable.
- Select a remote SIP server from the drop down menu. Refer to procedure Configure Remote SIP Servers on page 21 if there are no remote SIP servers to chose.

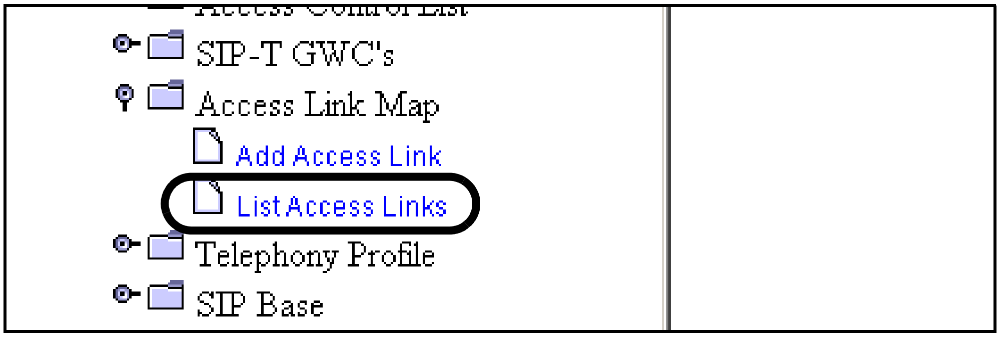
8 Once all selections are made and verified as correct, click the **Add** button.



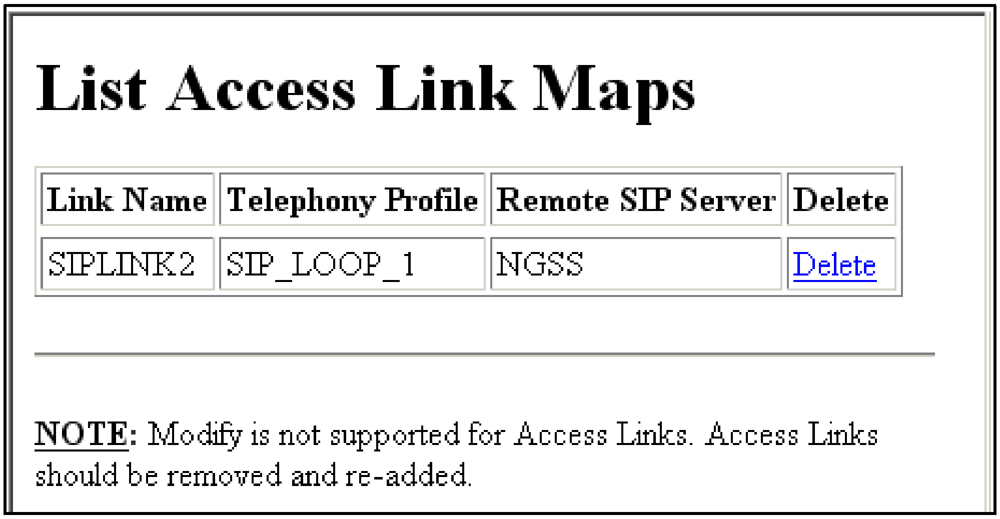
Remote SIP Server: Select a Remote SIP Server

9 Return to step 6 if you want to create additional Access Link Maps, otherwise return to step 5.

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.

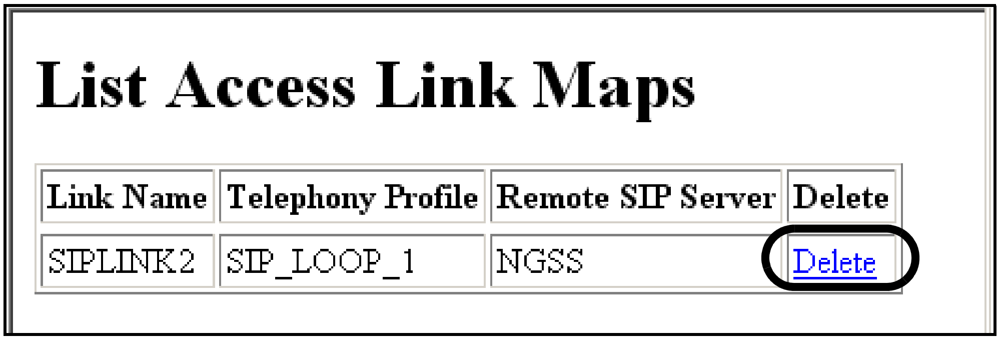


List Access Link Maps

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 5, otherwise continue with step 14.

14 If you have added, modified or deleted any access link maps, then it may be necessary to execute procedures Suspend the SIP Gateway application on page 166 and Unsuspend the SIP Gateway application on page 169, in the order listed, to force any parameter changes or maps to take effect. Otherwise skip to the next step.

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.

15 The procedure is complete.

Add/manage 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.

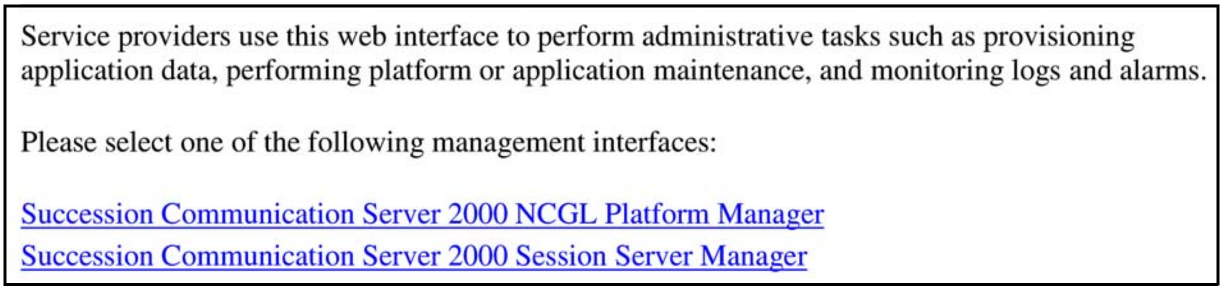
Prerequisites

There are no prerequisites for performing this procedure.

Action

At the CS 2000 Session Server Launch Point

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

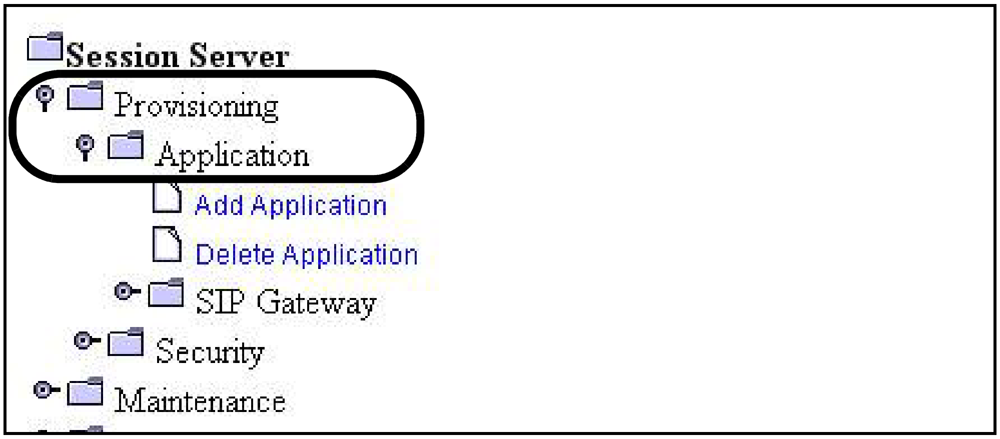


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

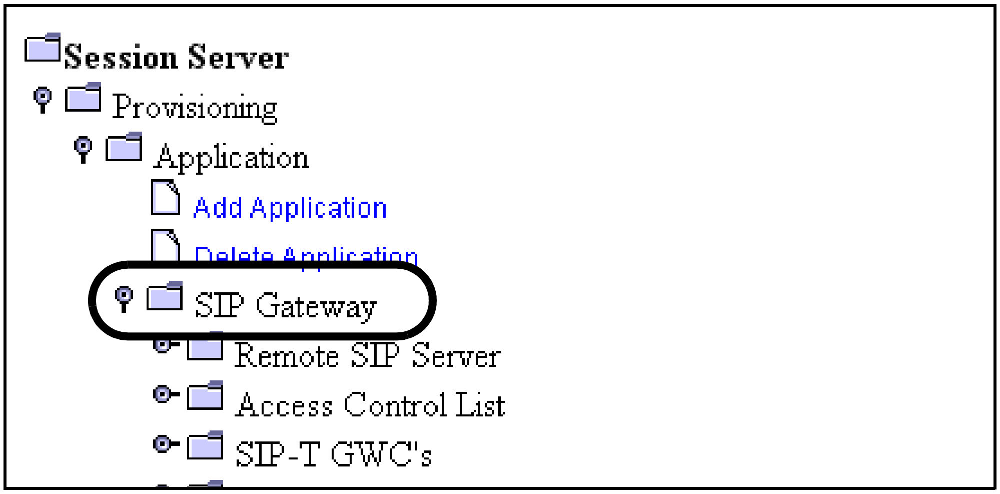
Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

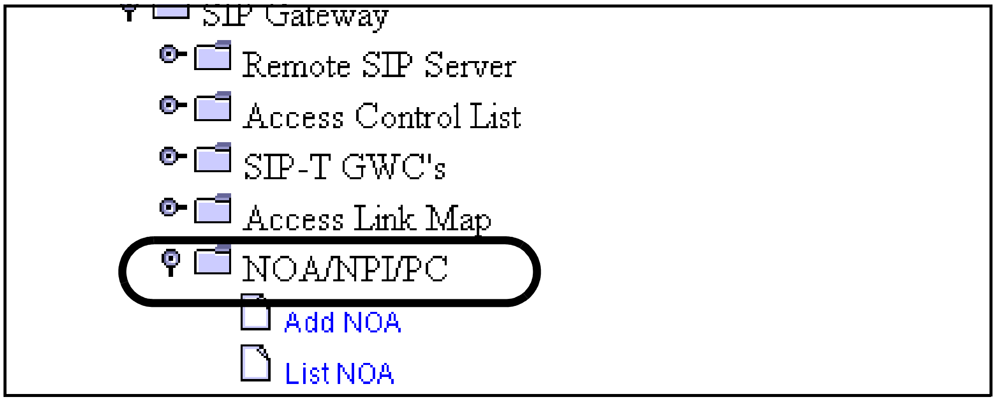
2 At the Session Server folder, click the **Provisioning folder,** then the **Application** folder.



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



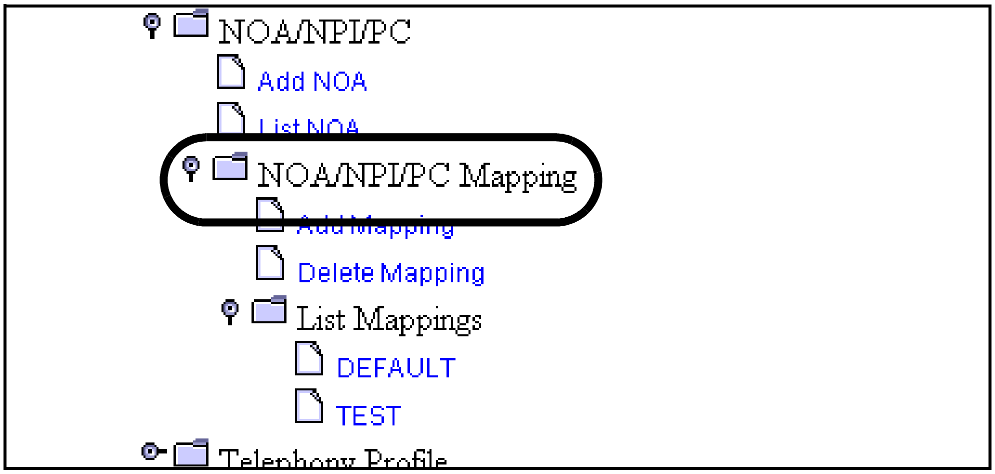
4 Click on the **NOA/NPI/PC** folder to open it.



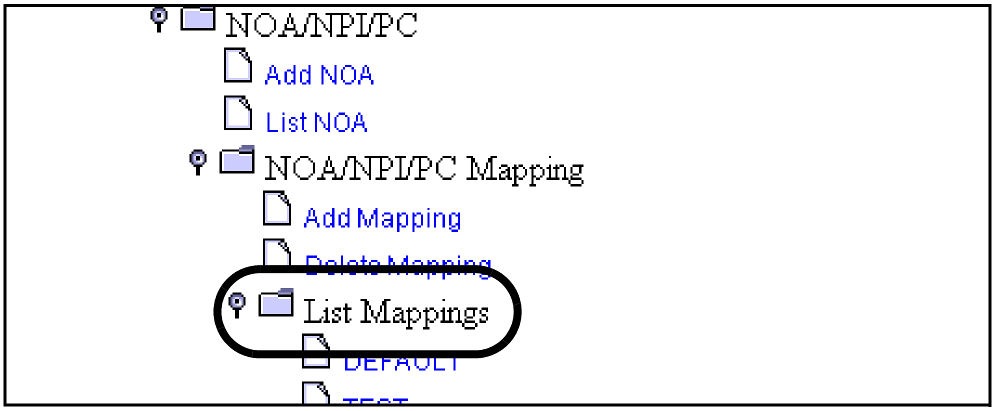
5 Use the following table to determine your next step:

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 9
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 25
you are done with this procedure	skip to step 29

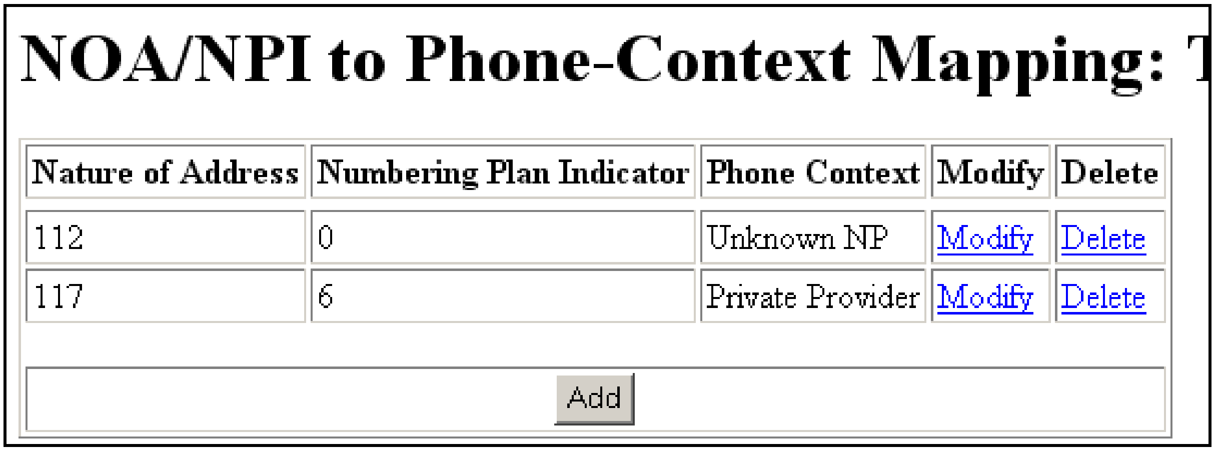
6 Click the **NOA/NPI/PC Mapping** link.



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

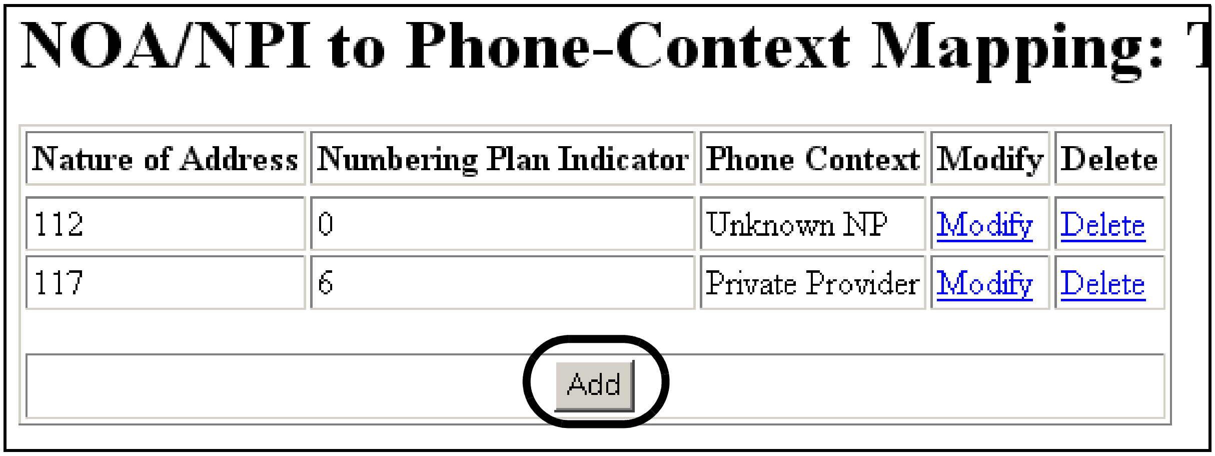
9 Use the following table to determine your next step:

If	Do
you are done reviewing this Phone Context map	skip to step 5
you want to add NOA-NPI tuples to the PC map	skip to 10a
you want to modify NOA-NPI tuples for this PC map	skip to 10d
you want to delete NOA-NPI tuples from this PC map	skip to 10g
you are done 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.

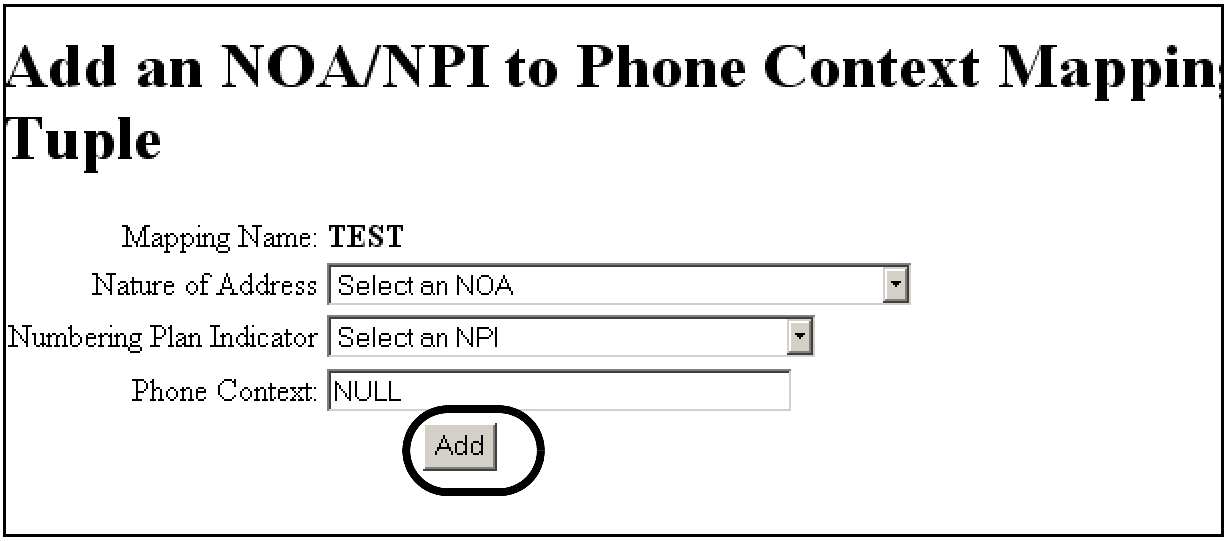
> ***Note:*** If this PC map is new, it may be empty of tuple content.



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

b Using Table of available NOAs (Nature of Addresses) and NPIs (Number Plan indicators) on page 84, 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 done making your selections, click the **Add** button.



Add an NOA/NPI to Phone Context Mappin Tuple

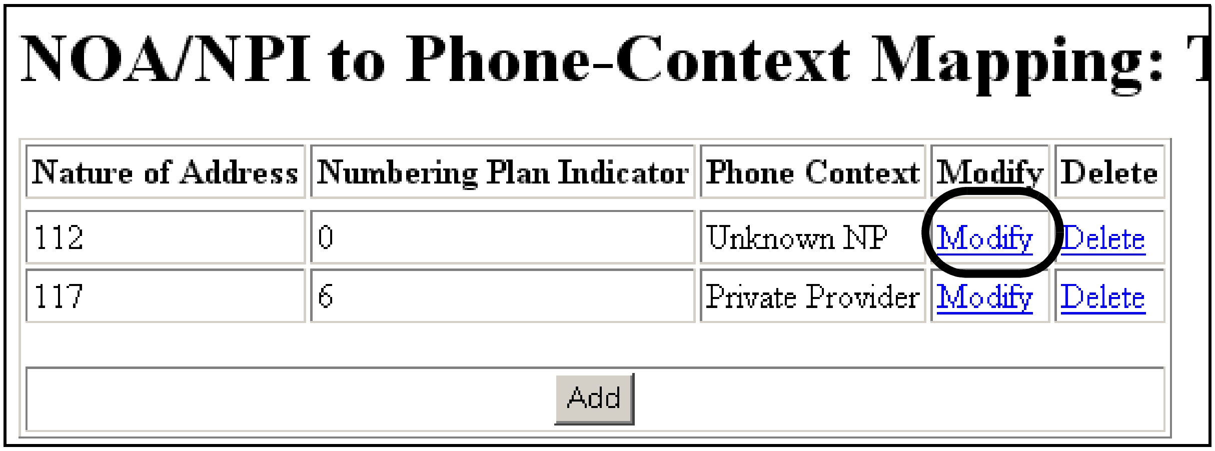
Mapping Name: **TEST**
Nature of Address: Select an NOA
Numbering Plan Indicator: Select an NPI
Phone Context: NULL

c Return to step a to add more tuples.

or

Return to step 9 when you are done 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.

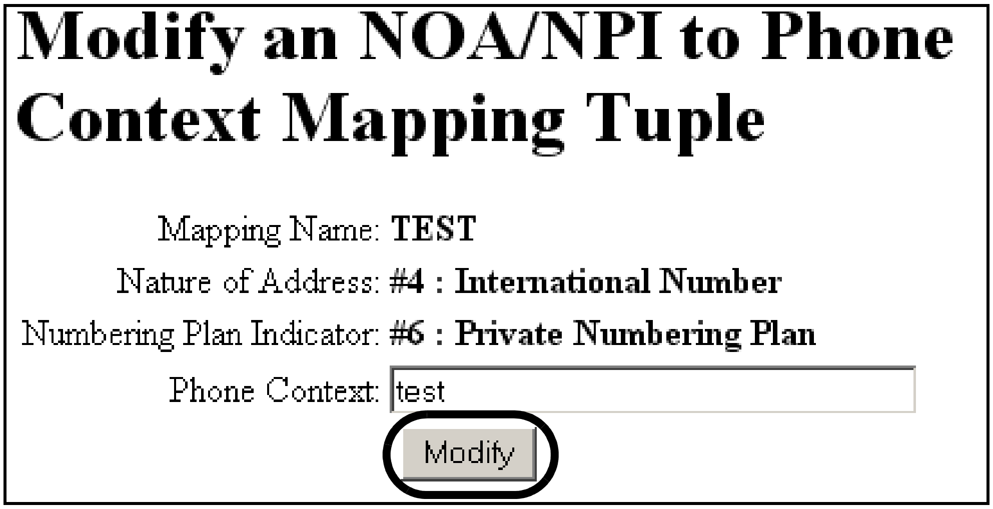


NOA/NPI to Phone-Context Mapping: T

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

e Use Table of available NOAs (Nature of Addresses) and NPIs (Number Plan indicators) on page 84 to assist you in modifying a NOA/NPI tuple, then click the **Modify** when you are done. For each mapping tuple, you can modify:

- the phone context name



Modify an NOA/NPI to Phone Context Mapping Tuple

Mapping Name: **TEST**

Nature of Address: **#4 : International Number**

Numbering Plan Indicator: **#6 : Private Numbering Plan**

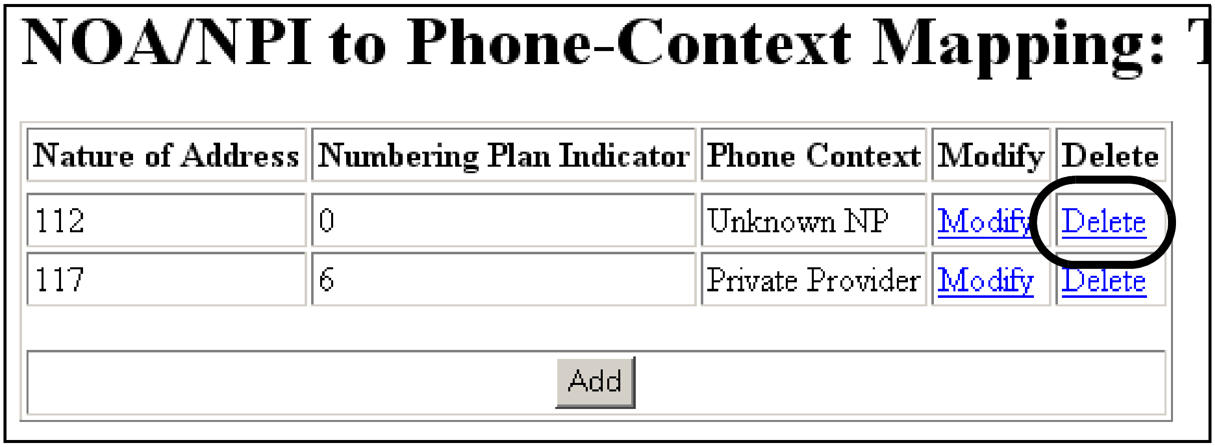
Phone Context: test

f Return to step d to modify more tuples.

or

Return to step 9 when you are done 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.



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

The system responds:

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

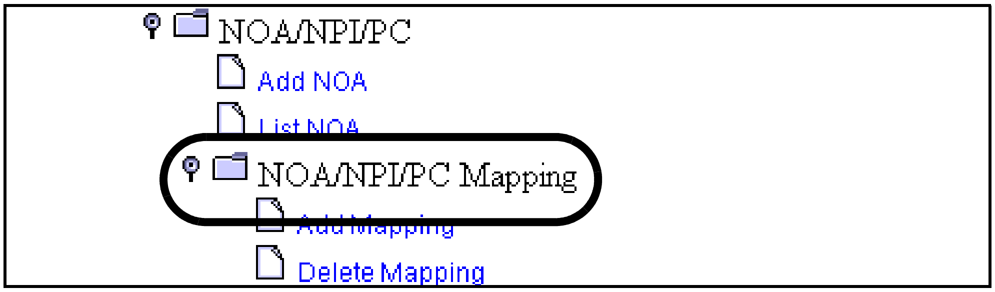
h Click **OK** to confirm the deletion.

i Return to step g to delete more tuples.

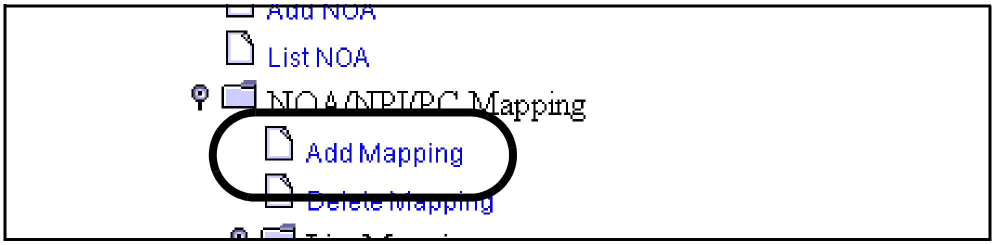
or

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

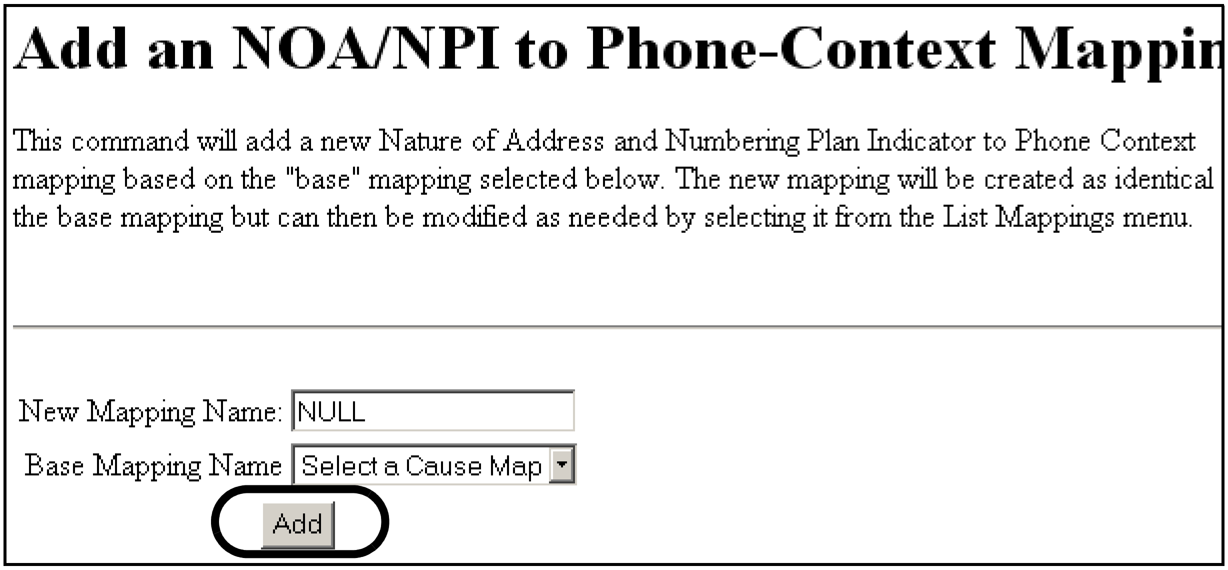
11 To create (add) a new Phone Context map, click the **NOA/NPI/PC Mapping** link.



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.



Add an NOA/NPI to Phone-Context Mappin

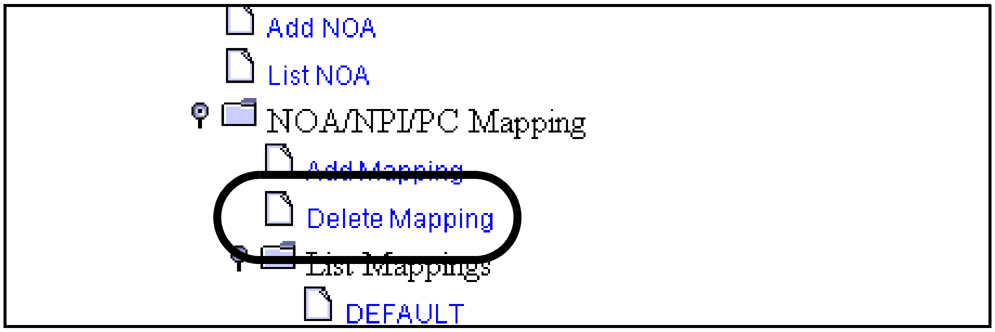
This command will add a new Nature of Address and Numbering Plan Indicator to Phone Context mapping based on the "base" mapping selected below. The new mapping will be created as identical the base mapping but can then be modified as needed by selecting it from the List Mappings menu.

New Mapping Name: NULL

Base Mapping Name: Select a Cause Map

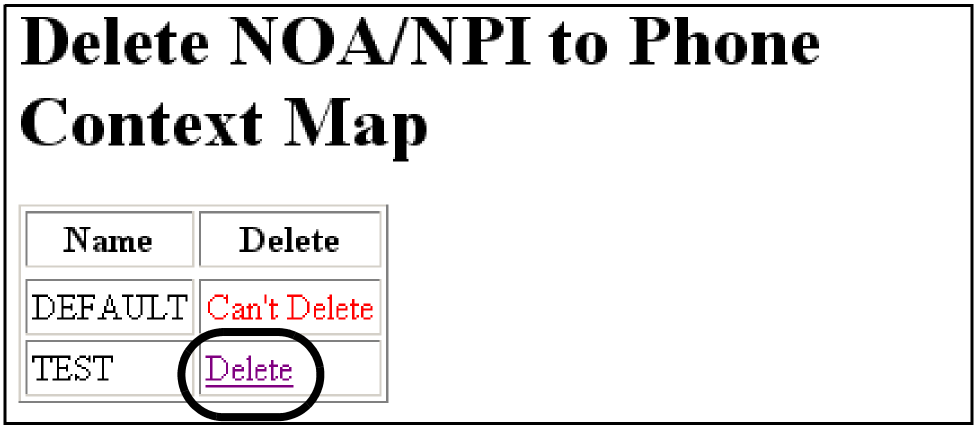
14 Return to step 5 when you are done adding a PC map.

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.

Note: You cannot delete the DEFAULT PC map.



Delete NOA/NPI to Phone Context Map

Name	Delete
DEFAULT	Can't Delete
TEST	Delete

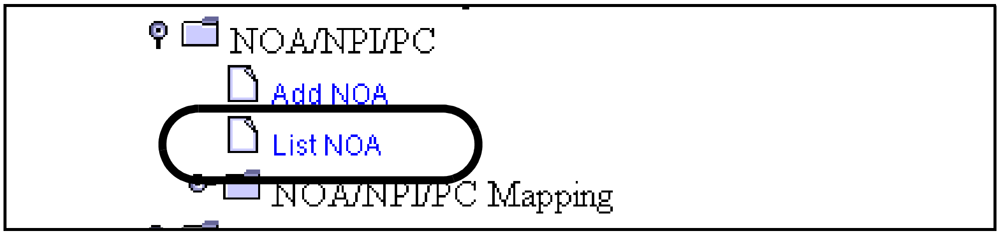
The system responses:

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

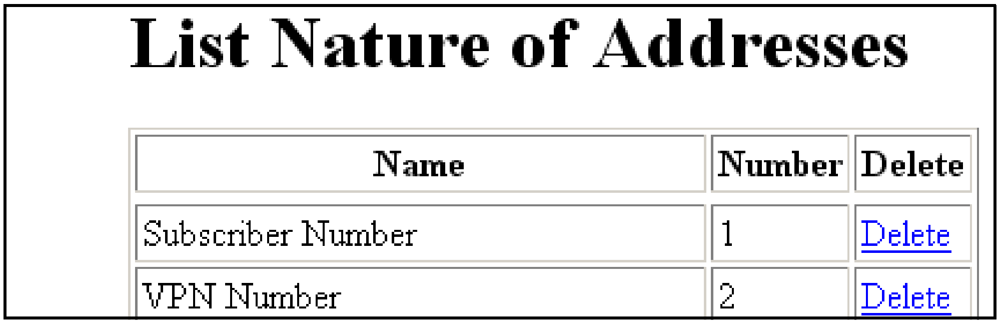
17 Click **OK** to confirm the deletion of the PC map.

18 Return to step 5 when you are done 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.



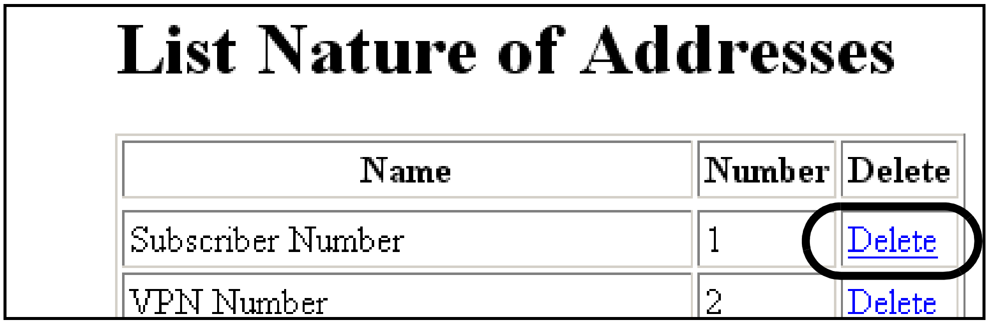
List Nature of Addresses

Name	Number	Delete
Subscriber Number	1	Delete
VPN Number	2	Delete

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.

> ***Note:*** 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.



List Nature of Addresses

Name	Number	Delete
Subscriber Number	1	Delete
VPN Number	2	Delete

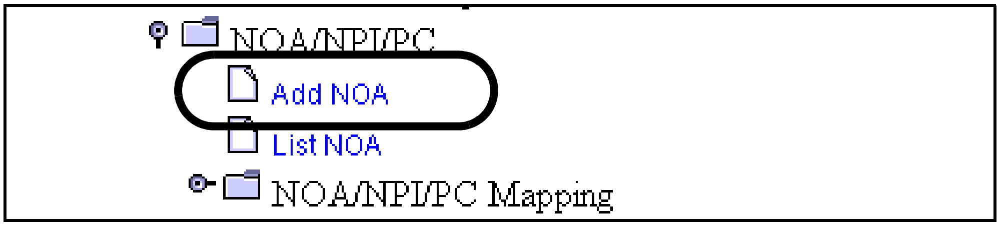
The system responses:

```
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 done deleting NOA entries.

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

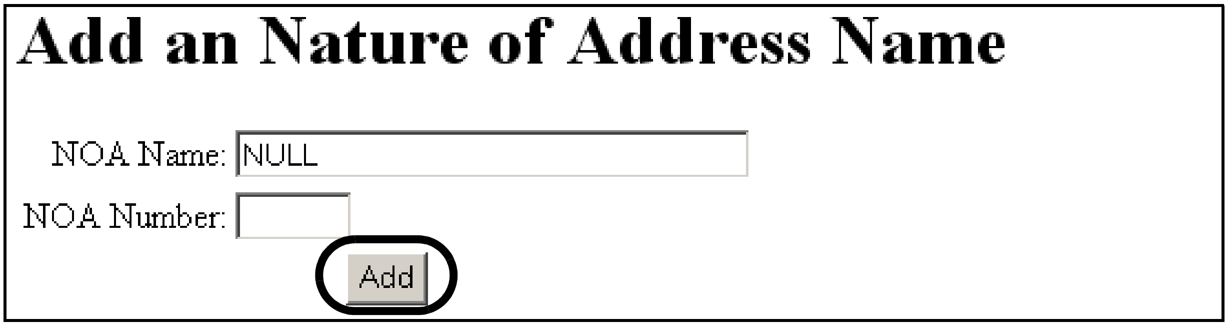


26 Type a new NOA entry name up to 32 alphanumeric characters, (spaces, hyphens and periods are also supported), assign an unused NOA number, then click the **Add** button.

Note 1: NOA names are added in the case entered.

Note 2: Assigned NOA entries should be unique across all interconnected systems. Acceptable NOA numbers range from 1 to 150.

Note 3: It is not recommended that the same NOA name be used for multiple NOA numbers.



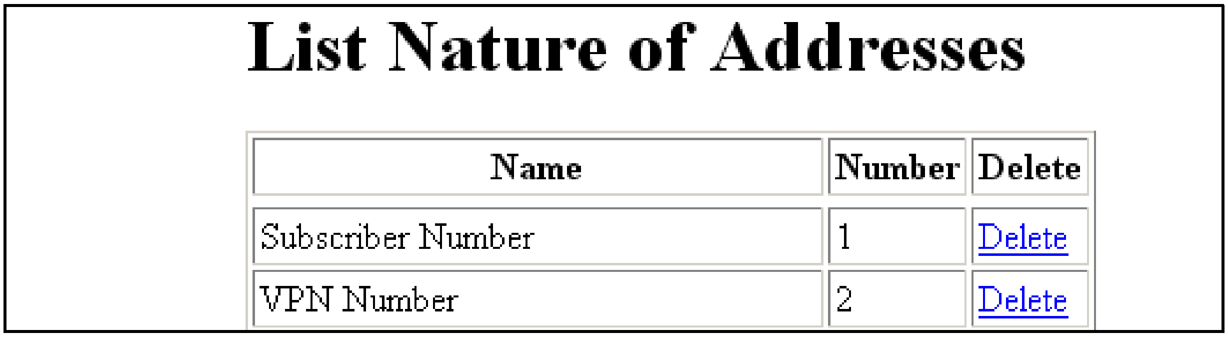
Add an Nature of Address Name

NOA Name: NULL

NOA Number:

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

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 done adding new mappings.

29 The procedure is complete.

Table of available NOAs (Nature of Addresses) and NPIs (Number Plan indicators)

The Nature of Address 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. 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
APN Number	120
International Inbound Operator Call	122

The Numbering Plan Indicator (NPI) identifies a numbering scheme for users of telecommunications services in different telecommunication networks. The Session Server 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

Add/Manage 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. These are listed in Table of available default SIP base protocol tuples on page 90.

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.

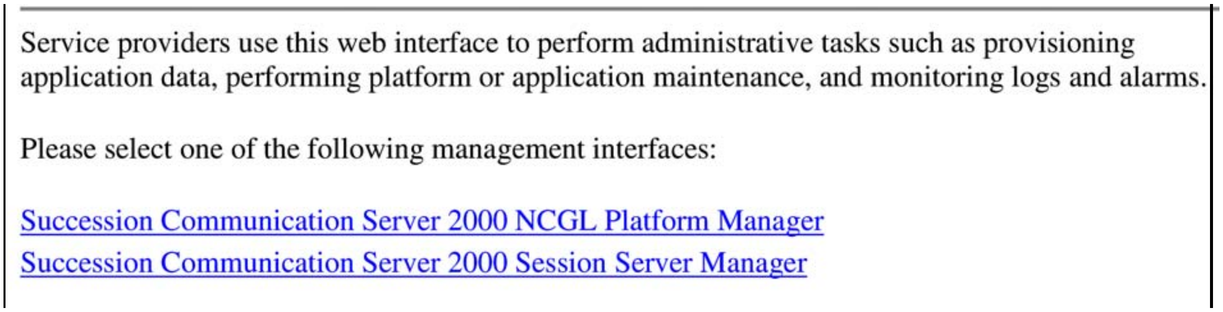
Prerequisites

There are no prerequisites for performing this procedure.

Action

At the CS 2000 Session Server Launch Point

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

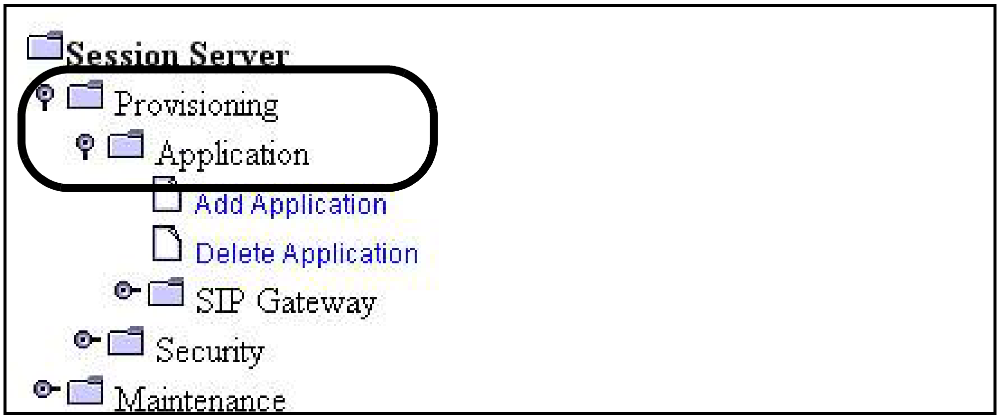


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

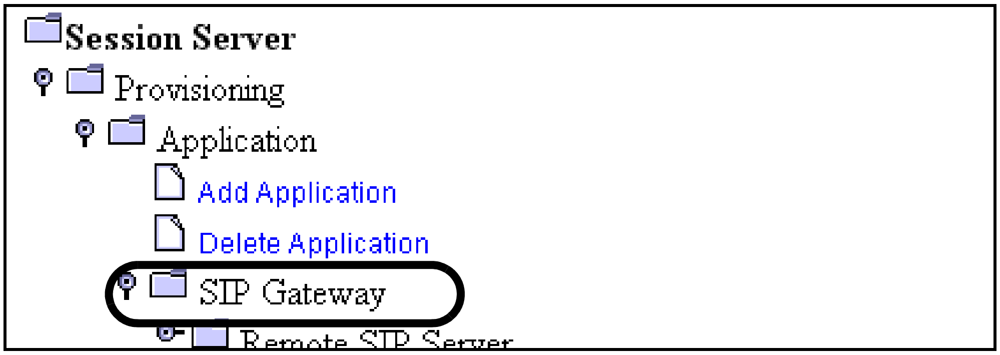
Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

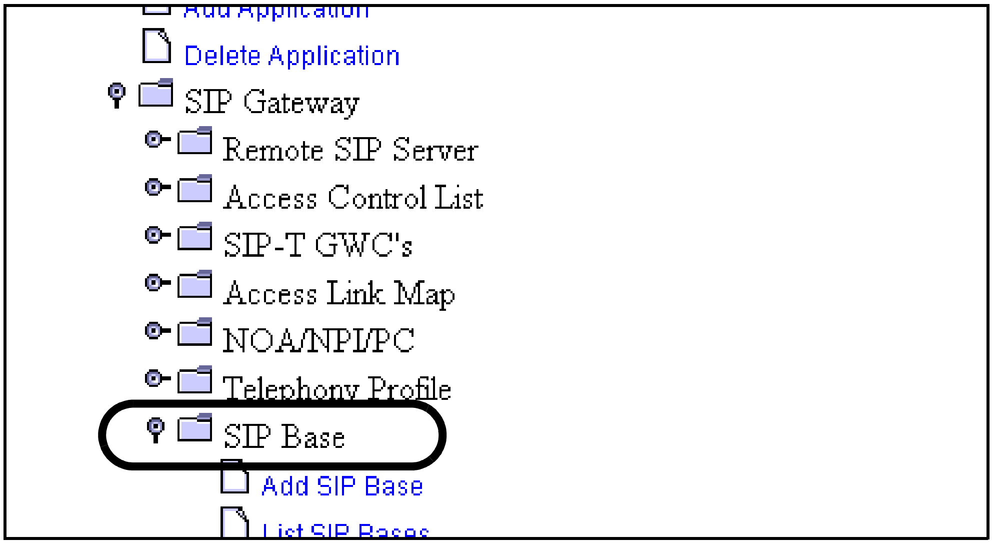
2 At the Session Server folder, click the **Provisioning folder,** then the **Application** folder.



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



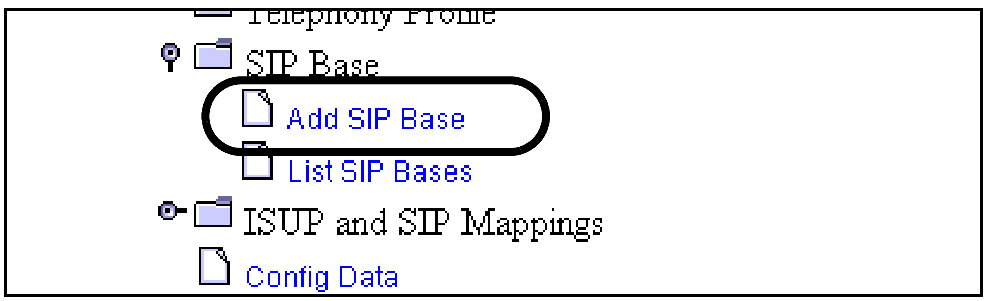
4 Click on the **SIP Base** folder to open it.



5 Use the following table to determine your next step:

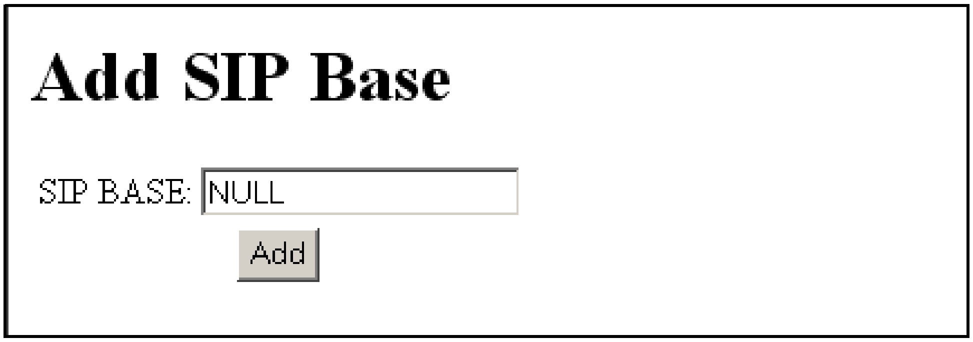
If	Do
you are adding a SIP base tuple to the SIP Gateway application database	step 6
you want to list existing SIP base tuples currently in the database	step 9
you are deleting a SIP base tuple from the SIP Gateway application database	step 9
you are done with this procedure	step 13

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.

Note: All alpha characters entered are converted to upper case.


Add SIP Base

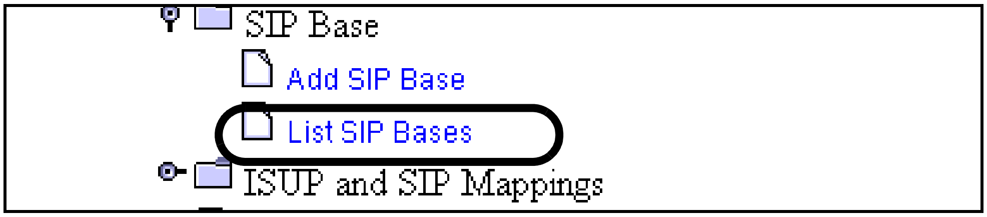
SIP BASE: NULL

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 6
you want to list or delete other user defined SIP base tuples	skip to step 9
you are done with this procedure	skip to step 13

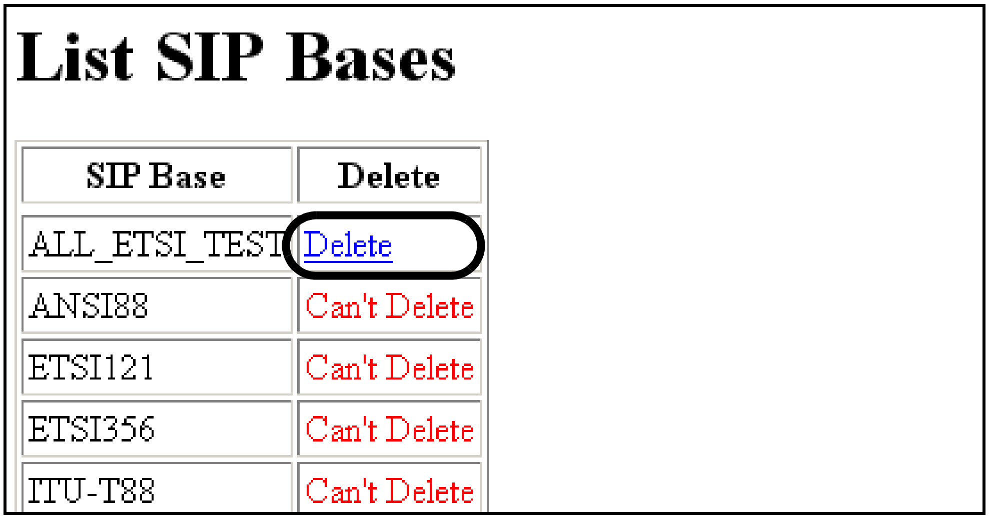
9 Click on the **List SIP Bases** page to open it.



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 skip to step 12.

> ***Note:*** 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.



List SIP Bases

SIP Base	Delete
ALL_ETSI_TEST	Delete
ANSI88	Can't Delete
ETSI121	Can't Delete
ETSI356	Can't Delete
ITU-T88	Can't Delete

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 continue with step 13.

13 The procedure is complete.

Table of available default SIP base protocol tuples

Protocol	Purpose
ANSI88	ISUP (ISDN User Part) variant
ANSI_UCP	ISUP variant
ITU-T88	ISUP variant
ITU-T92-PLUS	ISUP variant
ETSI121	ISUP variant
ETSI356	ISUP variant
TTC93-PLUS	ISUP variant

Add/Manage 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 Configure Remote SIP Servers on page 21. 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.

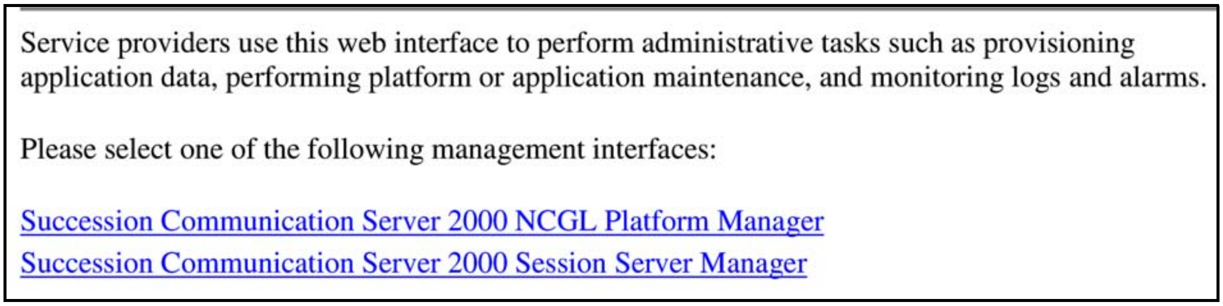
Prerequisites

There are no prerequisites for performing this procedure.

Action

At the CS 2000 Session Server Launch Point

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

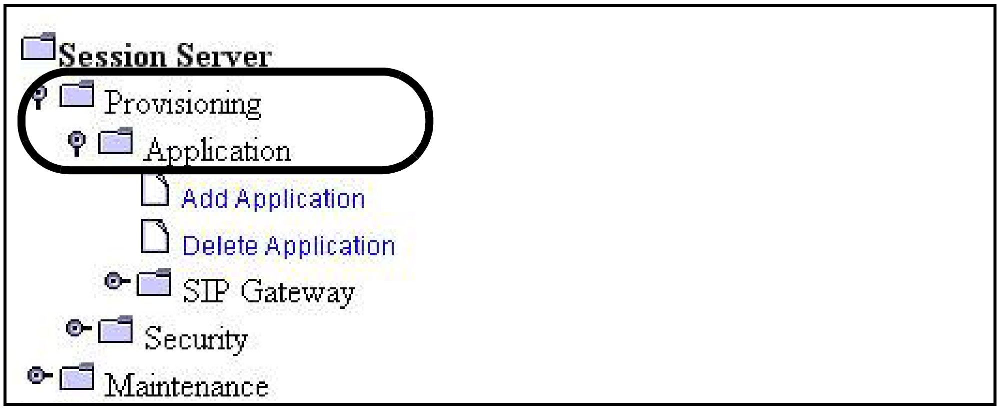


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

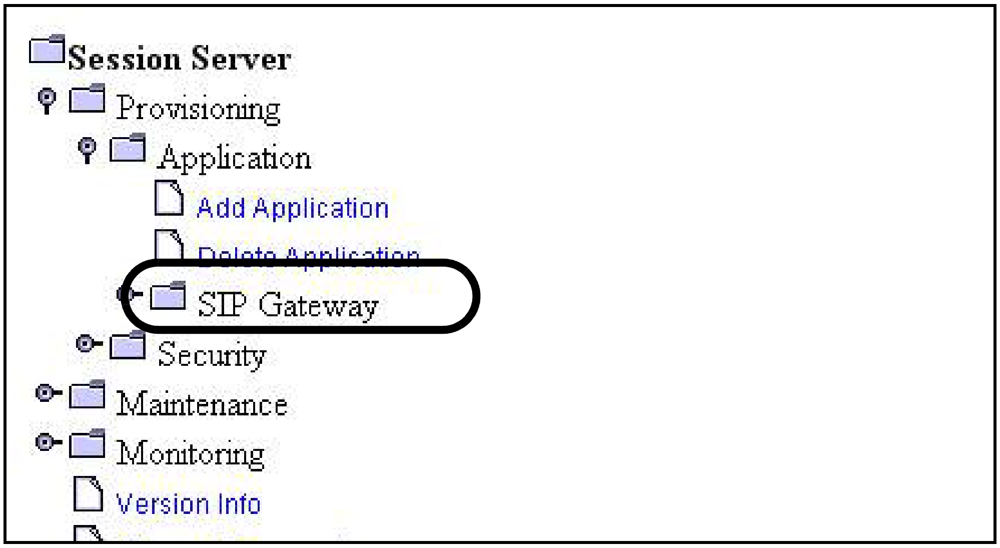
Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

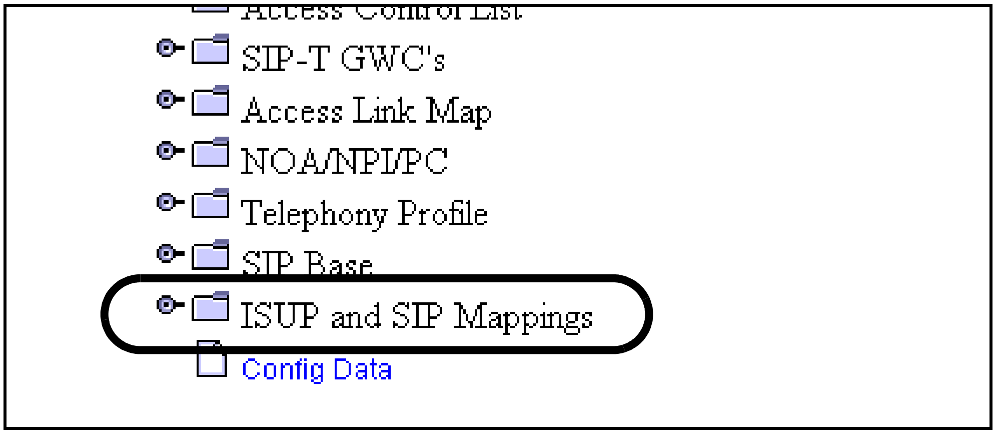
2 At the Session Server folder, click the **Provisioning folder,** then the **Application** folder.



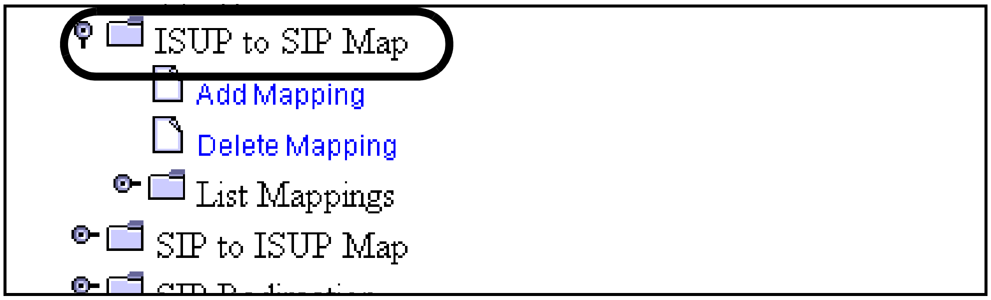
3 Click on the **SIP Gateway** folder to open the folder.



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



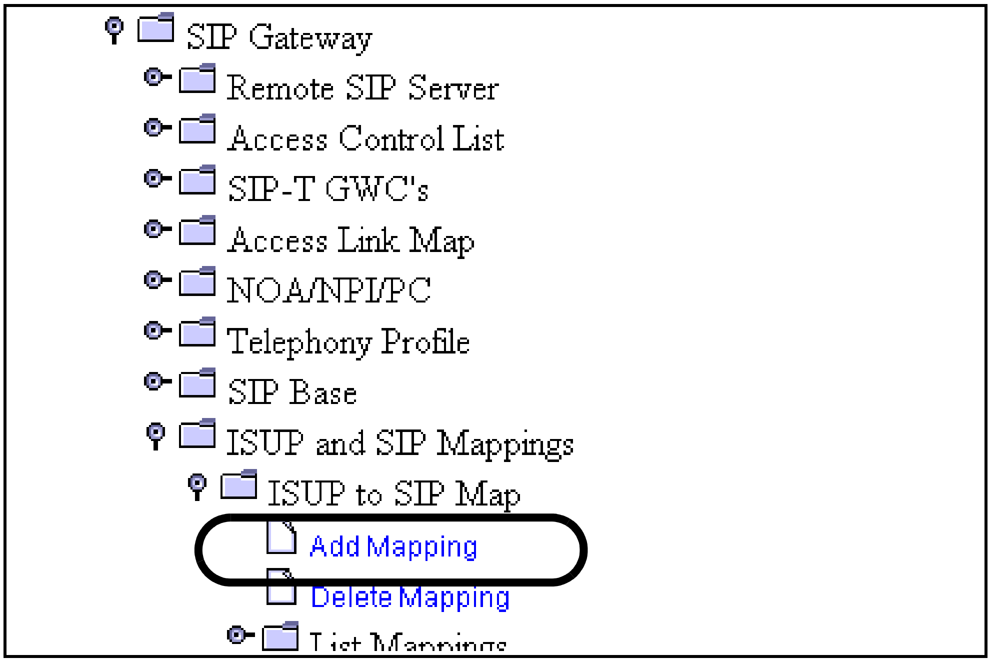
5 Click on the **ISUP to SIP Map** link to open it.



6 Use the following table to determine your next step:

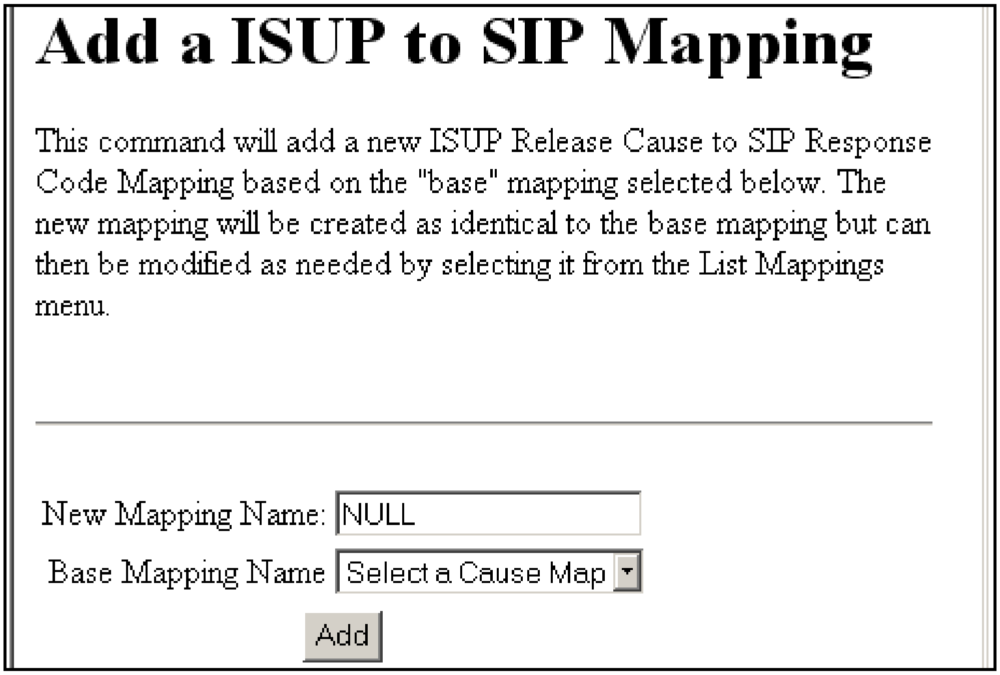
If	Do
you are adding an ISUP to SIP Map to the SIP Gateway application database	step 7
you want to list or modify an existing ISUP to SIP Map currently in the database	step 12
you are deleting an ISUP to SIP Map from the SIP Gateway application database	step 18
you are done with this procedure	step 22

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).

> ***Note:*** All alpha characters entered are converted to upper case.



Add a ISUP to SIP Mapping

This command will add a new ISUP Release Cause to SIP Response Code Mapping based on the "base" mapping selected below. The new mapping will be created as identical to the base mapping but can then be modified as needed by selecting it from the List Mappings menu.

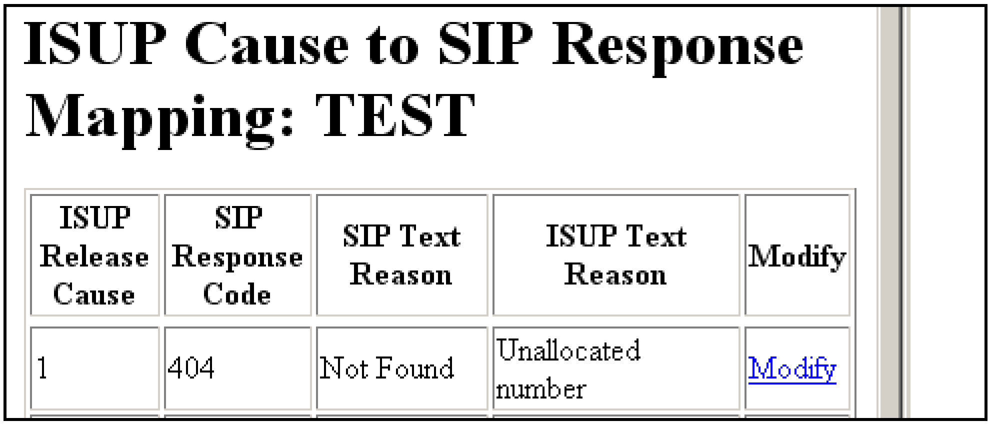
New Mapping Name: NULL

Base Mapping Name: Select a Cause Map

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.

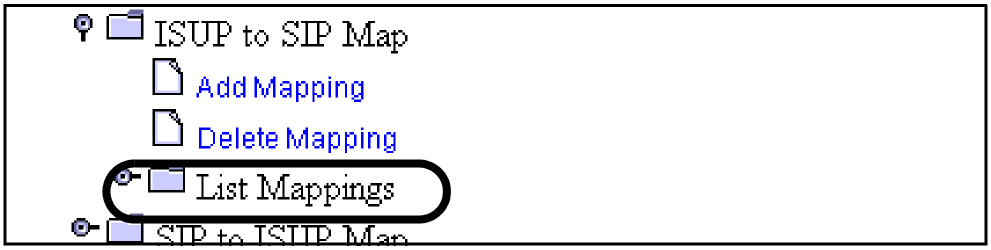


ISUP Cause to SIP Response Mapping: TEST

ISUP Release Cause	SIP Response Code	SIP Text Reason	ISUP Text Reason	Modify
1	404	Not Found	Unallocated number	Modify

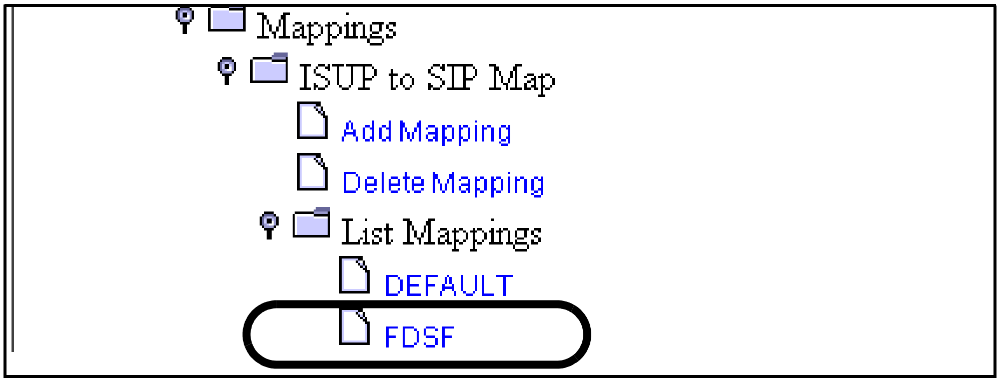
11 If you want to add another ISUP to SIP Map, return to step 7 otherwise return to step 6

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



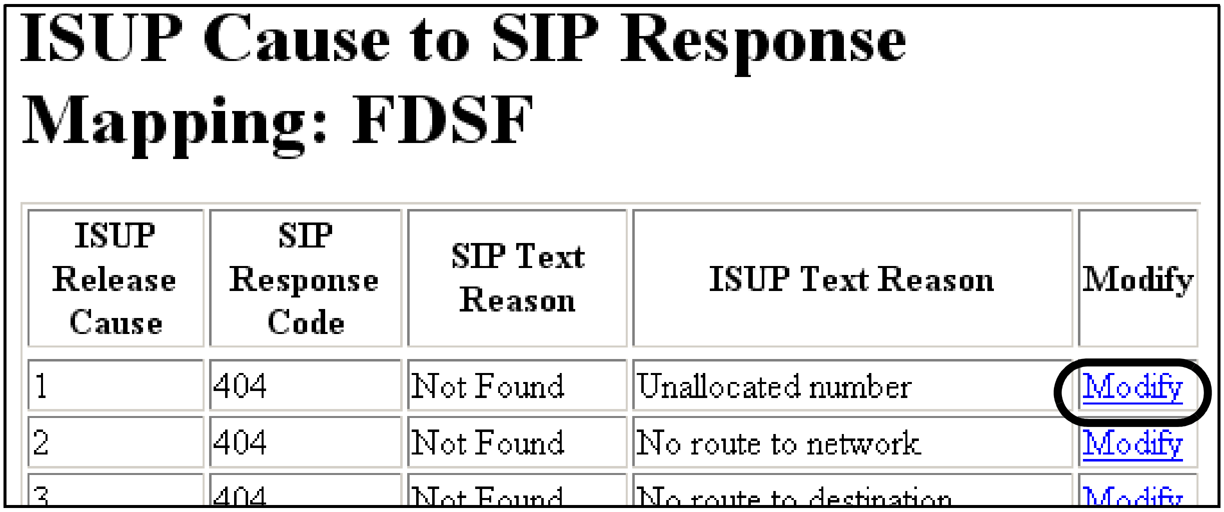
A list of existing maps is displayed, including the DEFAULT map.

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.



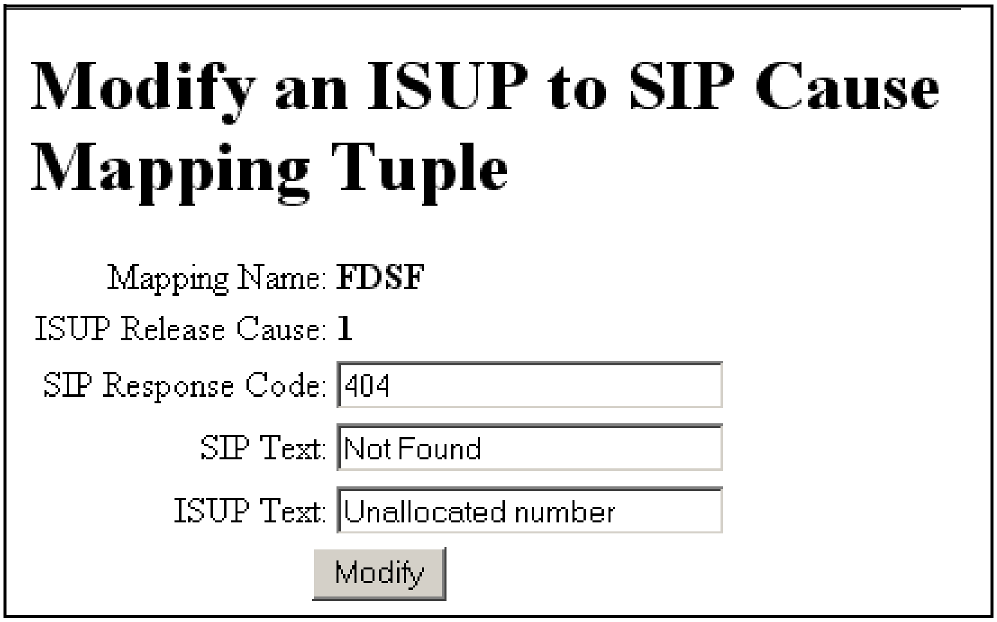
ISUP Cause to SIP Response Mapping: FDSF

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

Note: You cannot change the ISUP release Cause number.



Modify an ISUP to SIP Cause Mapping Tuple

Mapping Name: **FDSF**

ISUP Release Cause: **1**

SIP Response Code: 404

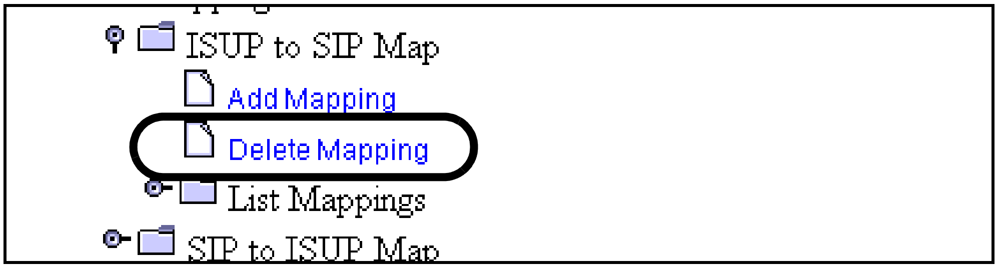
SIP Text: Not Found

ISUP Text: Unallocated number

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

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

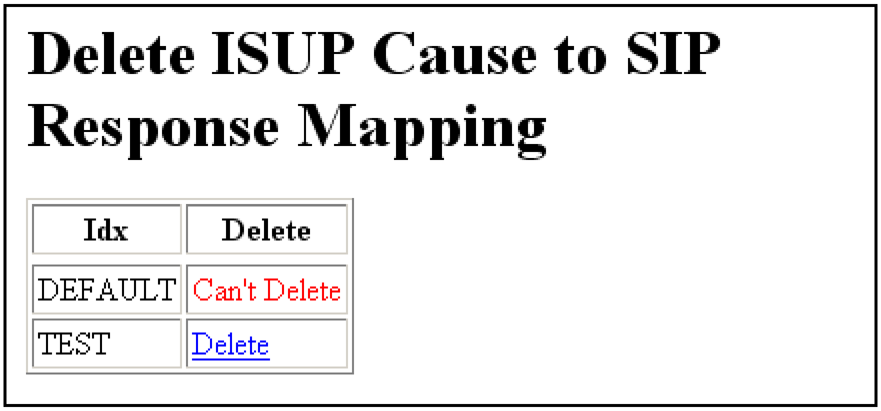
18 If you want to delete a map, click the **Delete Mapping** link, otherwise return to step 6.



A list of current maps is displayed

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

Note: 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.



Delete ISUP Cause to SIP Response Mapping

Idx	Delete
DEFAULT	Can't Delete
TEST	Delete

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 continue with step 22.

22 The procedure is complete.

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	Misdialled 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
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

ISUP Release Cause	SIP Response Code	SIP Text Reason Phrase	ISUP Text Reason Phrase
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

ISUP Release Cause	SIP Response Code	SIP Text Reason Phrase	ISUP Text Reason Phrase
54	503	Service Unavailable	Service Unavailable
55	403	Forbidden	Incoming calls barred within CUG
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

ISUP Release Cause	SIP Response Code	SIP Text Reason Phrase	ISUP Text Reason Phrase
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
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

Add/Manage 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 Configure Remote SIP Servers on page 21. 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.

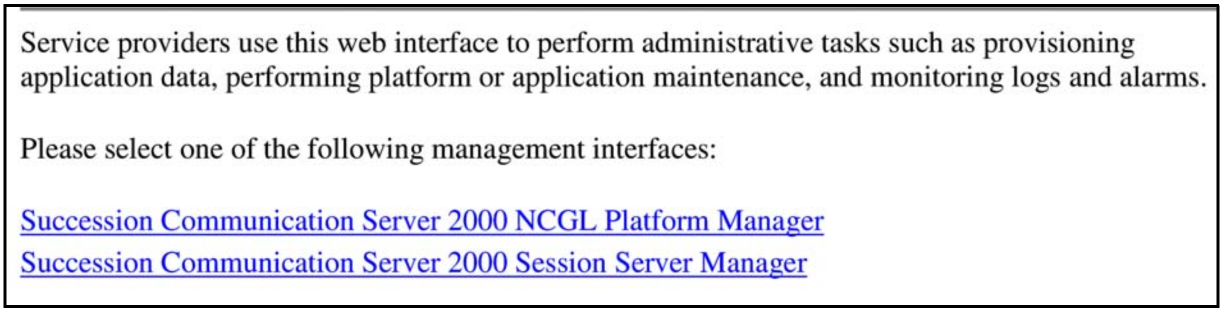
Prerequisites

There are no prerequisites for performing this procedure.

Action

At the CS 2000 Session Server Launch Point

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

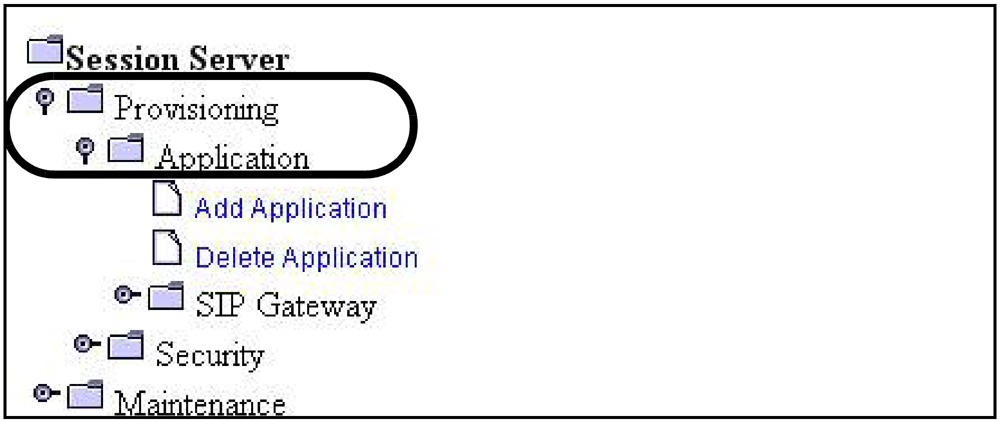


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

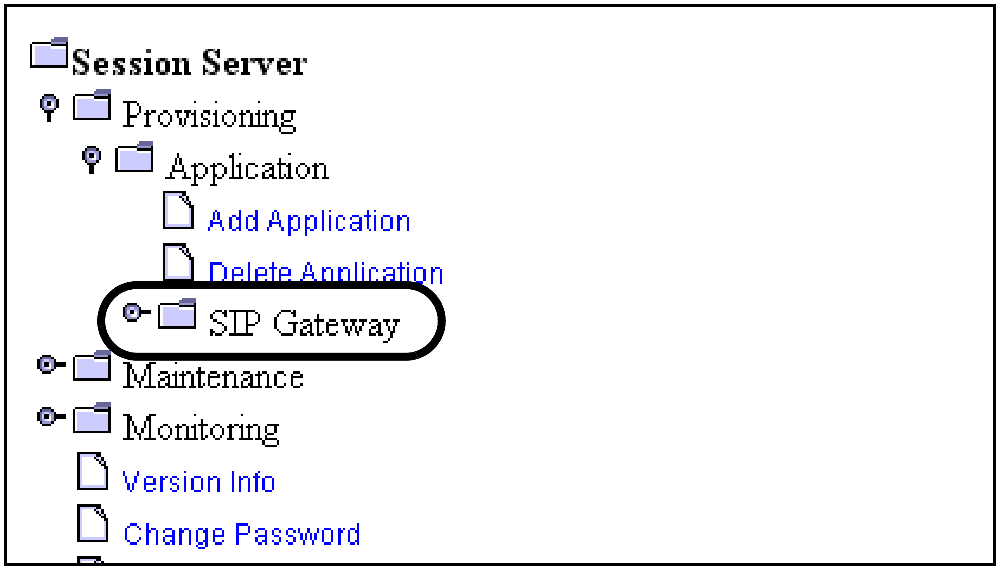
Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

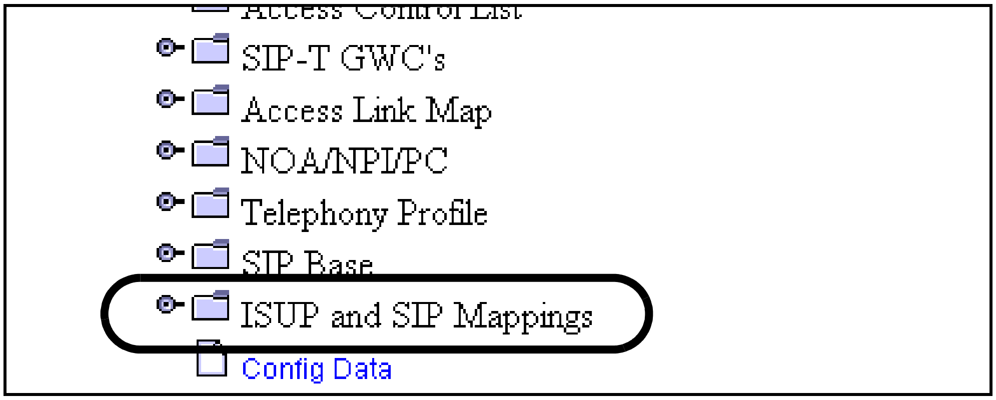
2 At the Session Server folder, click the **Provisioning folder,** then the **Application** folder.



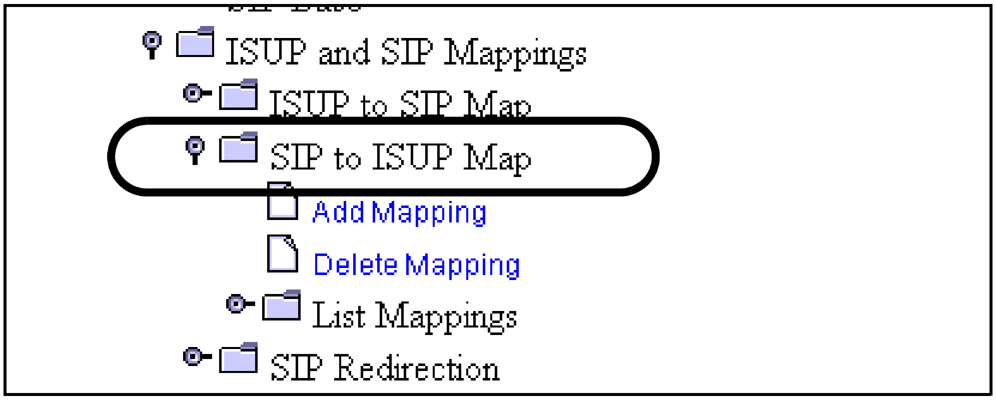
3 Click on the **SIP Gateway** folder to open the folder.



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



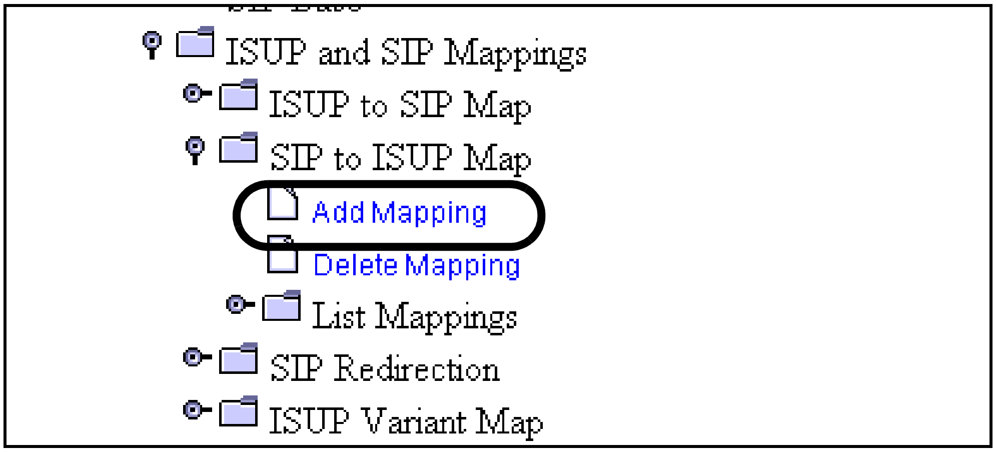
5 Click on the **SIP to ISUP Map** link to open it.



6 Use the following table to determine your next step:

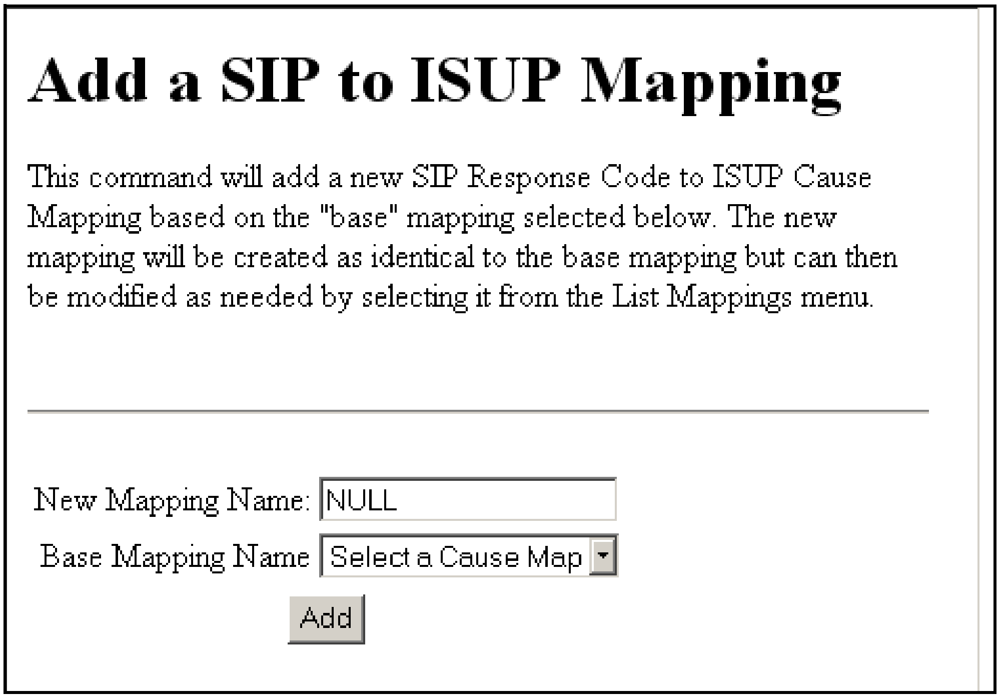
If	Do
you are adding a SIP to ISUP Map to the SIP Gateway application database	step 7
you want to list or modify an existing SIP to ISUP Map currently in the database	skip to step 12
you are deleting an SIP to ISUP Map from the SIP Gateway application database	skip to step 18
you are done with this procedure	skip to step 22

7 Click the **Add Mapping** link.



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

> ***Note:*** All alpha characters entered are converted to upper case.



Add a SIP to ISUP Mapping

This command will add a new SIP Response Code to ISUP Cause Mapping based on the "base" mapping selected below. The new mapping will be created as identical to the base mapping but can then be modified as needed by selecting it from the List Mappings menu.

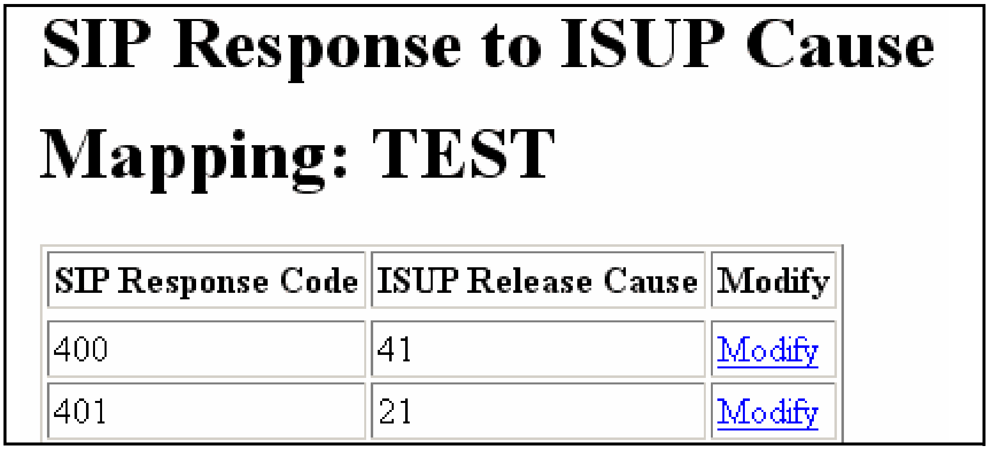
New Mapping Name: NULL

Base Mapping Name Select a Cause Map

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.



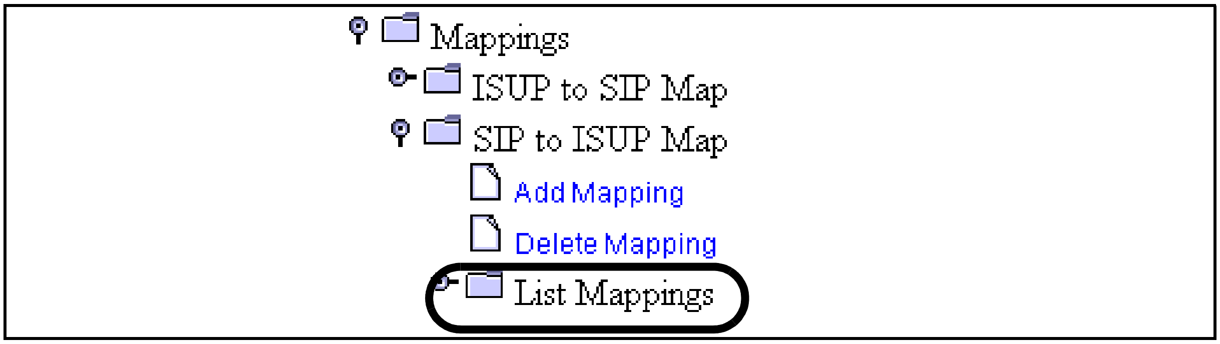
SIP Response to ISUP Cause Mapping: TEST

SIP Response Code	ISUP Release Cause	Modify
400	41	Modify
401	21	Modify

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

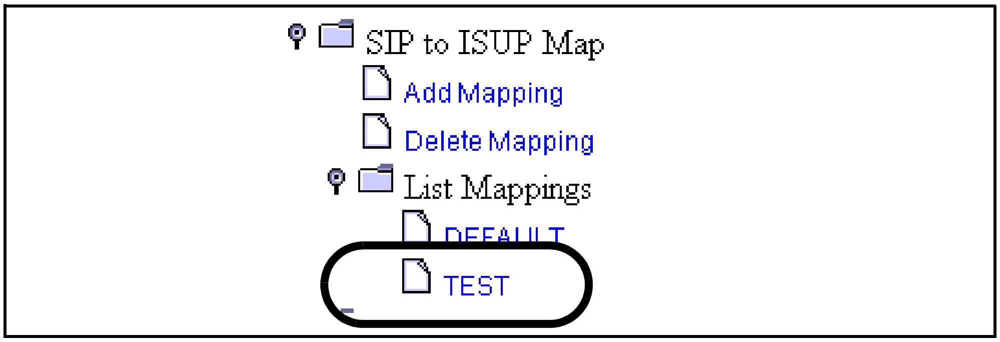
12 Click on the **List Mappings** folder to open it.

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

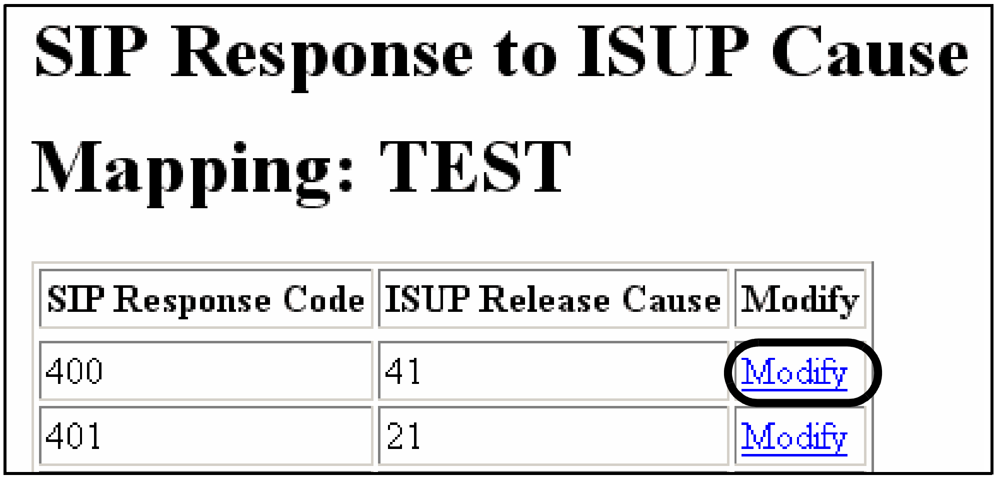


13 Click on the map name you want to review.

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.

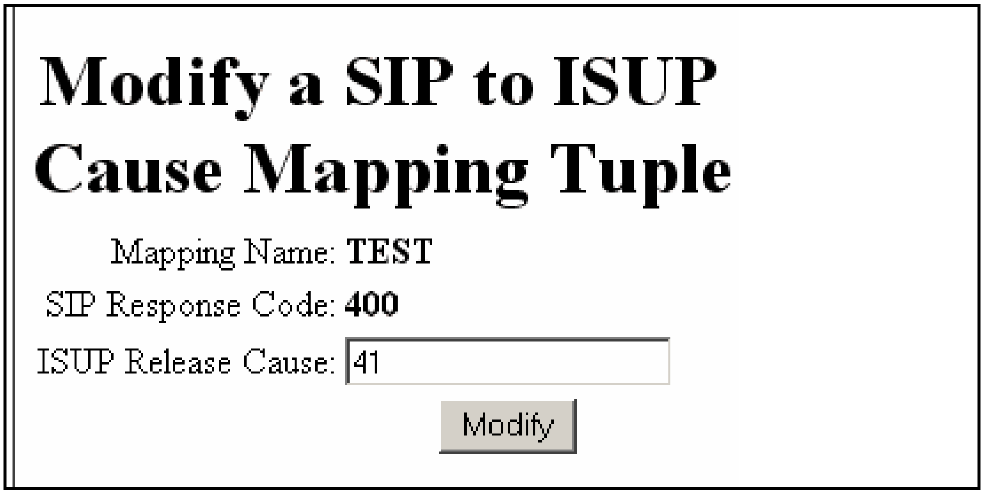


SIP Response to ISUP Cause Mapping: TEST

SIP Response Code	ISUP Release Cause	Modify
400	41	Modify
401	21	Modify

15 For each cause tuple, you can modify:

- the ISUP release Cause number



Modify a SIP to ISUP Cause Mapping Tuple

Mapping Name: **TEST**

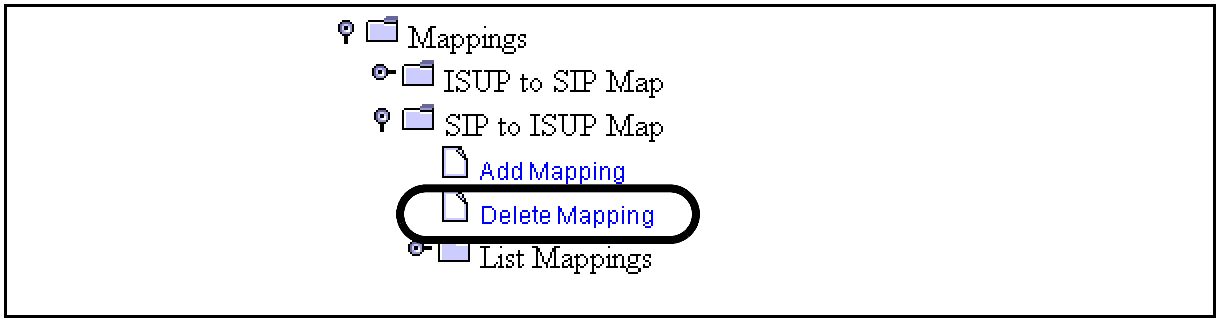
SIP Response Code: **400**

ISUP Release Cause: 41

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

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

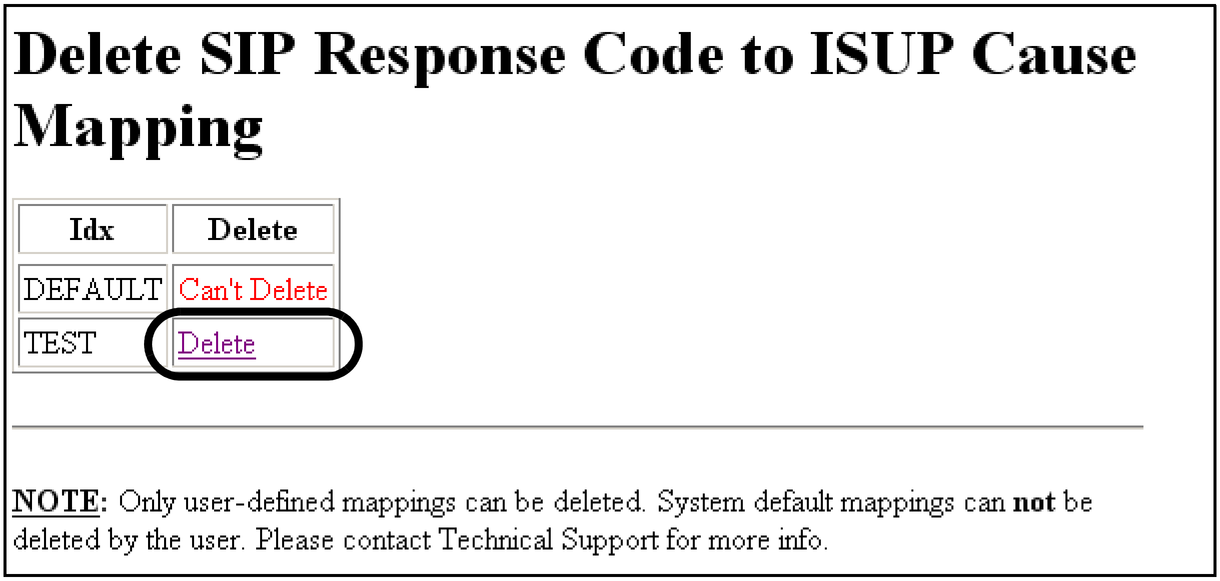
18 If you want to delete a map, click the **Delete Mapping** link. Otherwise skip to step 6.



A list of current maps is displayed

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

> ***Note:*** 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.



Delete SIP Response Code to ISUP Cause Mapping

Idx	Delete
DEFAULT	Can't Delete
TEST	Delete

NOTE: Only user-defined mappings can be deleted. System default mappings can **not** be deleted by the user. Please contact Technical Support for more info.

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 continue with step 22.

22 The procedure is complete.

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
416	127		600	17
420	127		603	21
421	127		604	1
423	127			

Add/Manage 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.

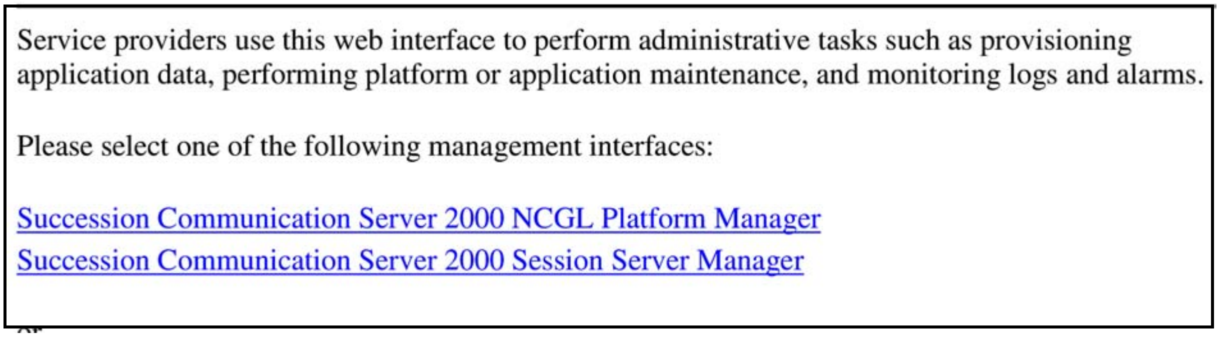
Prerequisites

There are no prerequisites for performing this procedure.

Action

At the CS 2000 Session Server Launch Point

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

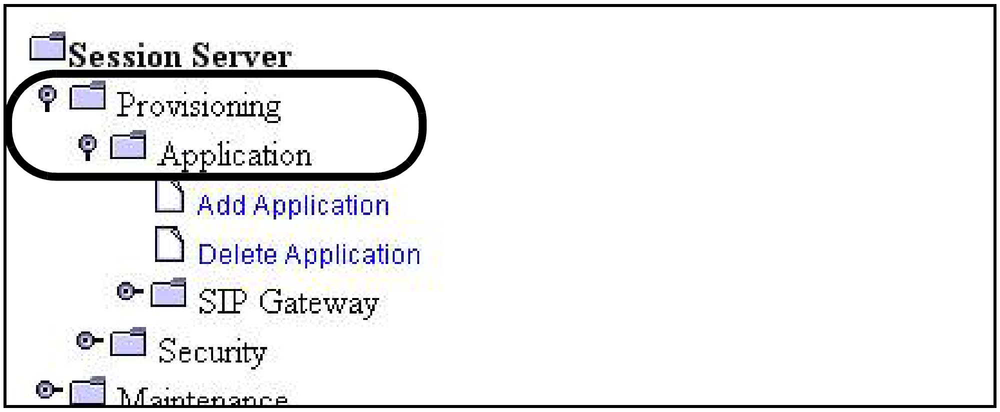


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

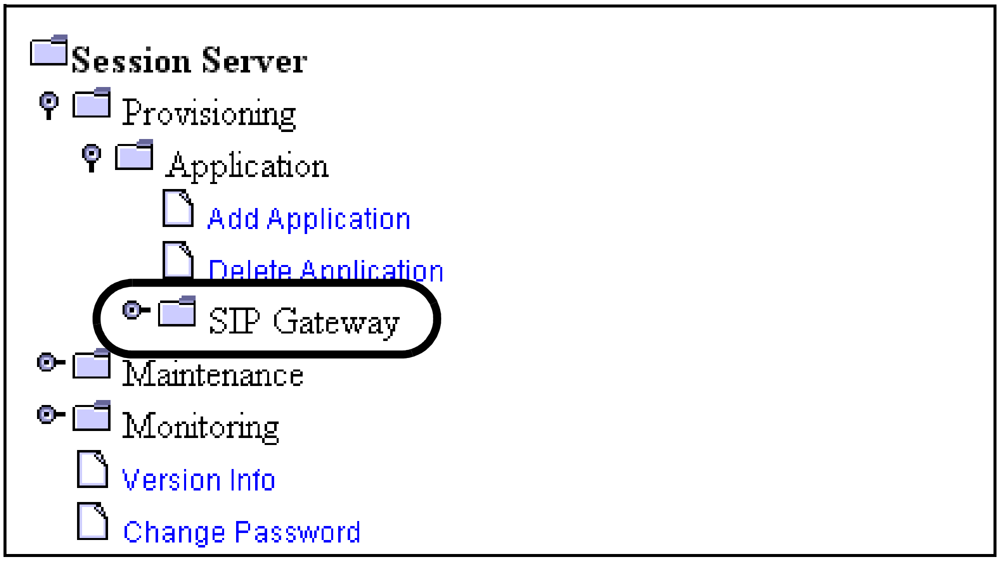
Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

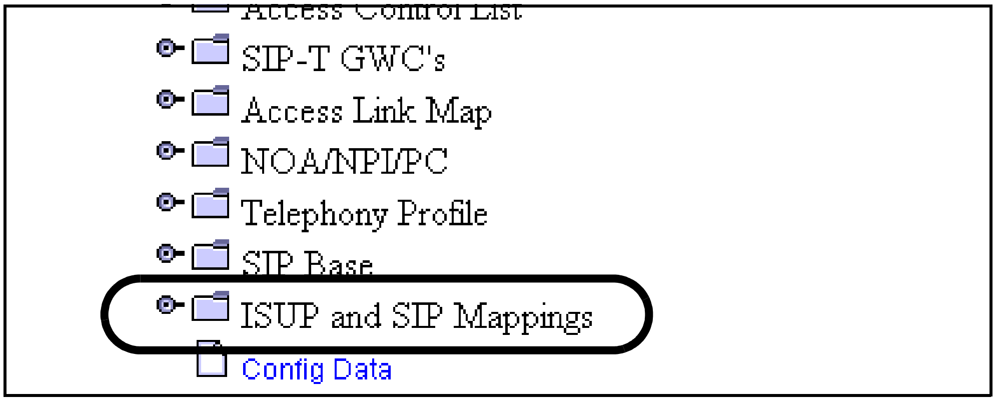
2 At the Session Server folder, click the **Provisioning folder,** then the **Application** folder.



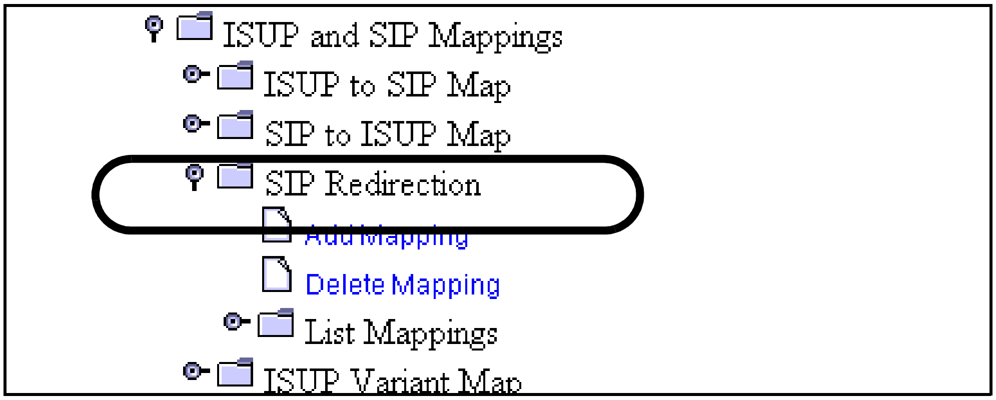
3 Click on the **SIP Gateway** folder to open the folder.



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



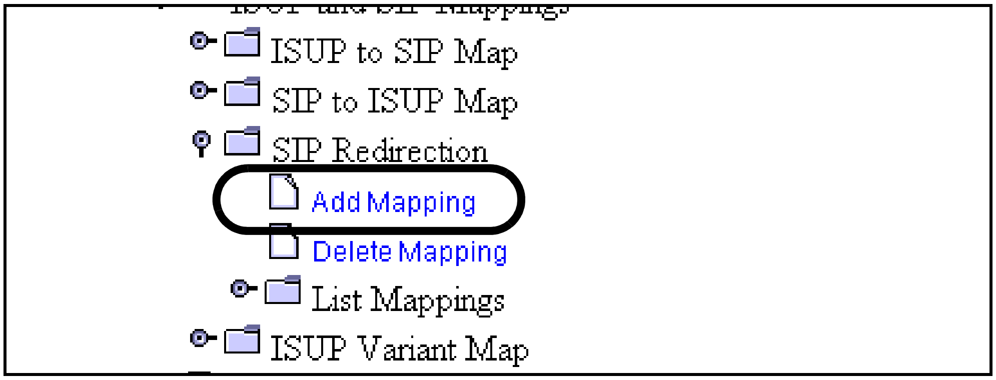
5 Click on the **SIP Redirection** link to open it.



6 Use the following table to determine your next step:

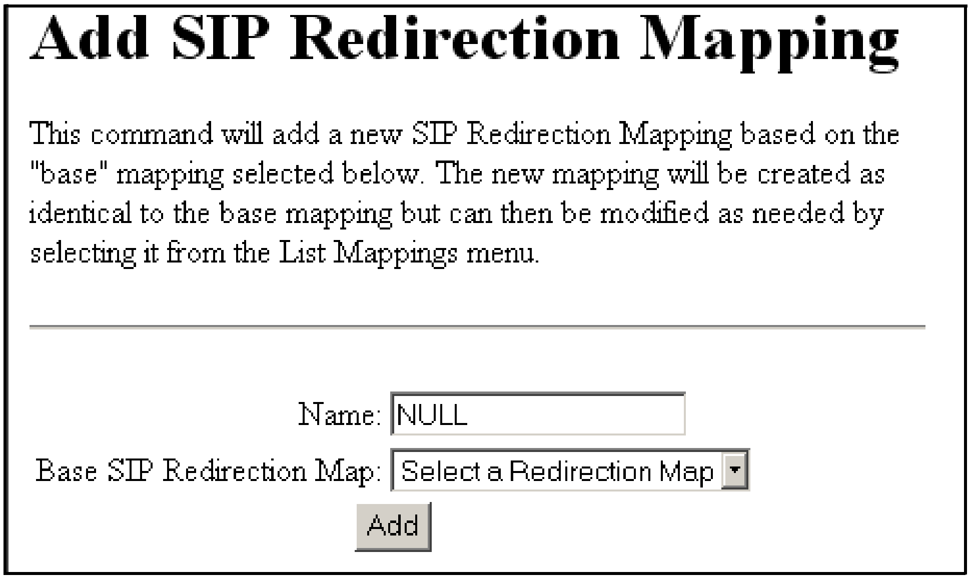
If	Do
you are adding a SIP Redirection Map to the SIP Gateway application database	continue with step 7
you want to list or modify an existing SIP Redirection Maps currently in the database	skip to step 12
you are deleting a SIP Redirection Map from the SIP Gateway application database	skip to step 12
you are done with this procedure	skip to step 22

7 Click the **Add Mapping** link.



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

Note: All alpha characters entered are converted to upper case.



Add SIP Redirection Mapping

This command will add a new SIP Redirection Mapping based on the "base" mapping selected below. The new mapping will be created as identical to the base mapping but can then be modified as needed by selecting it from the List Mappings menu.

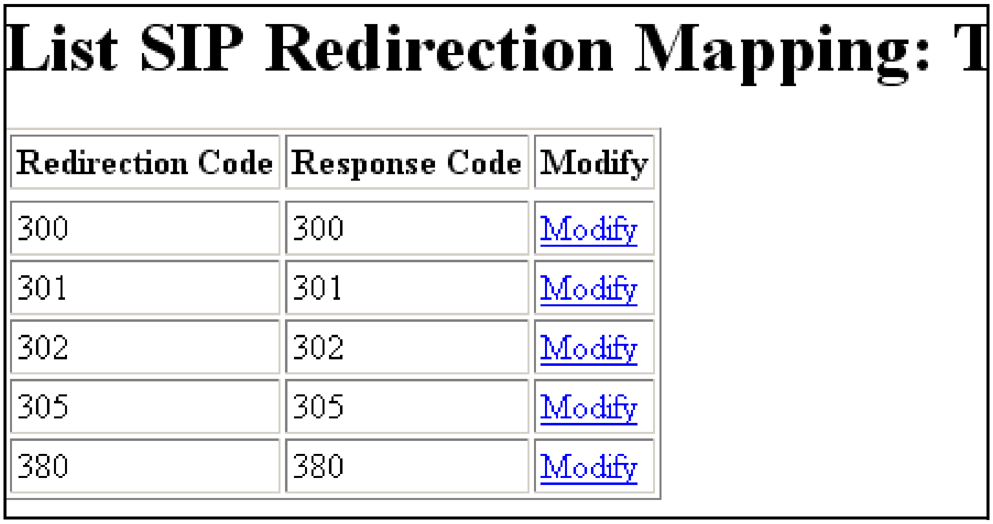
Name: NULL

Base SIP Redirection Map: Select a Redirection Map

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.



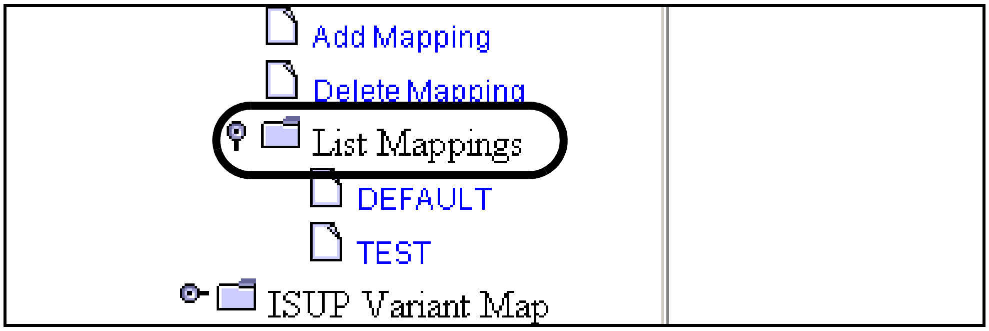
List SIP Redirection Mapping: T

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

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

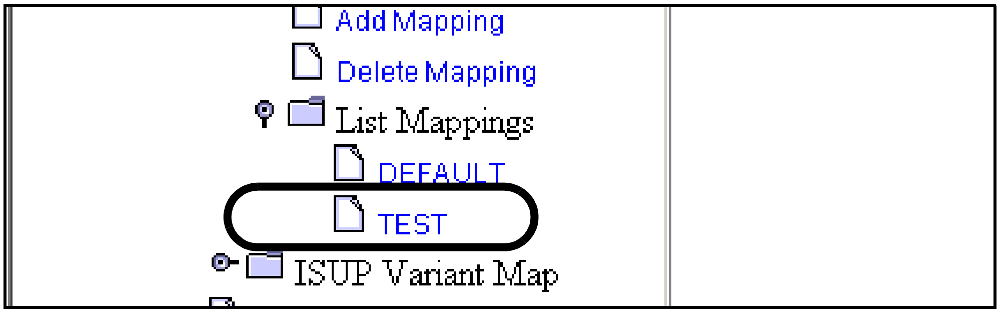
12 Click on the **List Mappings** folder to open it.

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

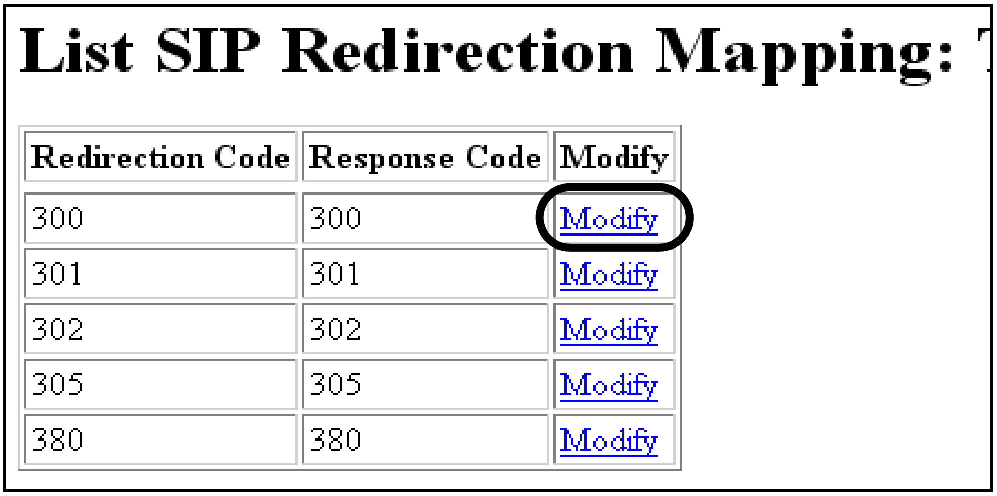


13 Click on the map name you want to review.

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.

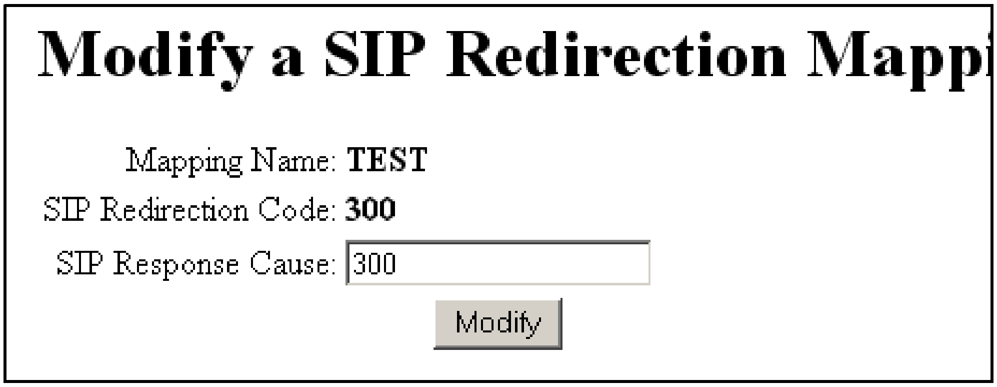


List SIP Redirection Mapping:

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



Modify a SIP Redirection Mappi

Mapping Name: **TEST**

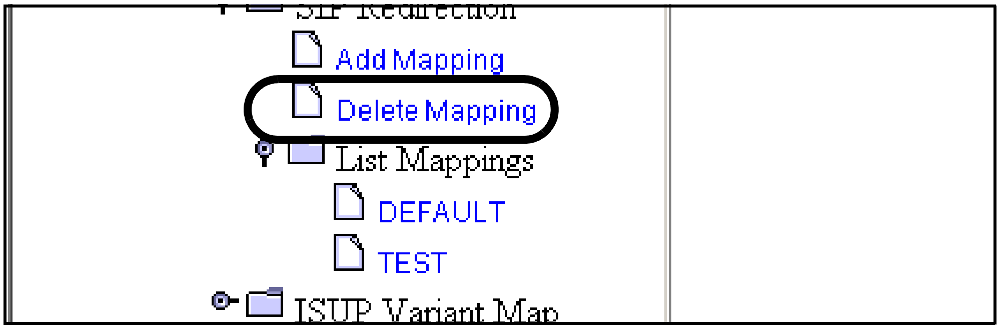
SIP Redirection Code: **300**

SIP Response Cause: 300

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

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

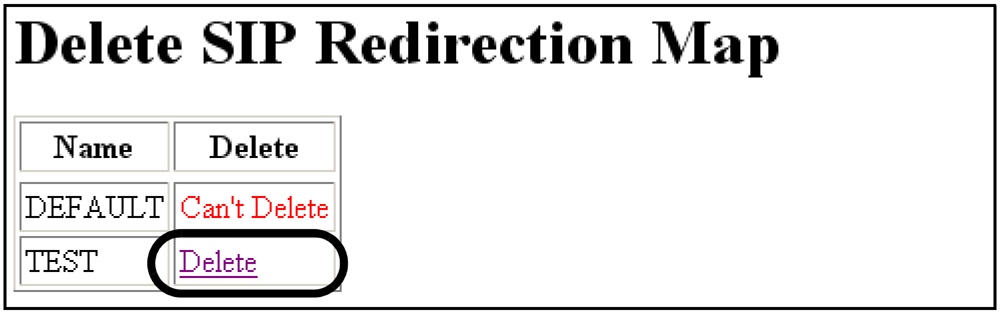
18 If you want to delete a map, click the **Delete Mapping** link. Otherwise skip to step 21.



A list of current maps is displayed

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

> ***Note:*** 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.



Delete SIP Redirection Map

Name	Delete
DEFAULT	Can't Delete
TEST	Delete

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 continue with step 22.

22 The procedure is complete.

Table of SIP Response Redirection mapping defaults

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

Add/Manage 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.

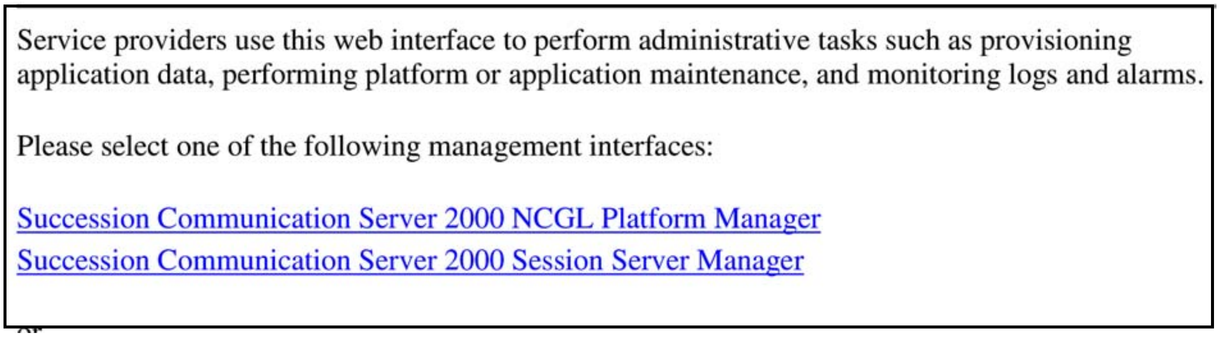
Prerequisites

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

At the CS 2000 Session Server Launch Point

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

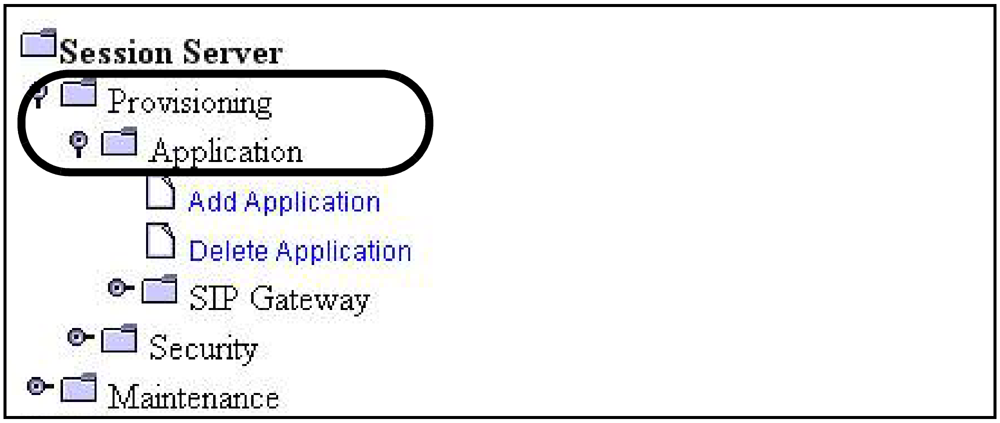


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

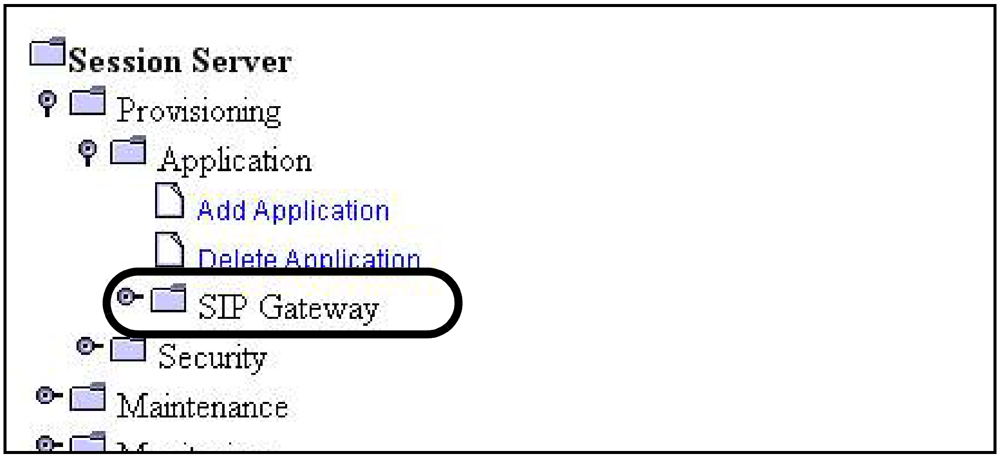
Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

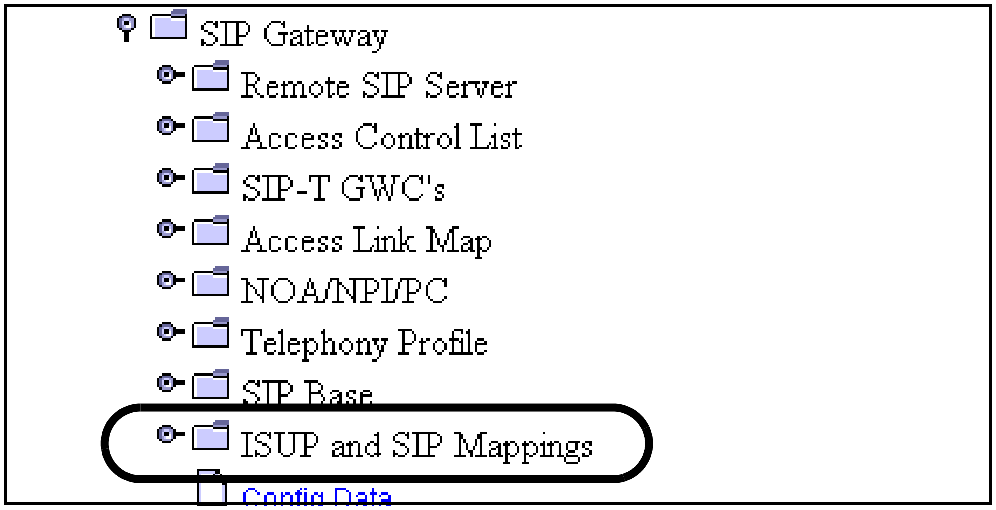
2 At the Session Server folder, click the **Provisioning folder,** then the **Application** folder.



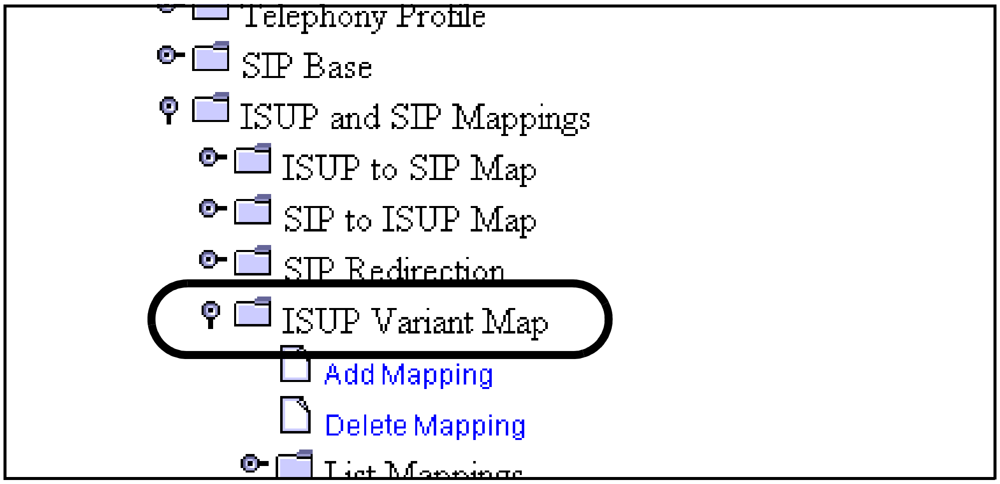
3 Click on the **SIP Gateway** folder to open the folder.



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



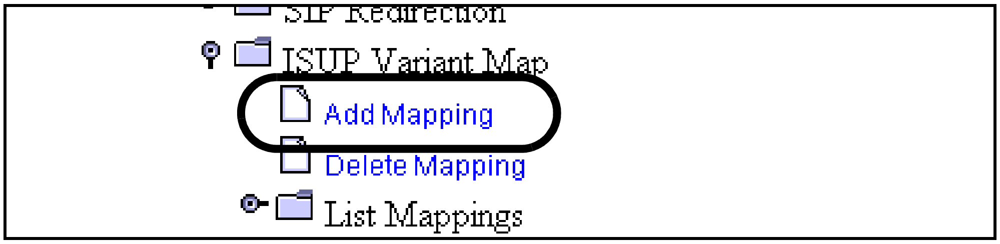
5 Click on the **ISUP Variant Map** link.



6 Use the following table to determine your next step:

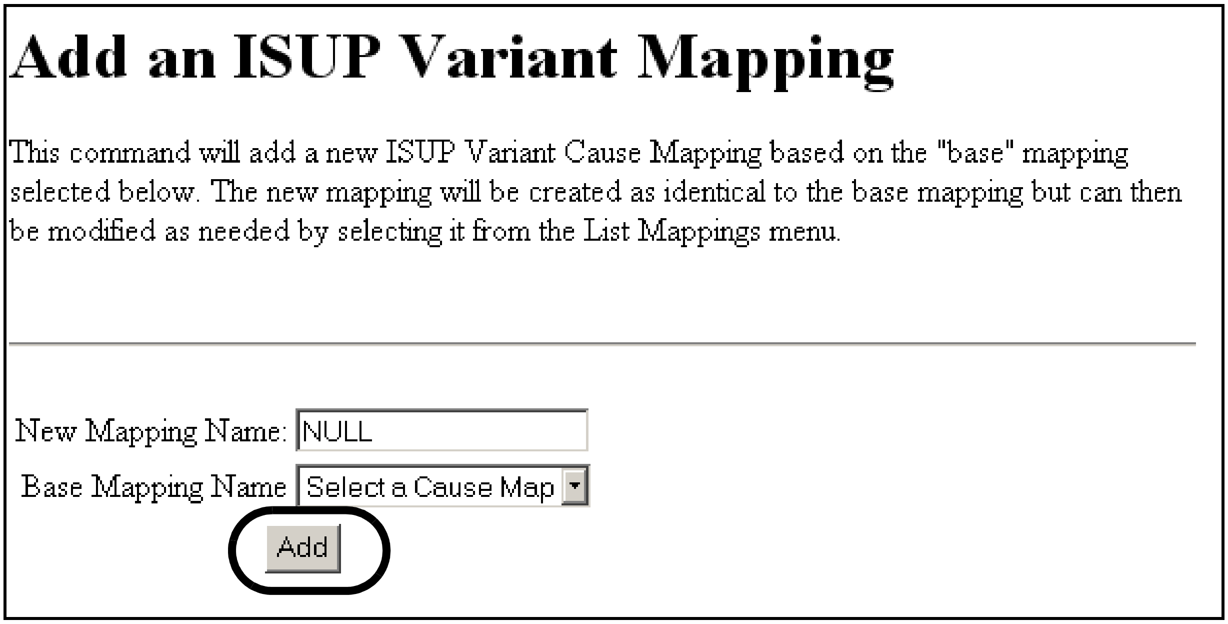
If	Do
you are adding an ISUP Variant Mapping to the SIP GW Application database, including modifying a new ISUP Variant Mapping	continue with step 7
you are listing or modifying the tuples of an existing ISUP Variant Mapping	skip to step 11
you are deleting an existing ISUP Variant Mapping (and not individual map tuples) from the database	skip to step 15
you are done adding, reviewing, changing or deleting variant mappings	skip to step 18

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.

Note: All alpha characters entered are converted to upper case.



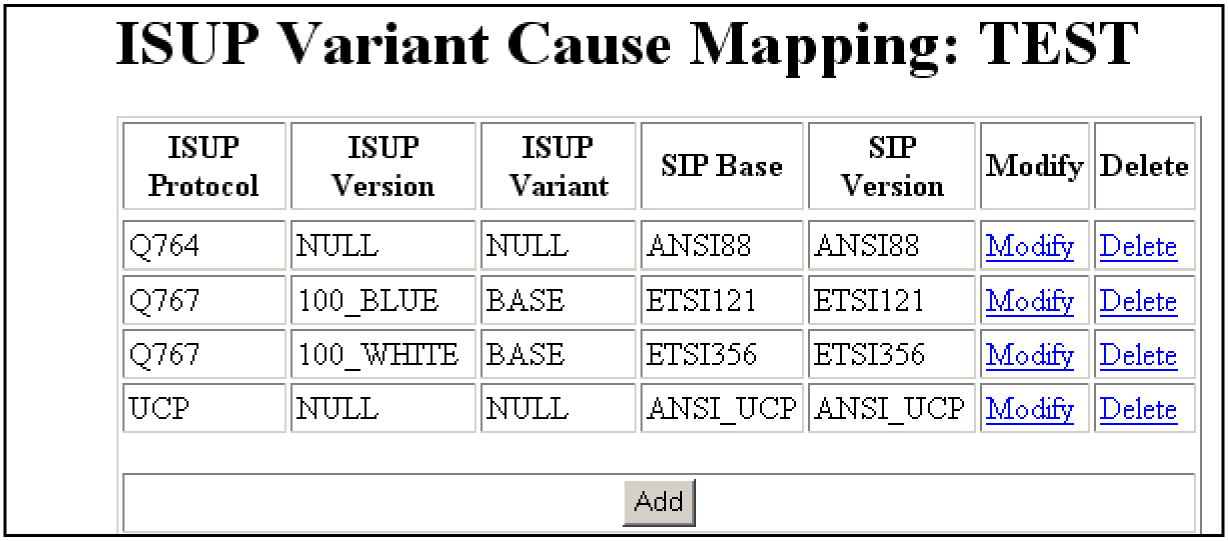
Add an ISUP Variant Mapping

This command will add a new ISUP Variant Cause Mapping based on the "base" mapping selected below. The new mapping will be created as identical to the base mapping but can then be modified as needed by selecting it from the List Mappings menu.

New Mapping Name: NULL

Base Mapping Name: Select a Cause Map

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.

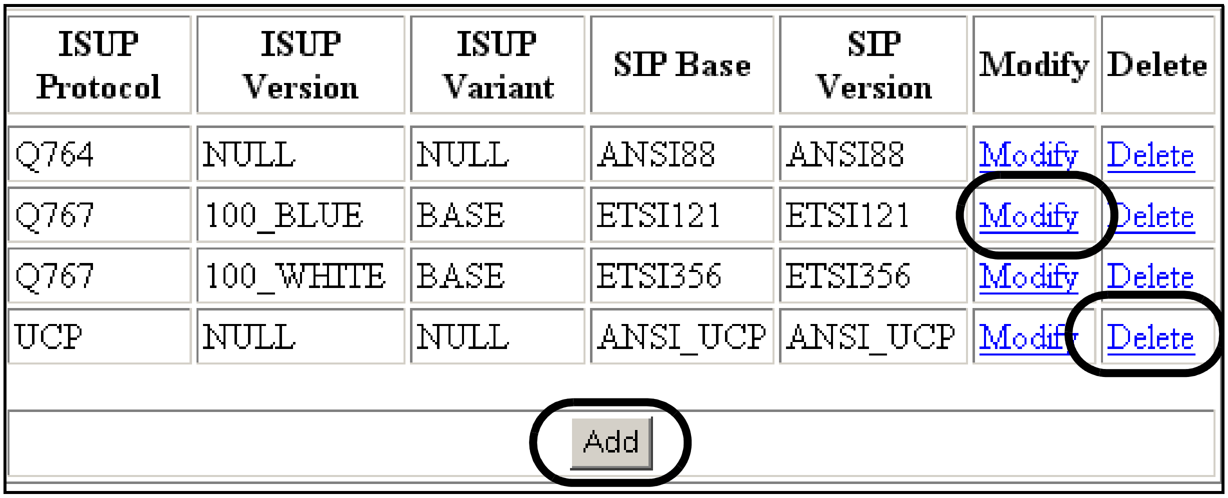


ISUP Variant Cause Mapping: TEST

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

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

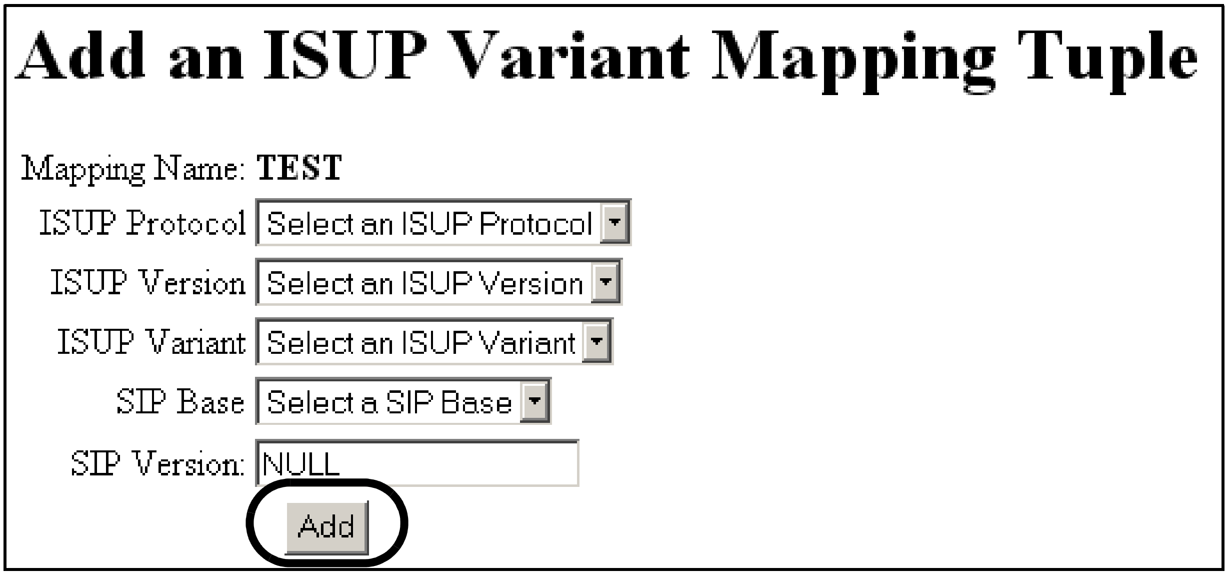
Note: Tuples within an ISUP Variant mapping table that are added or modified must adhere to specific datafill rules. The legal combinations of variables in a tuple are listed in Table of ISUP Variant to SIP Version mappings on page 127.



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

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 on page 127, create a new tuple by selecting the appropriate values from the drop-down menus and entering a SIP version. When you are done, click the **Add** button.



Add an ISUP Variant Mapping Tuple

Mapping Name: **TEST**

ISUP Protocol: Select an ISUP Protocol

ISUP Version: Select an ISUP Version

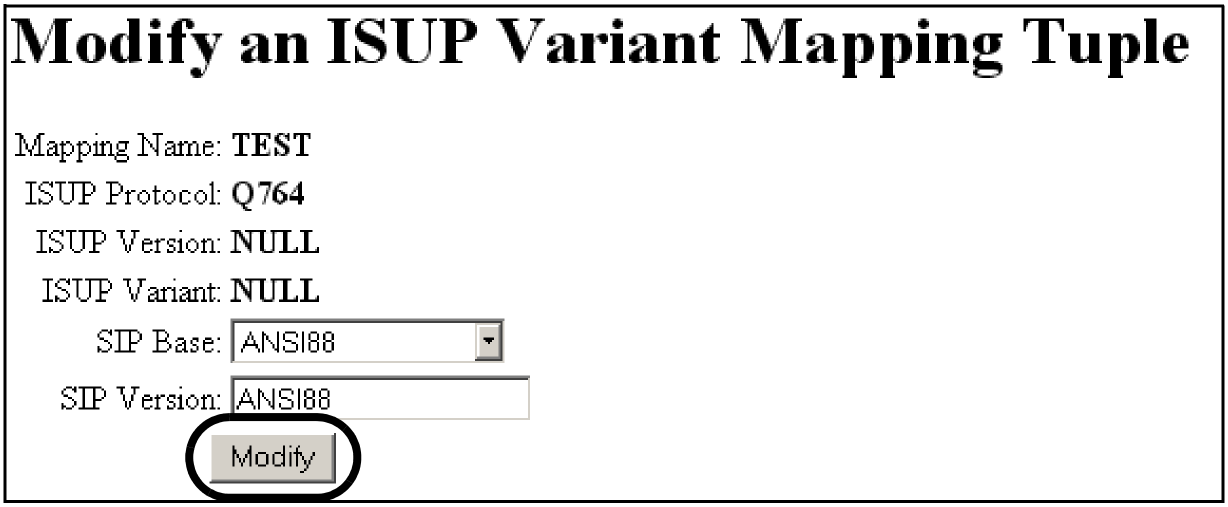
ISUP Variant: Select an ISUP Variant

SIP Base: Select a SIP Base

SIP Version: NULL

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



Modify an ISUP Variant Mapping Tuple

Mapping Name: TEST
ISUP Protocol: Q764
ISUP Version: NULL
ISUP Variant: NULL
SIP Base: ANSI88
SIP Version: ANSI88

> ***Note:*** 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.

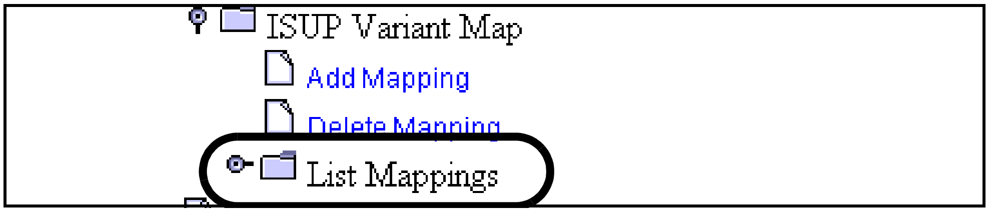
d If you want to delete a tuple from the mapping, click the **Delete** link next to the appropriate mapping name.

The system responses:

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

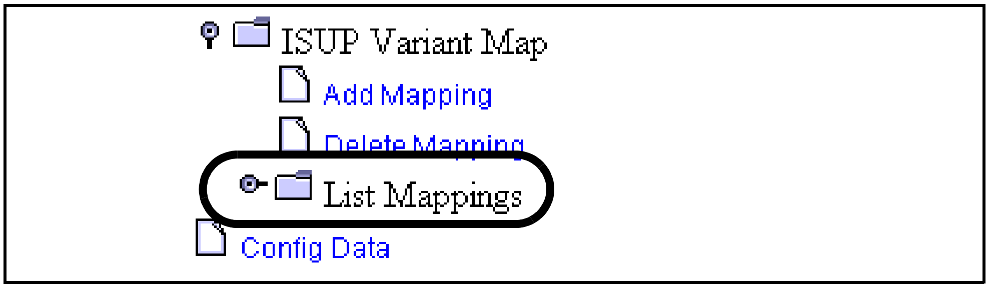
e Click **OK** to confirm the deletion.

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.



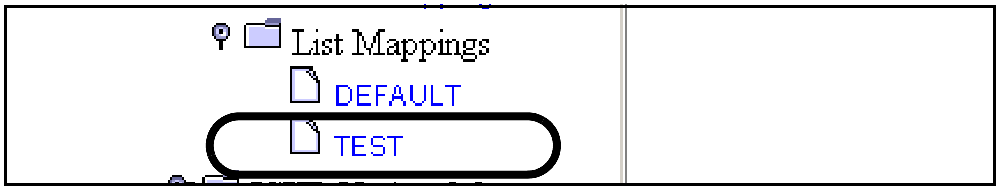
10 When you are done making changes to the new variant map, return to step 6.

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



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

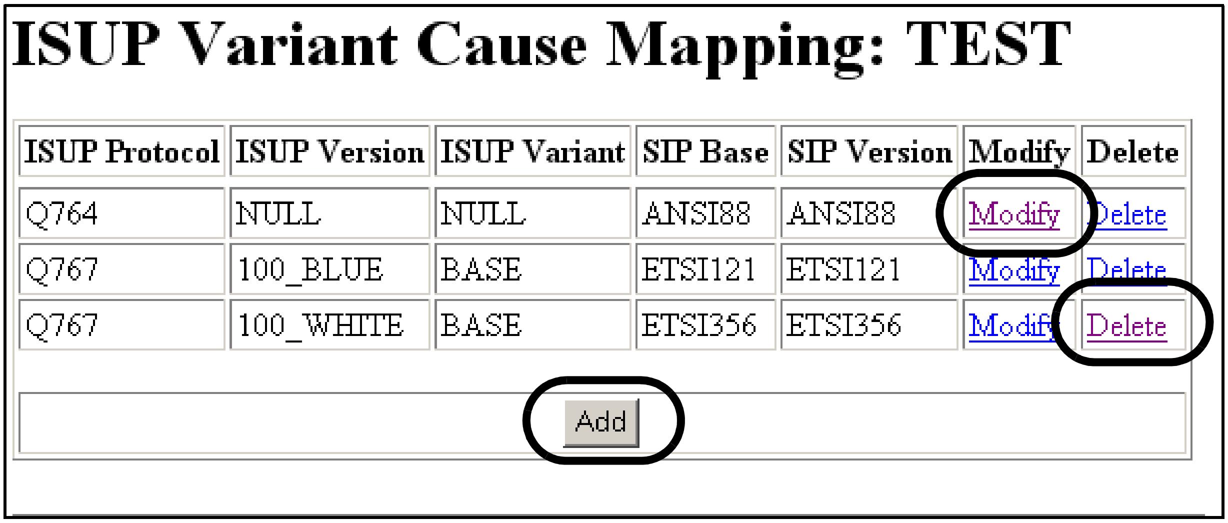
12 Click on the map name you want to review.



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.

> ***Note:*** 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 on page 127.

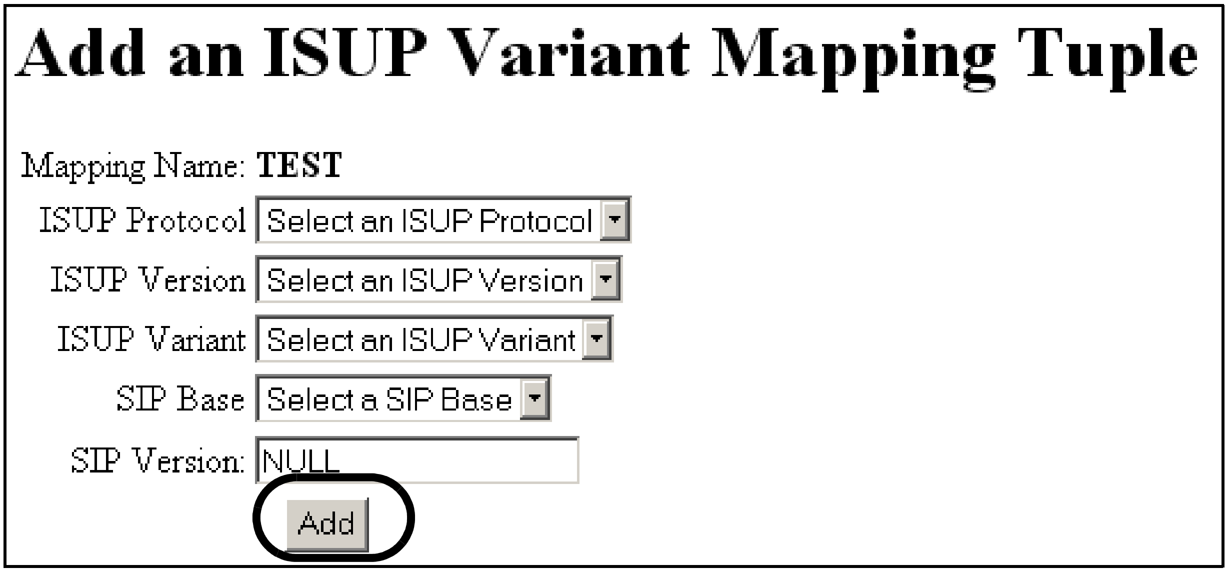


ISUP Variant Cause Mapping: TEST

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

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 on page 127, create a new tuple by selecting the appropriate values from the drop-down menus and entering a SIP version. When you are done, click the **Add** button.



Add an ISUP Variant Mapping Tuple

Mapping Name: **TEST**

ISUP Protocol: Select an ISUP Protocol

ISUP Version: Select an ISUP Version

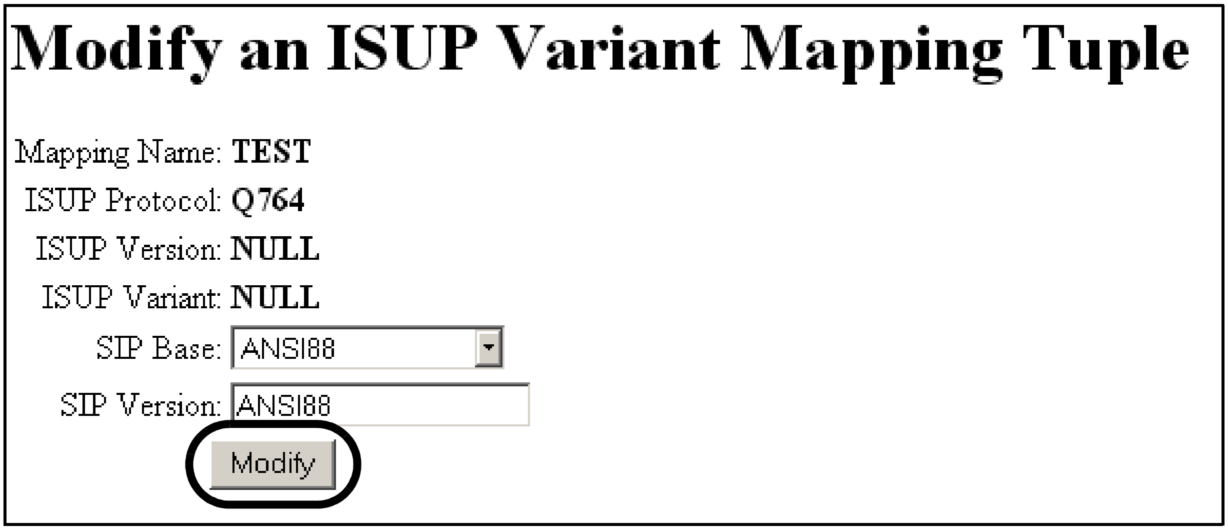
ISUP Variant: Select an ISUP Variant

SIP Base: Select a SIP Base

SIP Version: NULL

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



Modify an ISUP Variant Mapping Tuple

Mapping Name: **TEST**

ISUP Protocol: **Q764**

ISUP Version: **NULL**

ISUP Variant: **NULL**

SIP Base: ANSI88

SIP Version: ANSI88

Note: 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.

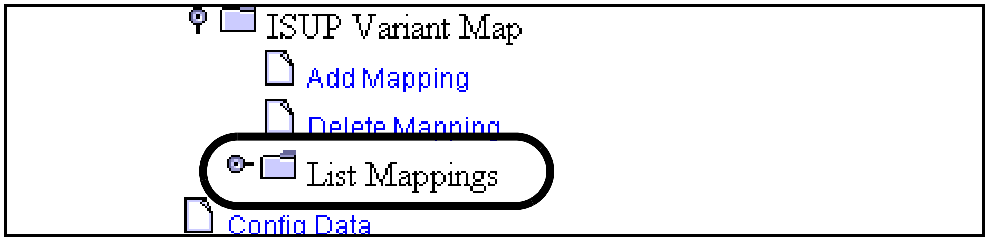
d If you want to delete a tuple from any of the mappings, click the **Delete** link next to the appropriate mapping name.

The system responses:

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

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

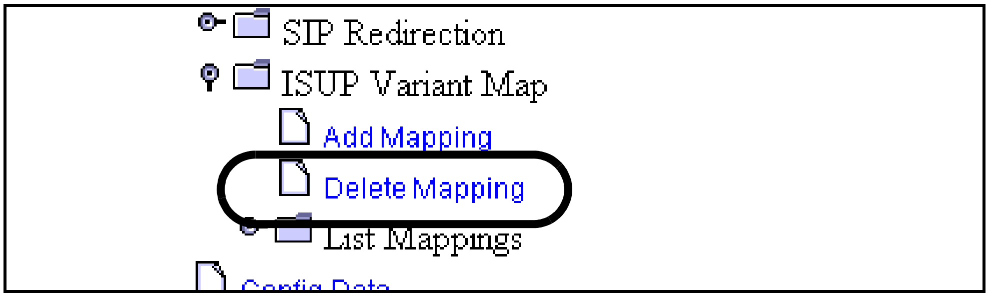
f Click again on the **List Mappings** link and select the variant map you just modified to review all changes you have made to tuples in the variant map.



14 When you are done 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.

Note: 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 done deleting mappings or continue with step 18 if you are done making changes on this Session Server unit.

18 The procedure is complete.

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

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
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
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

ISUP Protocol	ISUP Version	ISUP Variant	SIP Base	SIP Version
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 a Session Server 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

Manage 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 Security and Administration NTP, NN10338-511.

> **ATTENTION**
>
> Changing some security parameters (those marked in orange) 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

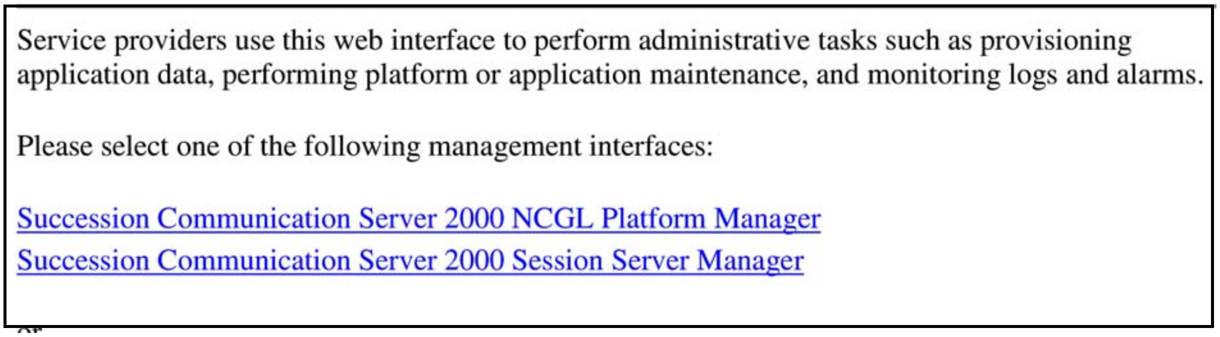
Verify that the remote SIP server you are configuring to use with Session Server TLS security supports TLS connections.

Security setting made to the Configurable Security Parameters page must match the settings made to the remote SIP server.

Action

At the CS 2000 Session Server Launch Point

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

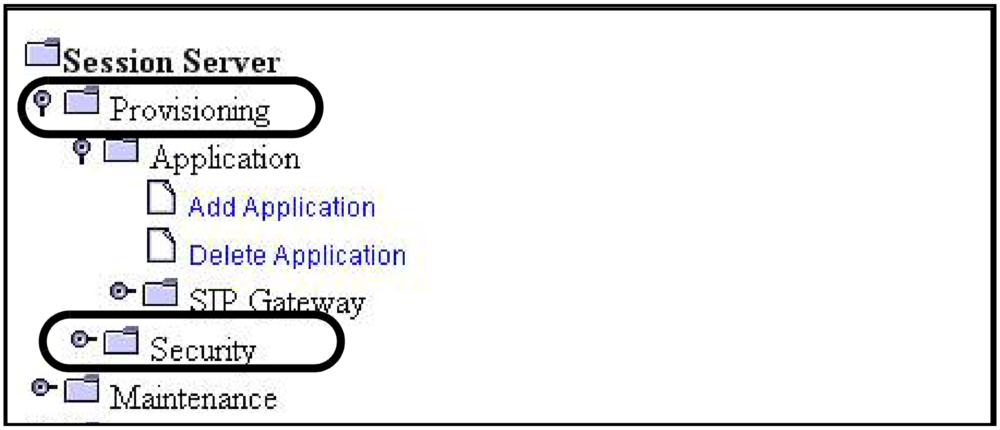


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

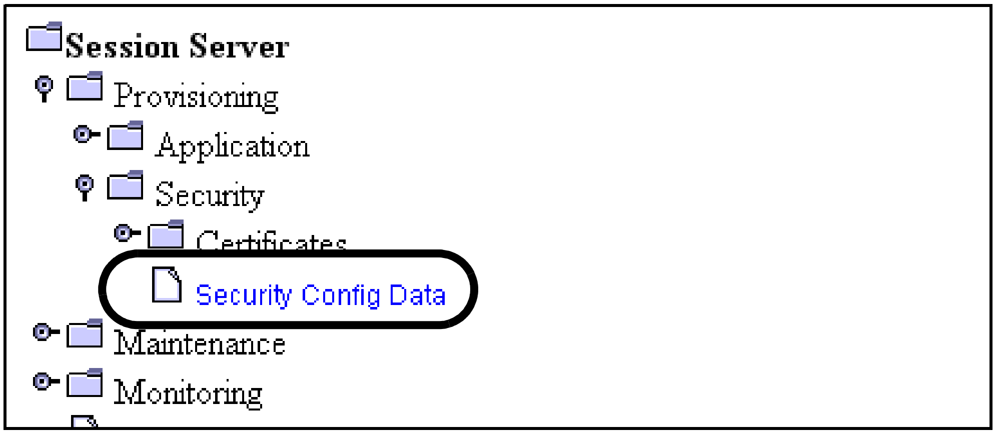
Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

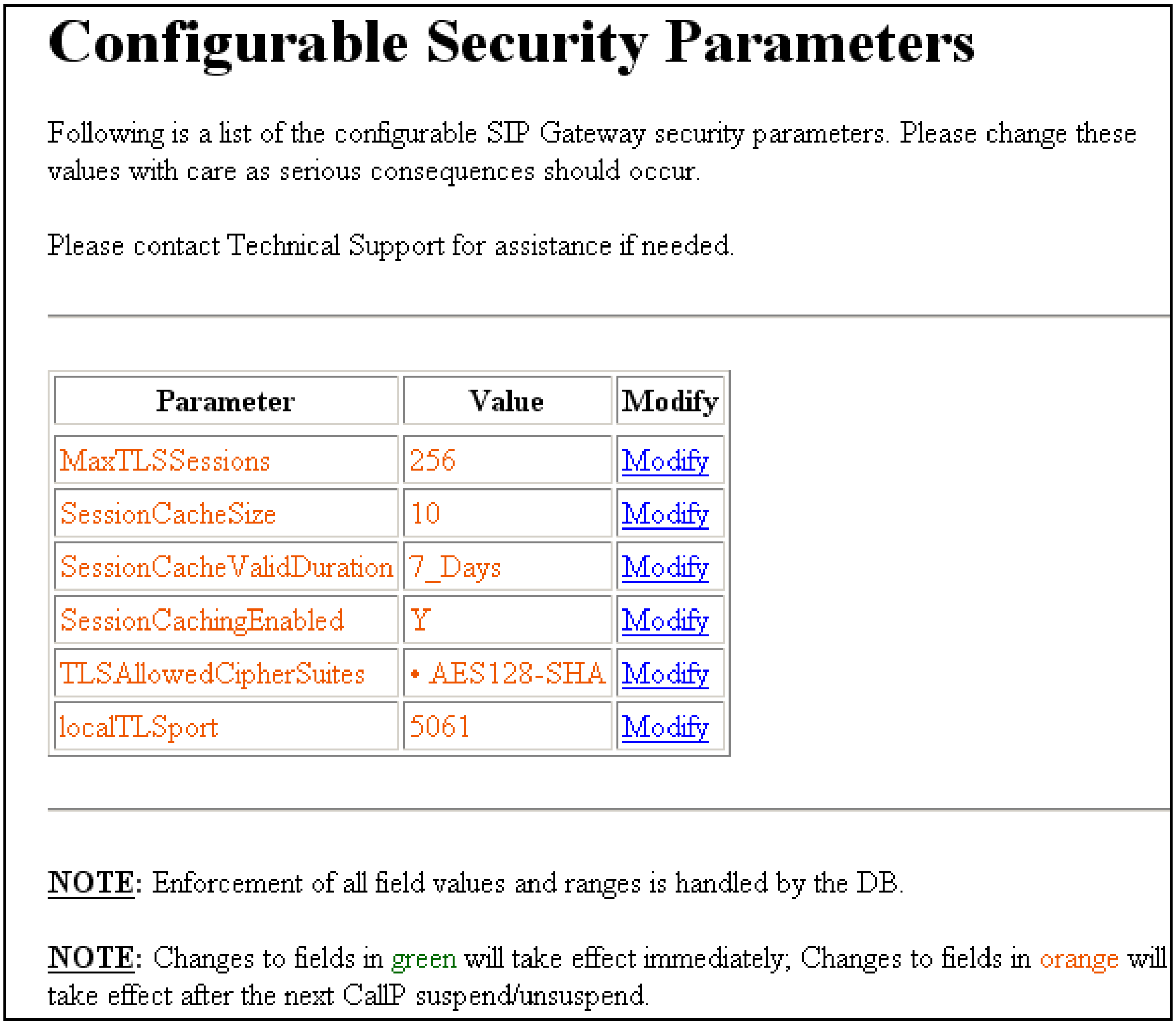
2 At the Session Server folder, click the **Provisioning folder,** then the **Security** folder.



3 Click the **Security Config Data** link to open it.



4 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	Value	Modify
MaxTLSSessions	256	Modify
SessionCacheSize	10	Modify
SessionCacheValidDuration	7_Days	Modify
SessionCachingEnabled	Y	Modify
TLSAllowedCipherSuites	• AES128-SHA	Modify
localTLSport	5061	Modify

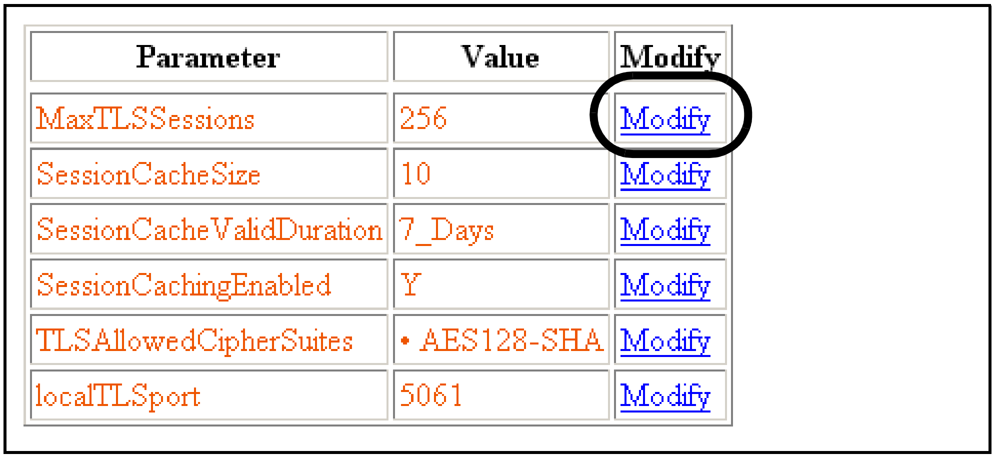
NOTE: Enforcement of all field values and ranges is handled by the DB.

NOTE: Changes to fields in green will take effect immediately; Changes to fields in orange will take effect after the next CallP suspend/unsuspend.

5 Use the following table to determine your next step:

If	Do
you are only reviewing the current parameters and their values	continue with step 10
you are modifying one or more parameter values	continue with step 6

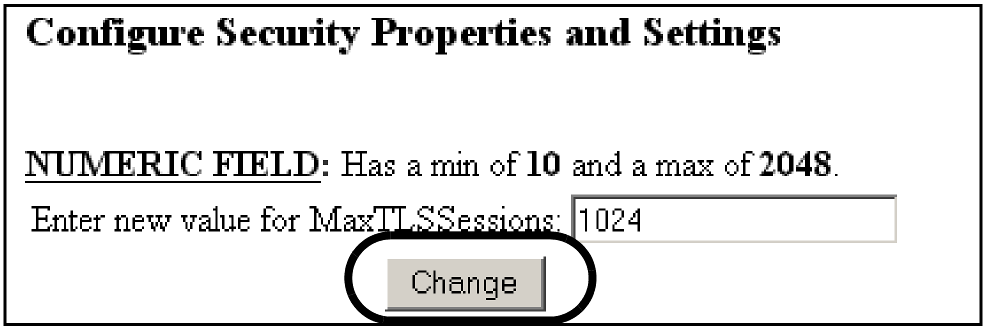
6 If you want to modify one or more security values, click the **Modify** link to the right of the value you want to change.



Parameter	Value	Modify
MaxTLSSessions	256	Modify
SessionCacheSize	10	Modify
SessionCacheValidDuration	7_Days	Modify
SessionCachingEnabled	Y	Modify
TLSAllowedCipherSuites	• AES128-SHA	Modify
localTLSport	5061	Modify

7 Refer to the table in section Additional TLS security information on page 134 to assist you with setting or changing a value for the security parameters, then click the **Change** button.

Note: Modifications to these parameters do not take effect until the SIP Gateway application is restarted in step 9.



Configure Security Properties and Settings

NUMERIC FIELD: Has a min of **10** and a max of **2048**.

Enter new value for MaxTLSSessions: 1024

8 Return to step 6 to change other security parameters, otherwise continue with step 9.

9 The SIP Gateway application must be stopped and restarted to allow it to load the new security parameters. Execute the following procedures, in the order listed, to stop and restart the application:
Lock the SIP Gateway application on page 160,
Suspend the SIP Gateway application on page 166,
Unsuspend the SIP Gateway application on page 169,
Unlock the SIP Gateway application on page 163.

10 The procedure is complete.

Additional TLS security information

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

> ***Note:*** 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
MaxTLS Sessions	The Maximum number of TLS sessions allowed.	256	10-2048
Notes: Setting the value lower than the number of clients (peer remote servers) trying to connect to the Session Server will be denied a secure connection. Set the value as high as the maximum number of peer remote servers that are expected to connect to this Session Server. The network should be engineered so that fewer than 2048 peer remote servers need to connect to a single Session Server at any one time.			
Session Cache Size	The size of the TLS session cache. The session cache increases system performance by allowing clients that support session caching to bypass the time-consuming TLS handshake procedure after a handshake is done.	10	10, 100, 1000
Notes: 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.			
Session Cache Valid Duration	The duration for which sessions are stored in the session cache. The session data is removed from the cache either 24 hours or 7 days from the time it was first inserted into the cache.	7_Days	24_Hours, 7_Days
Notes: Every connecting remote client server will be forced to do a full handshake on the first connection after its session is removed from the cache. Changing this value changes the frequency with which this can occur. Systems that have large numbers of clients making frequent connection requests may notice performance impact with the 24_Hours setting. Clients that typically stay connected for longer than 7 days will notice no difference on the 7_Days setting.			

<table>
<tr><th>Parameter Name</th><th>Description</th><th>Default Value</th><th>Range</th></tr>
<tr><td><b>Session Caching Enabled</b></td><td>Determines whether session caching is enabled or not.</td><td>Y</td><td>Yes (Y), No (N)</td></tr>
<tr><td colspan="4"><b>Notes:</b> Enabling the session cache speeds up the performance of TLS connection requests for enabled clients. If few or no peer servers to the Session Server have session-caching-enabled clients, then little or no performance increase will be observed for TLS connection requests.
Remote peer servers to the Session Server are considered clients when they initiate a connection request.</td></tr>
<tr><td><b>TLSAllowed Cipher Suites</b></td><td>The cipher suites that TLS is allowed to use in secure communications.</td><td>AES128-SHA</td><td>AES128-SHA
AES256-SHA</td></tr>
<tr><td colspan="4"><b>Notes:</b> Two ciphers are supported, but AES128-SHA is mandatory. When TLS is enabled, the Session Server will always accept TLS connections requested with the AES128-SHA cipher.
The optional AES256-SHA cipher uses larger (256-bit) keys. A performance impact may be noticed when using the AES256-SHA cipher as compared to using the default AES128-SHA cipher.</td></tr>
<tr><td><b>localTLSport</b></td><td>The port number TLS uses on the local NGSS.</td><td>5061</td><td>1024-65534</td></tr>
<tr><td colspan="4"><b>Notes:</b> Changing the default value changes the port that TLS uses.
<b>Caution:</b> 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.</td></tr>
</table>

View 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. This procedure may 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 SIP Gateway application software only. For instructions on determining the status of the Session Server platform, refer to procedure View the operational status of a Session Server NCGL platform on page 141.

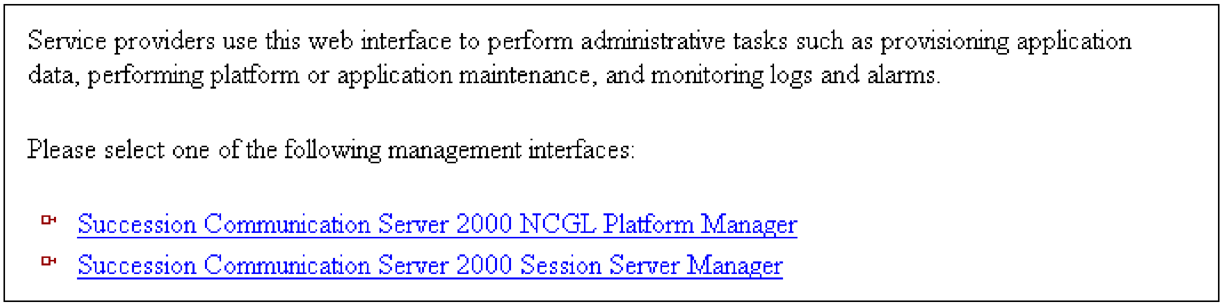
Prerequisites

There are no prerequisites for this procedure.

Action

At the Session Server GUI or Integrated EMS client

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

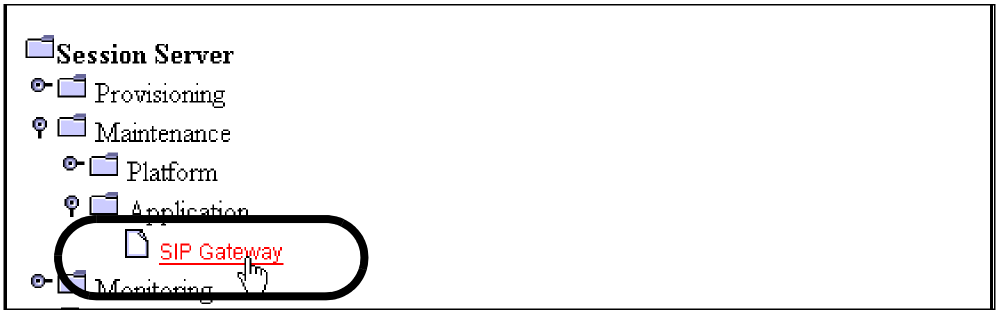


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

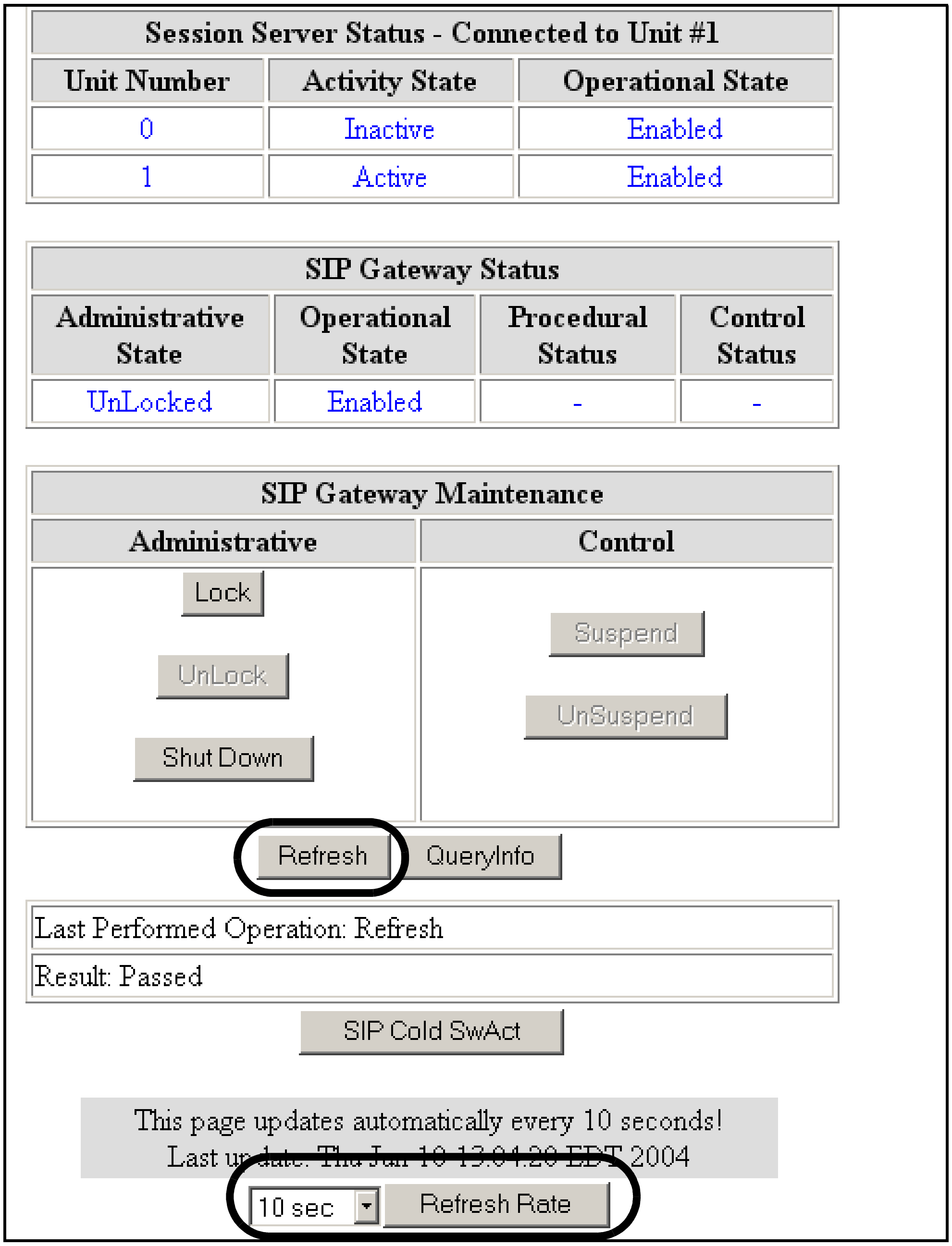
Please select one of the following management interfaces:

- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

2 At the Session Server folder, click **Maintenance > Application > SIP Gateway**.



3 Monitor the status of the SIP Gateway application on the active Session Server node from this view.



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

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

SIP Gateway Maintenance	
Administrative	**Control**

Last Performed Operation: Refresh

Result: Passed

This page updates automatically every 10 seconds!
Last update: Thu Jan 10 13:04:20 EDT 2004

Note: 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.

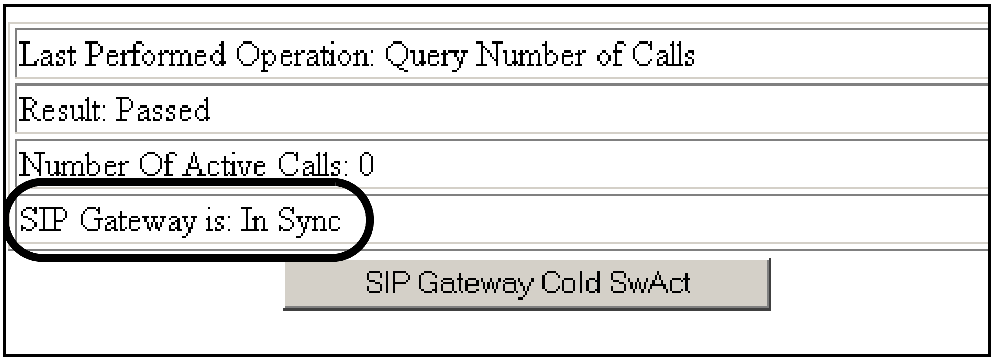
4 Refer to section Interpreting SIP Gateway application status and maintenance fields on page 139 to review the description of the various fields of this view.

> ***Note:*** For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section *Interpreting SIP Gateway application states* found in the Session Server Security and Administration NTP, NN10346-611.

5 To perform available SIP Gateway application maintenance activities, refer to the following procedures found in the Session Server Security and Administration NTP, NN10346-611:

- 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 sync status of the Session Server units, click the **QueryInfo** button.



Last Performed Operation: Query Number of Calls

Result: Passed

Number Of Active Calls: 0

SIP Gateway is: In Sync

7 The procedure is complete.

Interpreting SIP Gateway application status and maintenance fields

Use the following table to assist you in interpreting the Session Server Status area.

Session Server node status field descriptions

Field	Description
Unit Connection Status Bar	Indicates which Session Server unit in the node the CS 2000 Session Server Manager is connected to.
Unit Number	Indicates the units in the Session Server node, (labeled 0 and 1) and a maximum of one node on the Call Server-LAN
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 are operational.
Operational State	Indicates the service status of each Session Server unit (either Enabled or Disabled).

Use the following table to assist you in interpreting the SIP Gateway status area.

SIP Gateway application Status field descriptions

Field	indication
Administrative State	Locked, Unlocked, 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)
Unlocked	Disabled	-	-	System Busy (SYSB)
Shutting Down	Enabled	-	-	Going out of service (INSVD)

Note: (-) indicates a status of in-service

View the operational status of a Session Server NCGL platform

Purpose of this procedure

Use the following procedure to view the service status of the Session Server platform hardware and NCGL operating system using the CS 2000 NCGL Platform Manager. This procedure may 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 Session Server NCGL platform only. For instructions on determining the status of the SIP Gateway application, refer to procedure *View the operational status of the SIP Gateway application* in the Session Server Configuration Management NTP, NN10338-511.

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 change platform or NCGL settings such as changing BIOS settings or platform provisioning. Refer to the appropriate procedures in the Session Server Configuration Management NTP, NN10338-511, for changing these settings.

This procedure does not describe how to view customer logs or alarms or how to change the root password. For detailed instructions on viewing customer logs or alarms, refer to procedures in the Session Server Fault Management NTP, NN10332-911. For instructions on how to change the platform root password, refer to the Session Server Security and Administration NTP, NN10346-611.

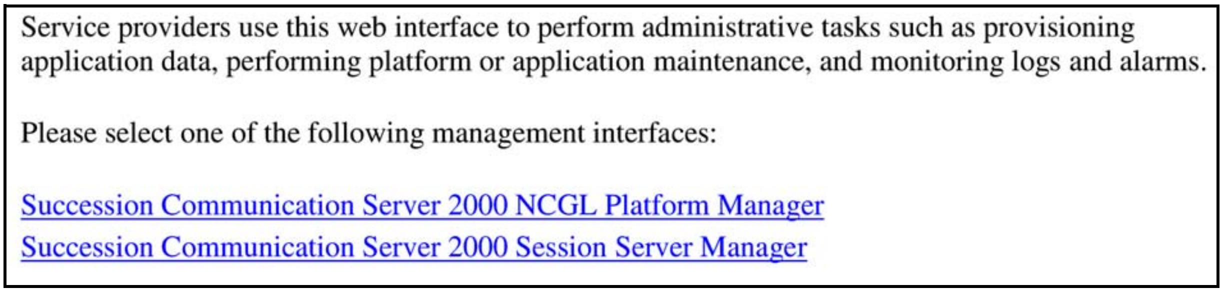
Prerequisites

There are no prerequisites for using this procedure.

Action

At the Session Server GUI or Integrated EMS client

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

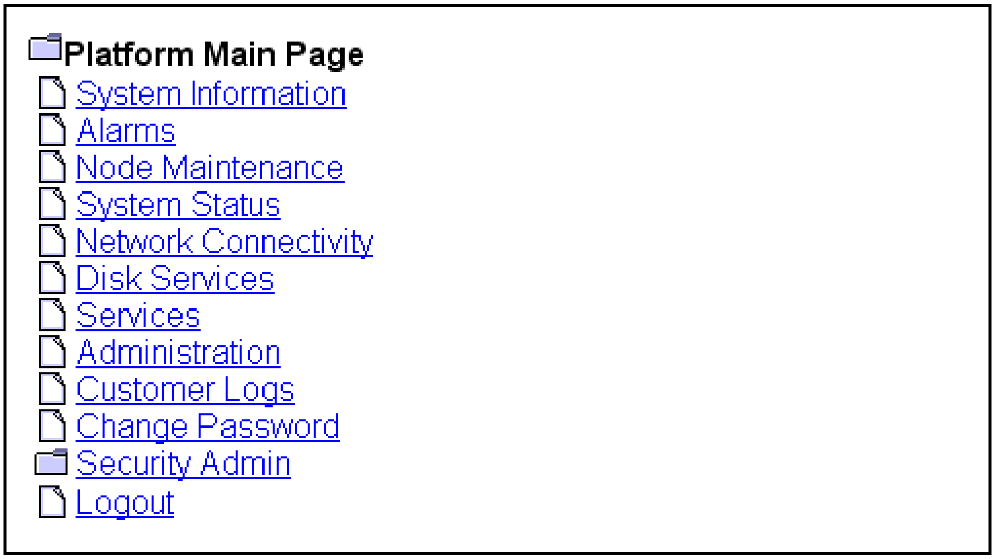


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

The Platform Main Page menu is displayed.



Platform Main Page
System Information
Alarms
Node Maintenance
System Status
Network Connectivity
Disk Services
Services
Administration
Customer Logs
Change Password
Security Admin
Logout

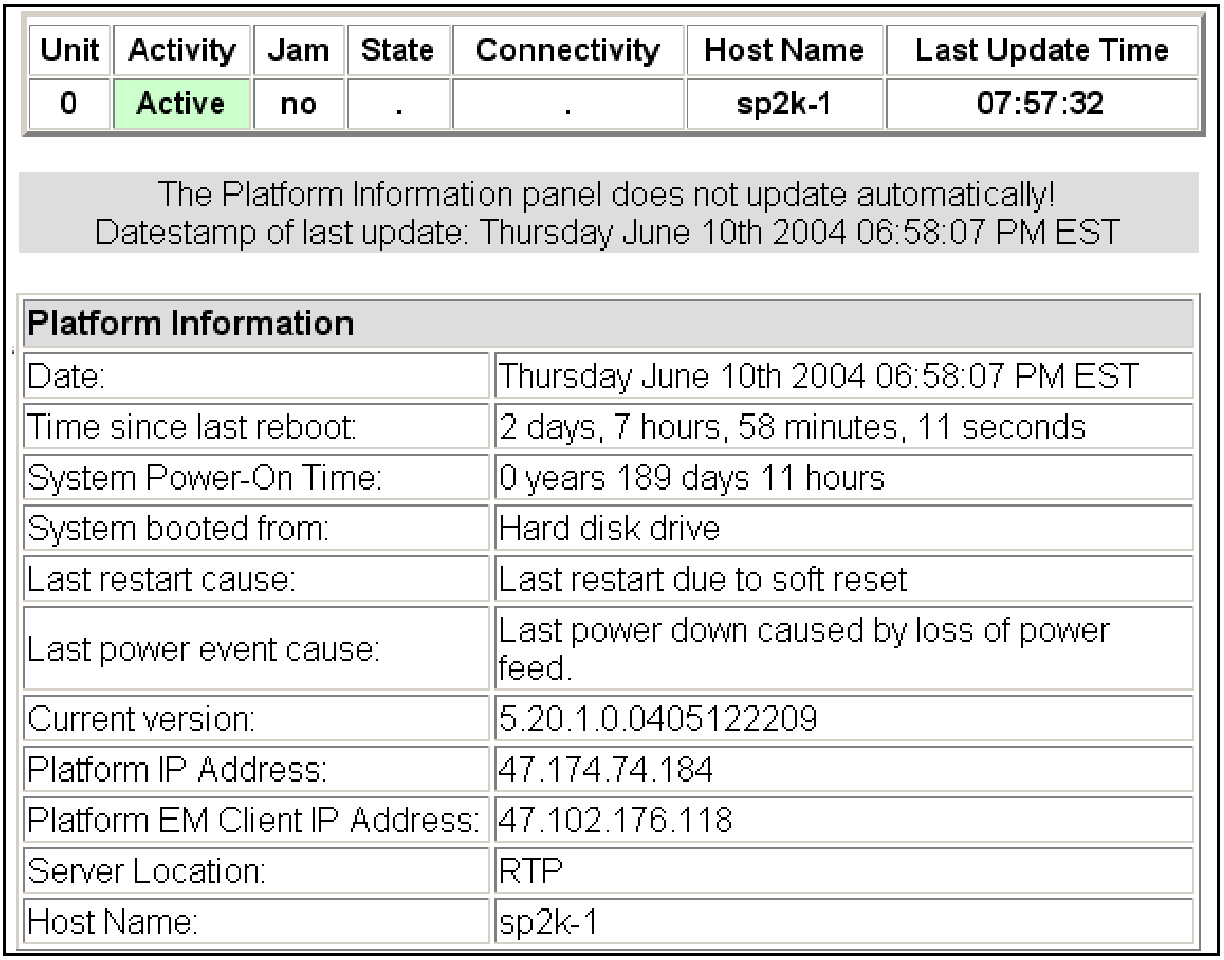
2 Use the following table to determine your next step:

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	Skip to step 17 and go to procedure *View Session Server alarms* in the Session Server Fault Management NTP, NN10332-911.
you want to review node maintenance status	Click the **Node Maintenance** link and go to step 5.

If	Do
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 the Session Server Security and Administration NTP, 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	Skip to step 17 and go to procedure *View Session Server logs* in the Session Server Fault Management NTP, NN10332-911.
you want to change root passwords	Skip to step 17 and go to procedure *Manage user passwords with the Session Server GUI* in the Session Server Security and Administration NTP, NN10346-611.
you want to view TLS security information or manage security certificates	Skip to step 17 and refer to the Session Server Security and Administration NTP, NN10346-611 to manage security certificates. Refer to the Session Server Configuration Management NTP, NN10338-511 to review TLS security settings.
you are finished reviewing information and want to logout 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:

> ***Note:*** 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
0	Active	no	.	.	sp2k-1	07:57:32

The Platform Information panel does not update automatically!
Datestamp of last update: Thursday June 10th 2004 06:58:07 PM EST

Platform Information	
Date:	Thursday June 10th 2004 06:58:07 PM EST
Time since last reboot:	2 days, 7 hours, 58 minutes, 11 seconds
System Power-On Time:	0 years 189 days 11 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:	5.20.1.0.0405122209
Platform IP Address:	47.174.74.184
Platform EM Client IP Address:	47.102.176.118
Server Location:	RTP
Host Name:	sp2k-1

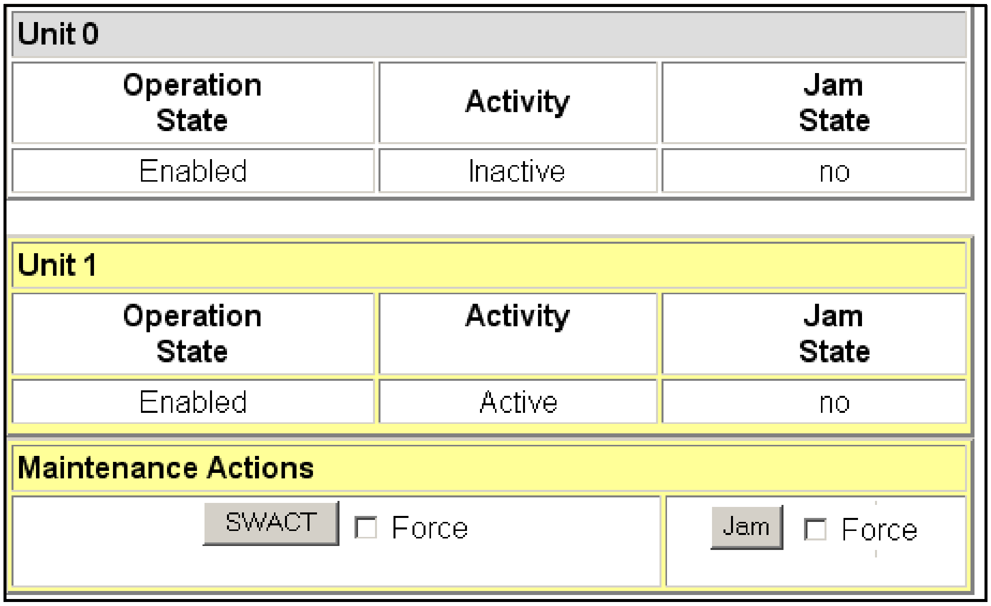
Field	Description
Unit	The unit number in the node that you are logged into.
Activity	Indicates the activity of the unit (either active or standby).
Jam	Indicates if an activity Jam has occurred on the active Session Server unit. This prevents the standby unit from becoming active, regardless of any failures on the active unit.

Field	Description
State	Indicates if the Session Server node is operating in a duplex (fault-tolerant) mode or a simplex mode (the standby unit is off-line).
Connectivity	Indicates the state of the network links on the node.
Host Name	Indicates the name of the Session Server unit (not node).
Date	Indicates the system date as maintained by the network time protocol (NTP) server.
Time since last reboot:	Indicates the amount of time that has elapsed since the Session Server was last rebooted for any reason.
System Power-On Time:	Indicates the recorded system time that the Session Server has been powered up.
System booted from:	Indicates whether the Session Server 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:	Indicates the installed version of the Session Server platform software. (Does not include the SIP Gateway application or other co-resident applications.) Refer to the Session Server Upgrades NTP, NN10349-461, for more procedures on acquiring version information.
Platform IP Address:	Indicates the IP address of the Session Server platform.
Platform EM Client IP Address:	Indicates the IP address of the Session Server client web interface. This is the IP address of the PC or Unix client from which the GUI was launched. When a web proxy is used, the IP address is the SSPFS proxy IP address.
Server Location:	Indicates the physical location of the Session Server.
Host Name:	Indicates the name of the Session Server 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:

> ***Note:*** The Node Maintenance panel is refreshed every 45 seconds.



Unit 0

Operation State	Activity	Jam State
Enabled	Inactive	no

Unit 1

Operation State	Activity	Jam State
Enabled	Active	no

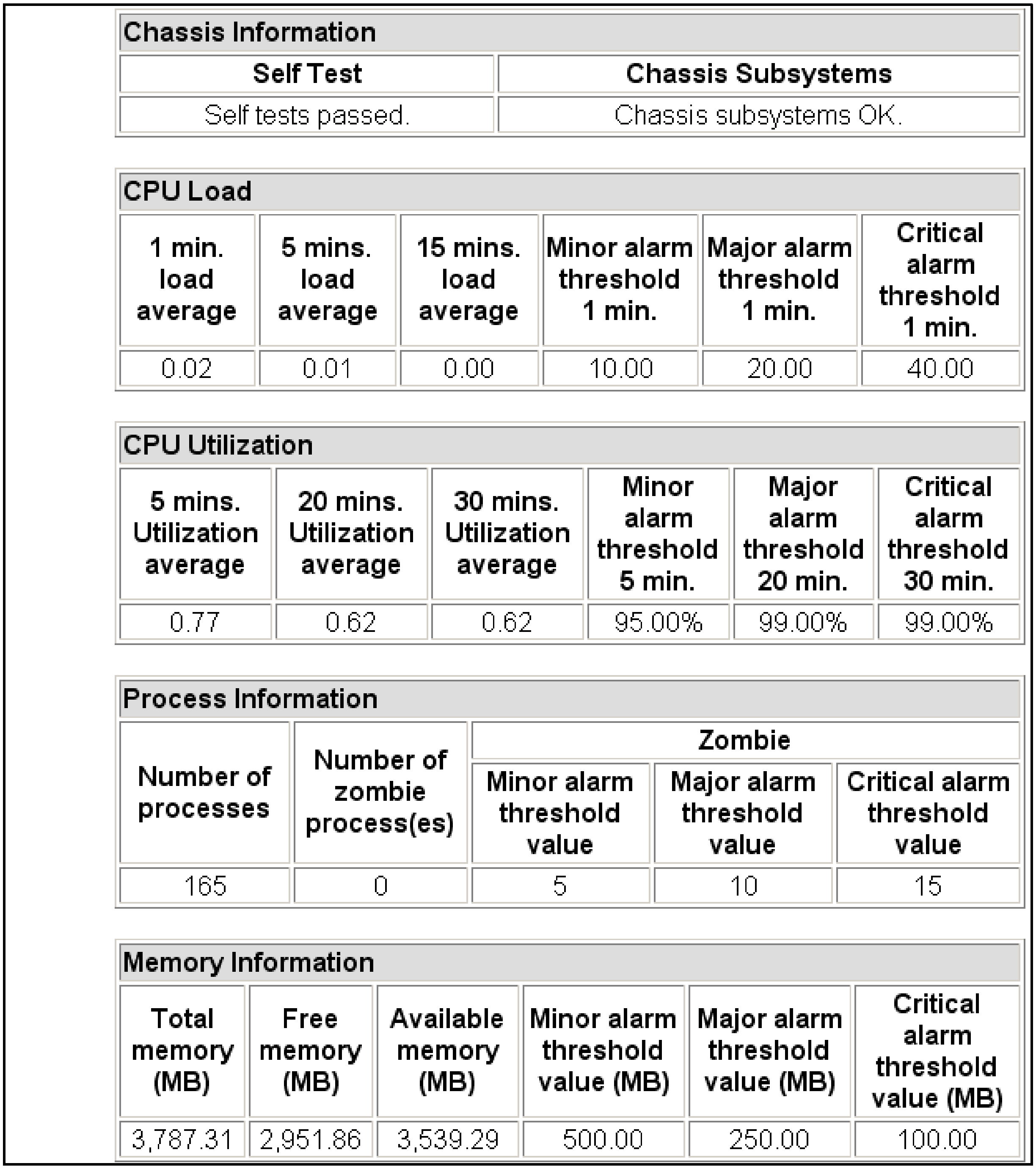
Maintenance Actions

Field	Description
Operation State (unit 0 or 1)	Indicates the operational state of the platform software.
Activity (unit 0 or 1)	Indicates the activity state of the platform software.
Jam State (active unit only)	Indicates whether or not an activity jam has been requested.
Maintenance Actions (active unit only)	Maintenance panel for performing node SwAct activity and to unjam node activity. Refer to the Session Server Security and Administration NTP, NN10346-611, for procedures on performing a SwAct or Jam/unJam of the active unit.

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:

Note: The Chassis Information panel is not automatically refreshed.



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.
0.02	0.01	0.00	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.
0.77	0.62	0.62	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
165	0	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)
3,787.31	2,951.86	3,539.29	500.00	250.00	100.00

Field	Description
Chassis information: Self Test	Indicates the status of the self test performed on the platform at boot up.
Chassis information: Chassis Subsystems	Indicates the status of the platform hardware subsystems including the memory, CPU, all drives, network connection, power supplies, cooling and other I/O connections.
CPU Information: load average	Indicates the 1, 5 and 15 minute load averages for the CPU utilization.
CPU information: load average threshold values	Indicates the 1 minute CPU load average utilization threshold value. When the set threshold value is exceeded, the appropriate minor, major or critical alarm is raised.
Chassis Utilization: Utilization average	Indicates the 5, 20 and 30 minute CPU utilization average. When the threshold value is exceeded, an alarm is raised.
Chassis Utilization: alarm threshold values	Indicates the 5, 20 and 30 minute CPU utilization average threshold value. When the set threshold value is exceeded, an alarm is raised.
Process Information: Number of Processes	Indicates the total number of processes (non-threaded) that are running on the Session Server Platform.
Process Information: Number of zombie processes	Indicates the number of defunct or terminated NCGL zombie processes. ***Note:*** 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.
Process Information-zombie: minor alarm threshold value	Indicates the 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.

Field	Description
Process Information-zombie: major alarm threshold value	Indicates the 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.
Process Information-zombie: critical alarm threshold value	Indicates the 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)	The total amount of RAM installed on the motherboard of each Session Server unit. Both units must have the same amount.
Memory Information: Free Memory (MB)	The amount of memory available unallocated for use.
Memory Information: Available memory (MB)	The amount of memory available for programs.
Memory Information: minor alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a minor alarm is raised.
Memory Information: major alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a major alarm is raised.
Memory Information: critical alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a critical alarm is raised.

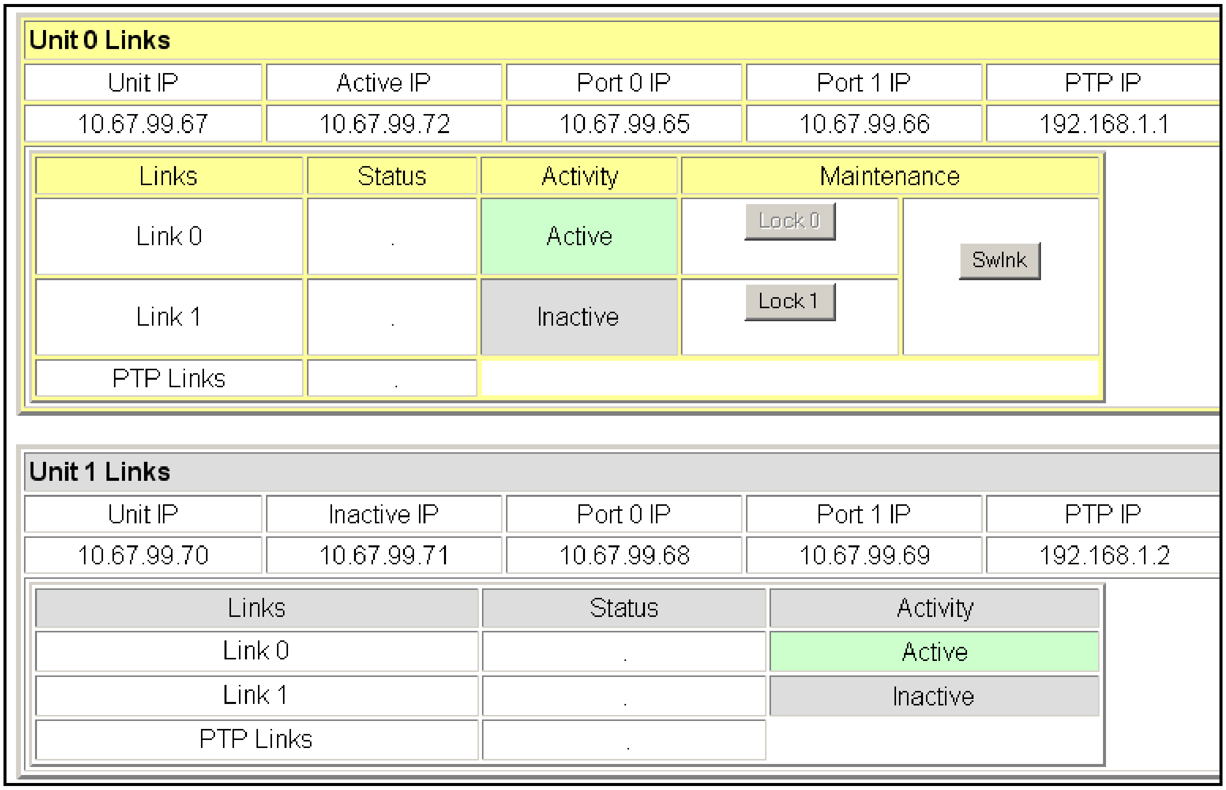
8 When you have completed reviewing the System Status, return to step 2.

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

ATTENTION

Do not perform link management activities such as Lock, Suspend or Swlink using this procedure. Refer to the Session Server Security and Administration NTP, NN10346-611, to perform these activities.

Note: The Network Connectivity panel is refreshed every 45 seconds.



Unit 0 Links

Unit IP	Active IP	Port 0 IP	Port 1 IP	PTP IP
10.67.99.67	10.67.99.72	10.67.99.65	10.67.99.66	192.168.1.1

Links	Status	Activity	Maintenance	
Link 0	.	Active	Lock 0	Swlnk
Link 1	.	Inactive	Lock 1	
PTP Links	.			

Unit 1 Links

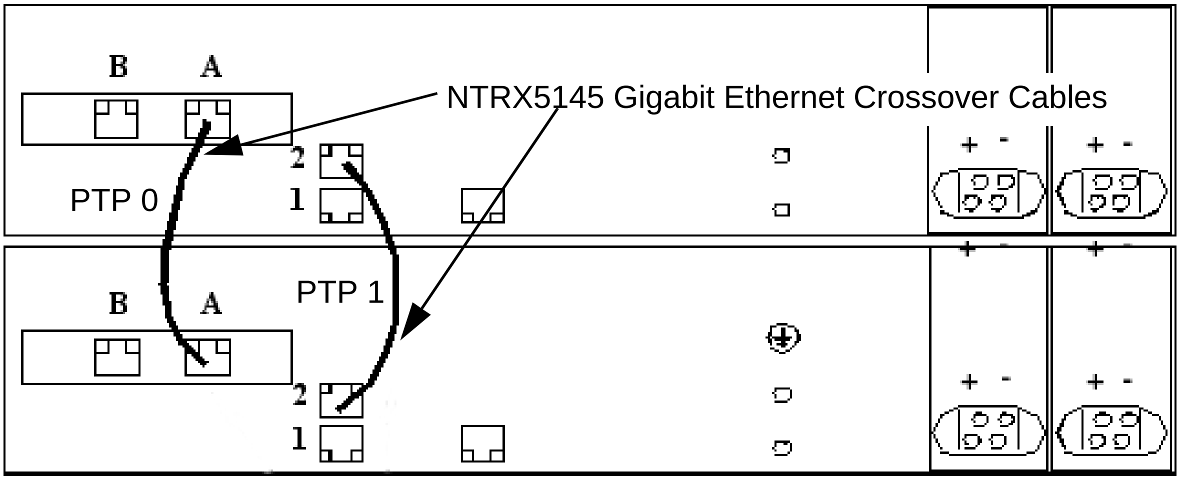
Unit IP	Inactive IP	Port 0 IP	Port 1 IP	PTP IP
10.67.99.70	10.67.99.71	10.67.99.68	10.67.99.69	192.168.1.2

Links	Status	Activity
Link 0	.	Active
Link 1	.	Inactive
PTP Links	.	

Field	Description
Unit 0,1 Links	Indicates which ethernet IP links are installed on the Session Server units (each unit has two links).
Unit 0,1 Status	Indicates the status of the ethernet links.

Field	Description
Unit 0,1 Activity	Indicates the 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. Refer to the Session Server Security and Administration NTP, NN10346-611, to perform link management.
Unit 0,1 PTP Links status	Indicates the status of the PTP links between both units in the node.
Unit IP	The network IP address of the Session Server unit.
Active IP	The IP address of the local (active) Session Server unit.
Inactive IP	The IP address of the mate (inactive) Session Server unit.
Port 0 IP	The IP address of the active or inactive ethernet port 0.
Port 1 IP	The IP address of the active or inactive ethernet port 1.
PTP IP	The IP address of the active or inactive PTP link.

Crossover and LAN ethernet cable connections for Session Server units



Ethernet Ports:

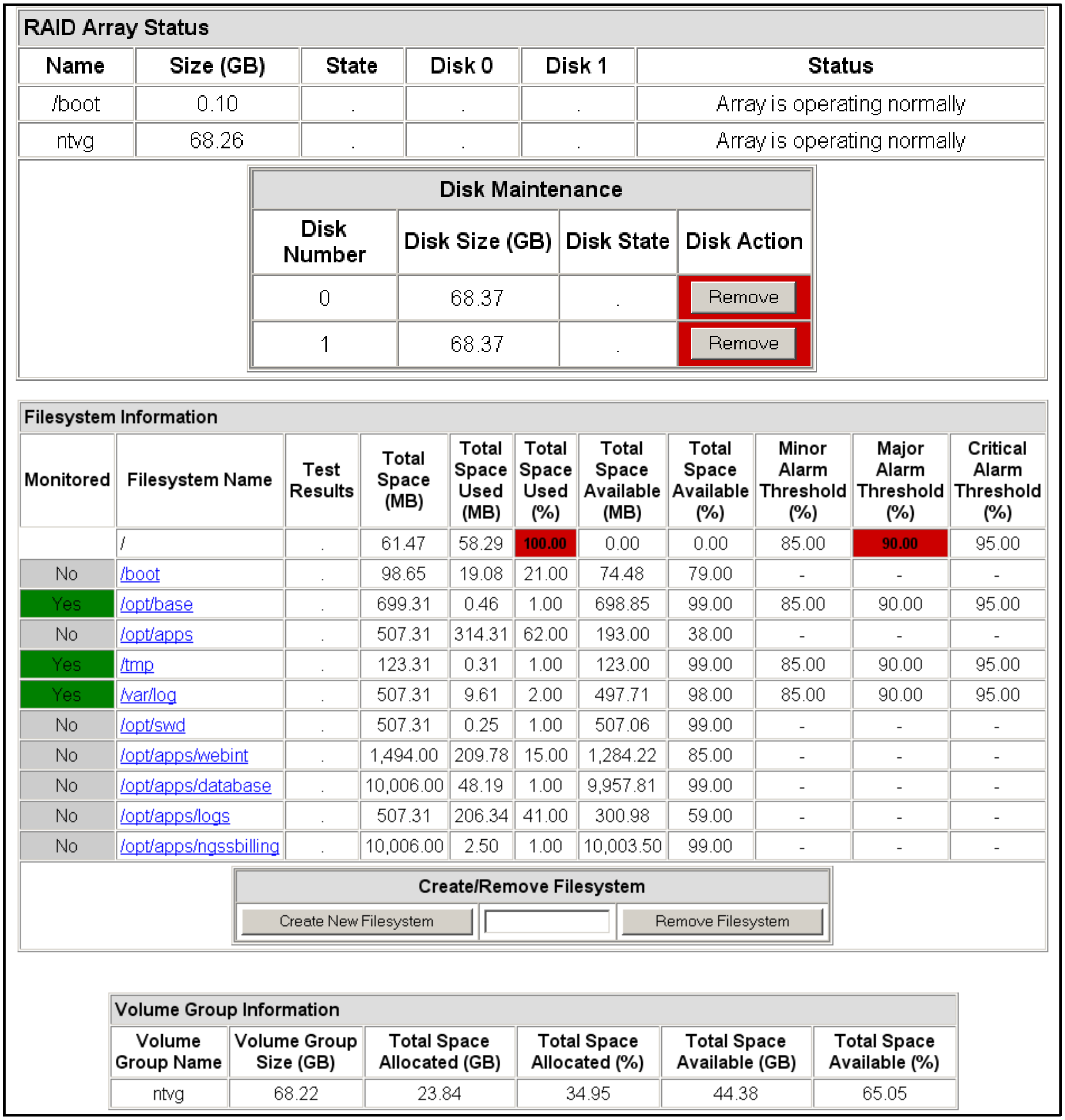
Ports 1 and B (both sets) go to CS-LAN Switch

Ports 2 (PTP1) and A (PTP0) are point-to-point connections between Session Server 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:

Note 1: The Disk Services panel does not update automatically. Click the **Disk Services** link again to update it.

Note 2: To create and remove file systems, refer to applicable procedures in the Session Server Configuration Management NTP, NN10338-511.



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

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.

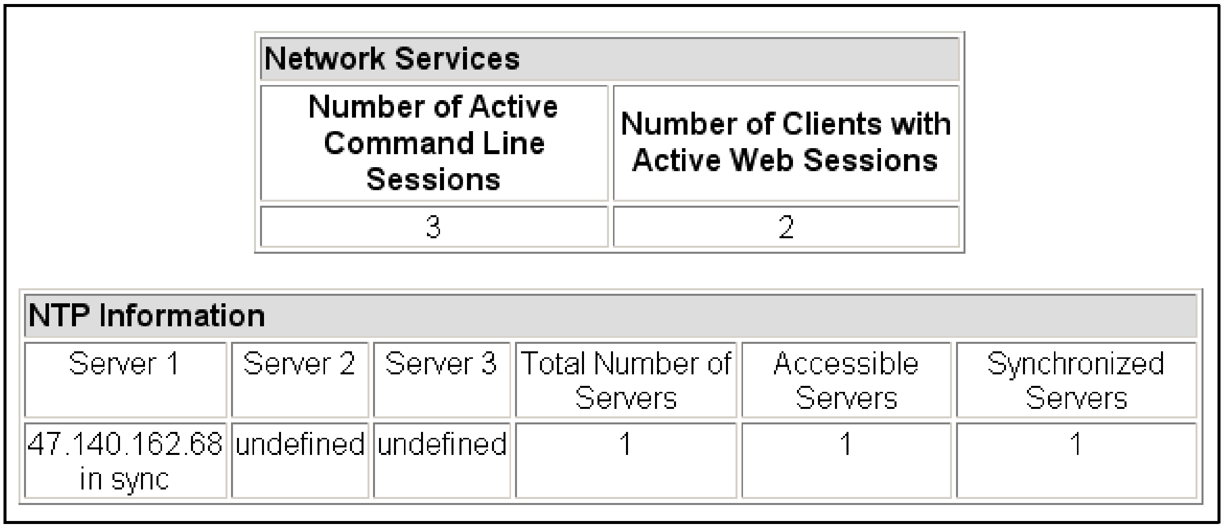
Field	Description
RAID Array Status: State	Indicates a high level state for the array: - “.”: indicates the array is functioning normally. - Missing: a disk was removed from the array. - Failed: a disk in the array has failed and needs to be replaced. - Rebuilding: the array is in the process of rebuilding to a fault-tolerant mode.
RAID Array Status: Disk 0	Indicates the service status of disk 0.
RAID Array Status: Disk 1	Indicates the service status of disk 1.
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)	Indicates the total capacity of the disk drive in gigabytes.
Disk Maintenance: Disk State	Indicates the installation state of the disk.
Disk Maintenance: Disk Action	Indicates whether a hard disk can be inserted into the operating system. For more information about the **Remove** and **Insert** commands, refer to the Session Server Upgrades NTP, NN10349-461.
Filesystem Information: Monitor	Indicates the status of individual filesystems on the disk array. For more information about the **Monitor** command, refer to procedures in the Configuration Management NTP, NN10338-511.
Filesystem Information: Filesystem Name	Indicates the name of the filesystem on the disk array. Some filesystem 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 filesystem operations are working on each of the filesystems.
Filesystem Information: Total Space (MB)	Indicates the total amount of disk space (in MB) allocated for this filesystem.

Field	Description
Filesystem Information: Total Space Used (MB)	Indicates the total amount of disk space (in MB) in use on this file system.
Filesystem Information: Total Space Used (%)	Indicates the total amount of disk space (in %) in use on this file system.
Filesystem Information: Total Space Available (MB)	Indicates the percent of total disk space (in MB) free for use on this filesystem.
Filesystem Information: Total Space Available (%)	Indicates the amount of disk space (in %) available for use by platform processes and applications.
Filesystem Information: Minor Alarm Threshold (%)	Indicates the maximum amount of disk space (in %) that can be utilized before a minor alarm is raised indicating that the set threshold has been exceeded.
Filesystem Information: Major Alarm Threshold (%)	Indicates the maximum amount of disk space (in %) that can be utilized before a major alarm is raised indicating that the set threshold has been exceeded.
Filesystem Information: Critical Alarm Threshold (%)	Indicates the maximum amount of disk space (in %) that can be utilized before a critical alarm is raised indicating that the set threshold has been exceeded.
Volume Group Information: Volume Group Name	Indicates the name of the volume group in the array.
Volume Group Information: Volume Group Size (GB)	Indicates the total size of the volume group in the array.
Volume Group Information: Total Space Allocated (GB)	Indicates the amount of volume group space, in gigabytes, currently allocated to filesystems.
Volume Group Information: Total Space Allocated (%)	Indicates the amount of volume group space (in %) currently allocated to filesystems.
Volume Group Information: Total Space Available (GB)	Indicates the amount of unallocated volume group space, in gigabytes, available for filesystems.
Volume Group Information: Total Space Available (%)	Indicates the amount of unallocated volume group space (in %) available for filesystems.

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:

> ***Note:*** 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
3	2

NTP Information

Server 1	Server 2	Server 3	Total Number of Servers	Accessible Servers	Synchronized Servers
47.140.162.68 in sync	undefined	undefined	1	1	1

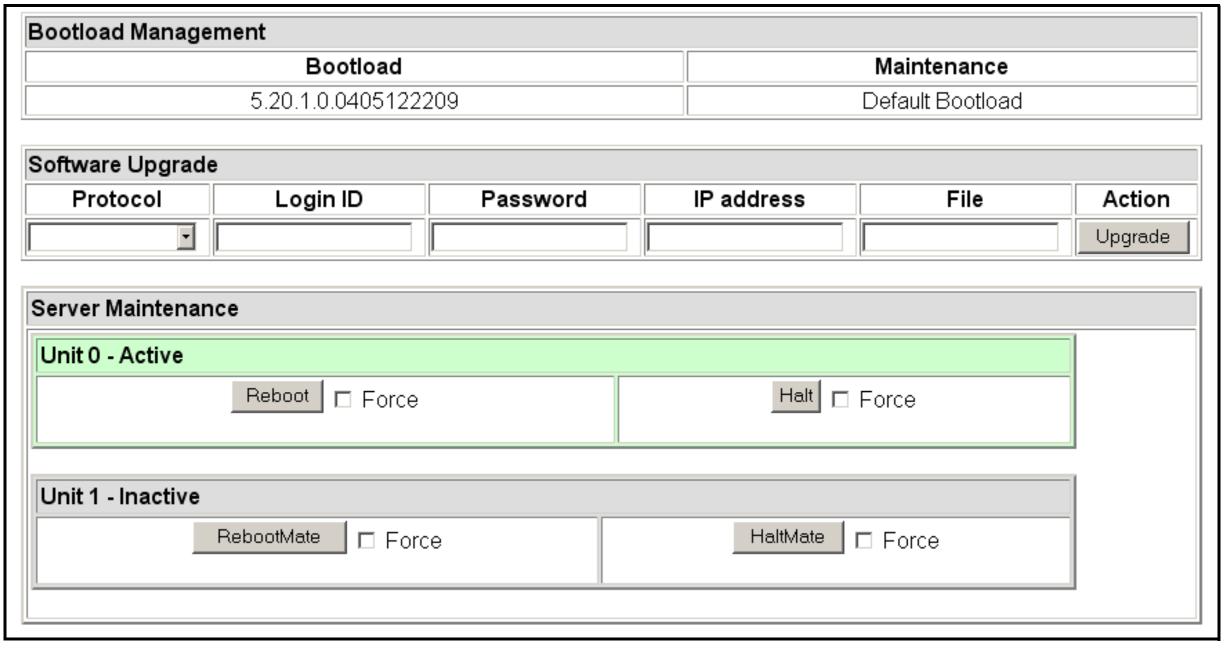
Field	Description
Network Services: Number of Active Command Line Sessions	Indicates the number of command line interface (CLI) sessions (both remote and local) on the Session Server.
Network Services: Number of Clients with Active Web Sessions	Indicates the number of clients running one or more web GUI sessions.
NTP Information: Server1 - Server 3	Indicates the 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	Indicates the number of NTP servers registered with the CS-LAN network.
NTP Information: Accessible Servers	Indicates the number of NTP servers accessible to the Session Server.
NTP Information: Synchronized Servers	Indicates the number of NTP servers to which the Session Server 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:

> ***Note:*** The Administration panel does not update automatically. Click the link again to update it.

> **ATTENTION**
> To perform software upgrades to the NCGL platform, refer to the Session Server Upgrades NTP, NN1010349-461.



Bootload Management

Bootload	Maintenance
5.20.1.0.0405122209	Default Bootload

Software Upgrade

Protocol	Login ID	Password	IP address	File	Action
					Upgrade

Server Maintenance

Unit 0 - Active

Unit 1 - Inactive

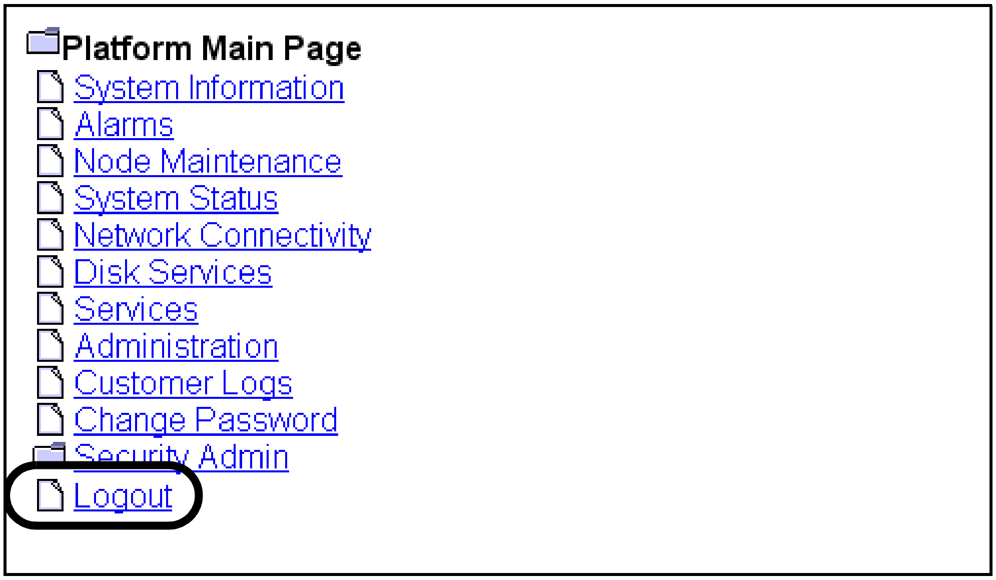
Field	Description
Bootload Management: Bootload	Indicates the load ID for the NCGL platform software load.
Bootload Management: Maintenance	Indicates whether the Bootload is the default. May also allow choosing a new default bootload if there is more than one load available. Additional loads can come from maintenance releases.

Field	Description
Software Upgrade: Protocol	Indicates the file transfer protocol or source location for the platform software upgrade: FTP, Anonymous FTP, HTTP, HTTPS, Local File, Local CDROM.
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.
Software Upgrade: File	The target upgrade load path and filename is entered here.
Software Upgrade: Action Upgrade button	The **Upgrade** button initiates a platform NCGL upgrade. Refer to the Session Server Upgrades NTP, NN10349-461, for instructions on using this function.
Server Maintenance (active and inactive units)	To execute the **Reboot**, **Halt**, **Rebootmate** and **Haltmate** functions, refer to the applicable procedures in the Session Server Security and Administration NTP, NN10346-611.

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 platform GUI, click the **Logout** button.

You are returned to the login page



17 The procedure is complete.

Lock the SIP Gateway application

Purpose of this procedure

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

> ***Note:*** For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section of the Session Server Security and Administration NTP, 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 Session Server platform, refer to procedure View the operational status of a Session Server NCGL platform on page 141.

> **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.

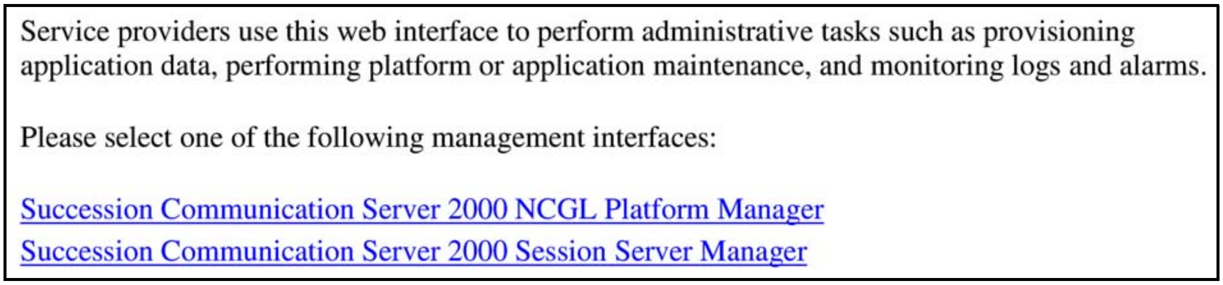
Prerequisites

There are no prerequisites for this procedure.

Action

At the Session Server GUI or Integrated EMS client

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

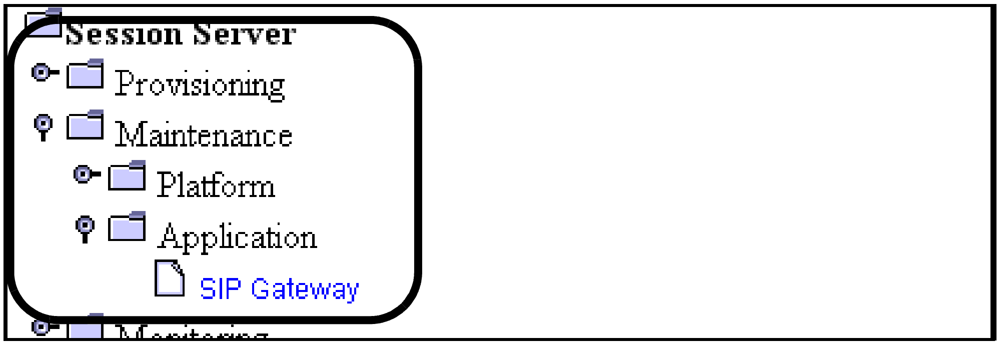


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

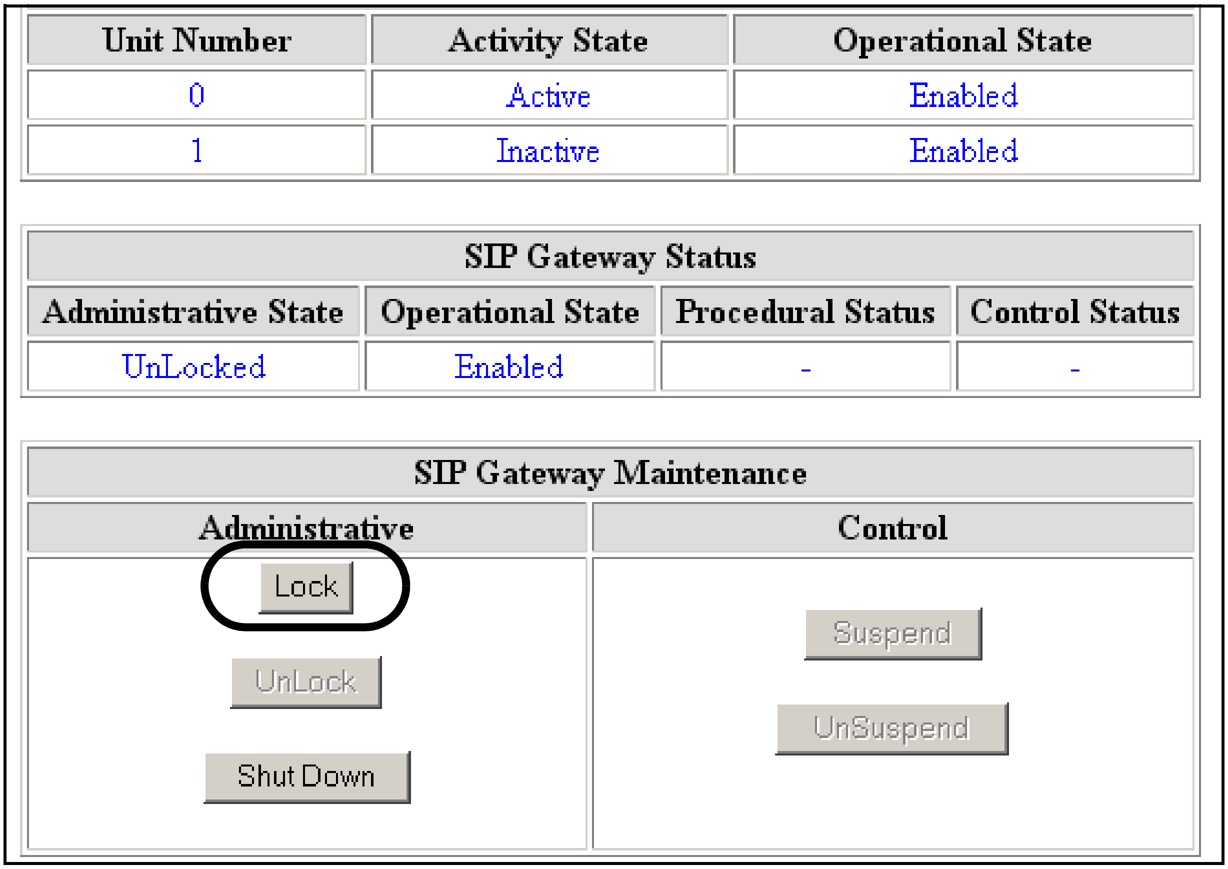
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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



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

4 In the SIP Gateway panel click the **Lock** button.



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	-	-

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?
```

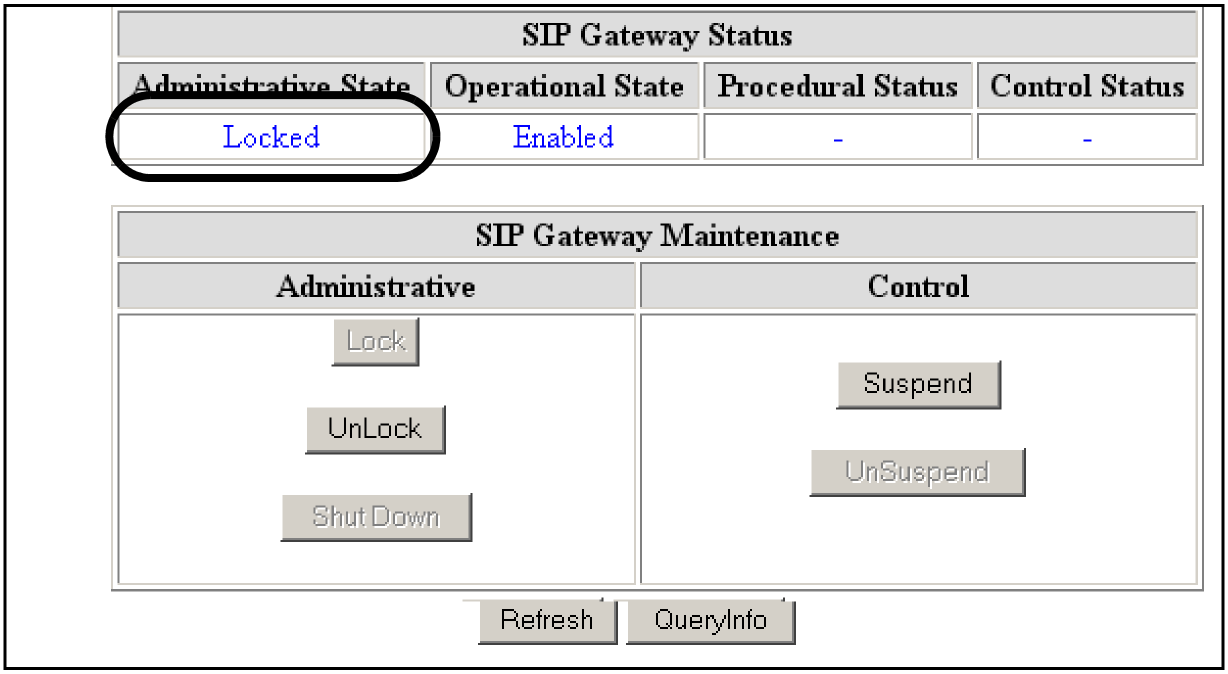
5 Click **OK** to confirm locking the SIP Gateway application.

CAUTION

Locking the SIP Gateway application releases all SIP calls in progress, regardless of call state, and causes an outage of all SIP media communications.

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

- the Administrative State changes to **Locked**



SIP Gateway Status

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

Note: 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.

7 The procedure is complete.

Unlock 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 callP to begin.

> ***Note:*** For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section of the Session Server Security and Administration NTP, 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 Session Server platform, refer to procedure View the operational status of a Session Server NCGL platform on page 141.

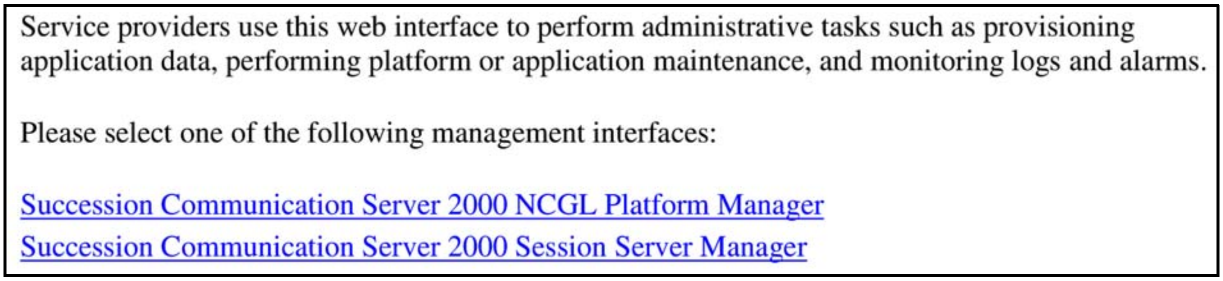
Prerequisites

The active Session Server 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 Lock the SIP Gateway application on page 160.

Action

At the Session Server GUI or Integrated EMS client

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



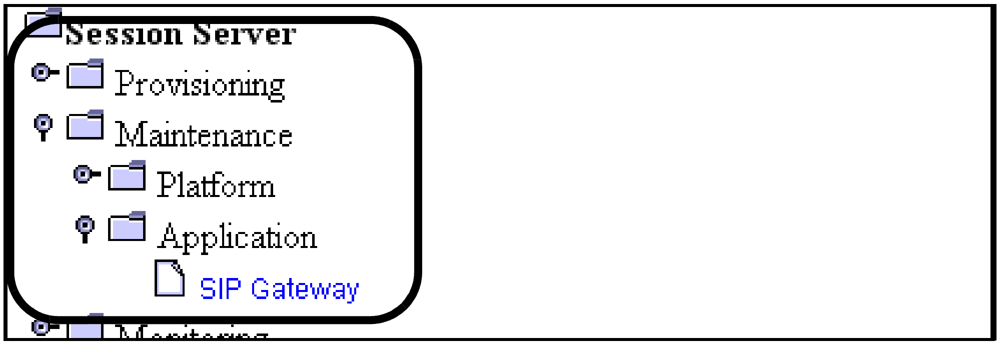
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager

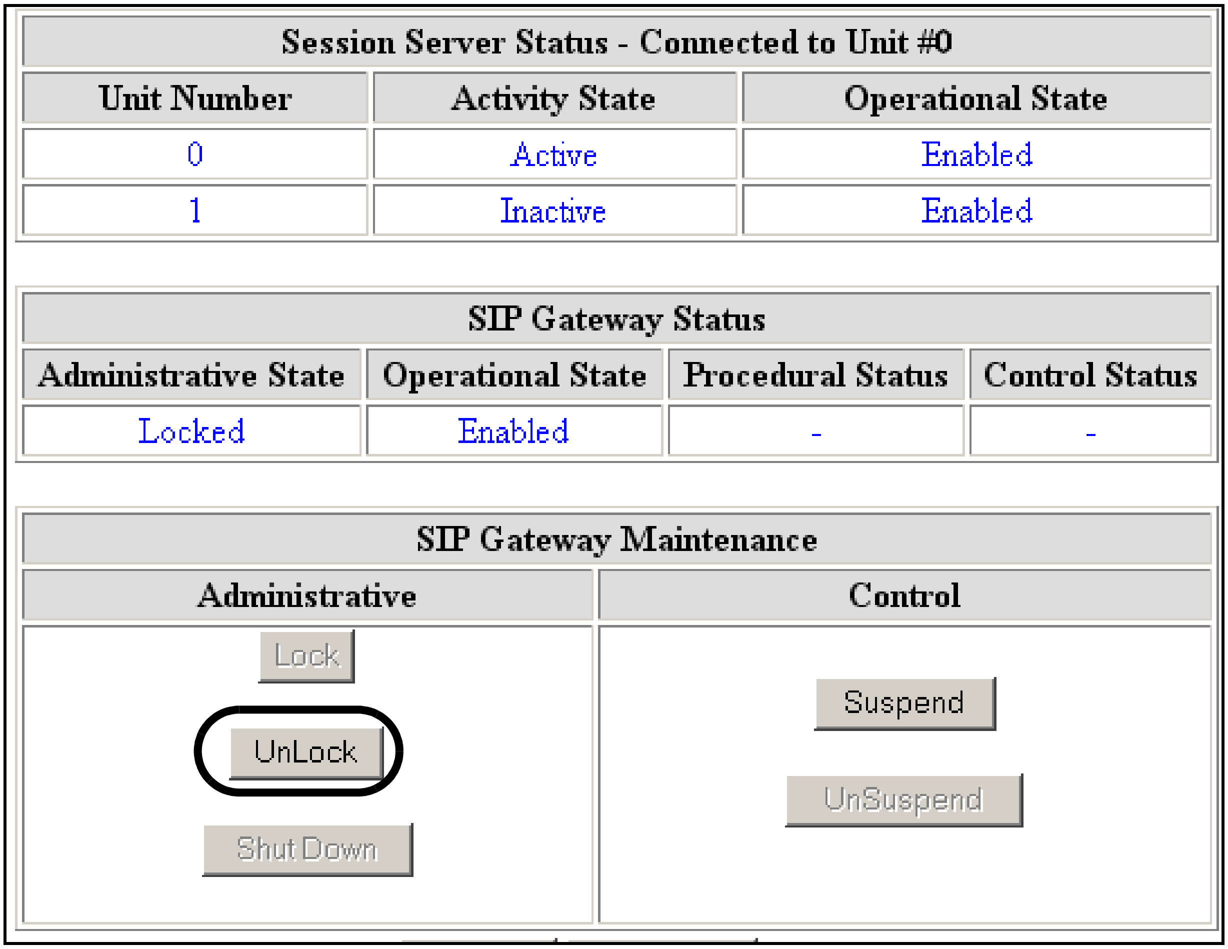
Succession Communication Server 2000 Session Server Manager

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



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

4 In the SIP Gateway panel click the **Unlock** button.



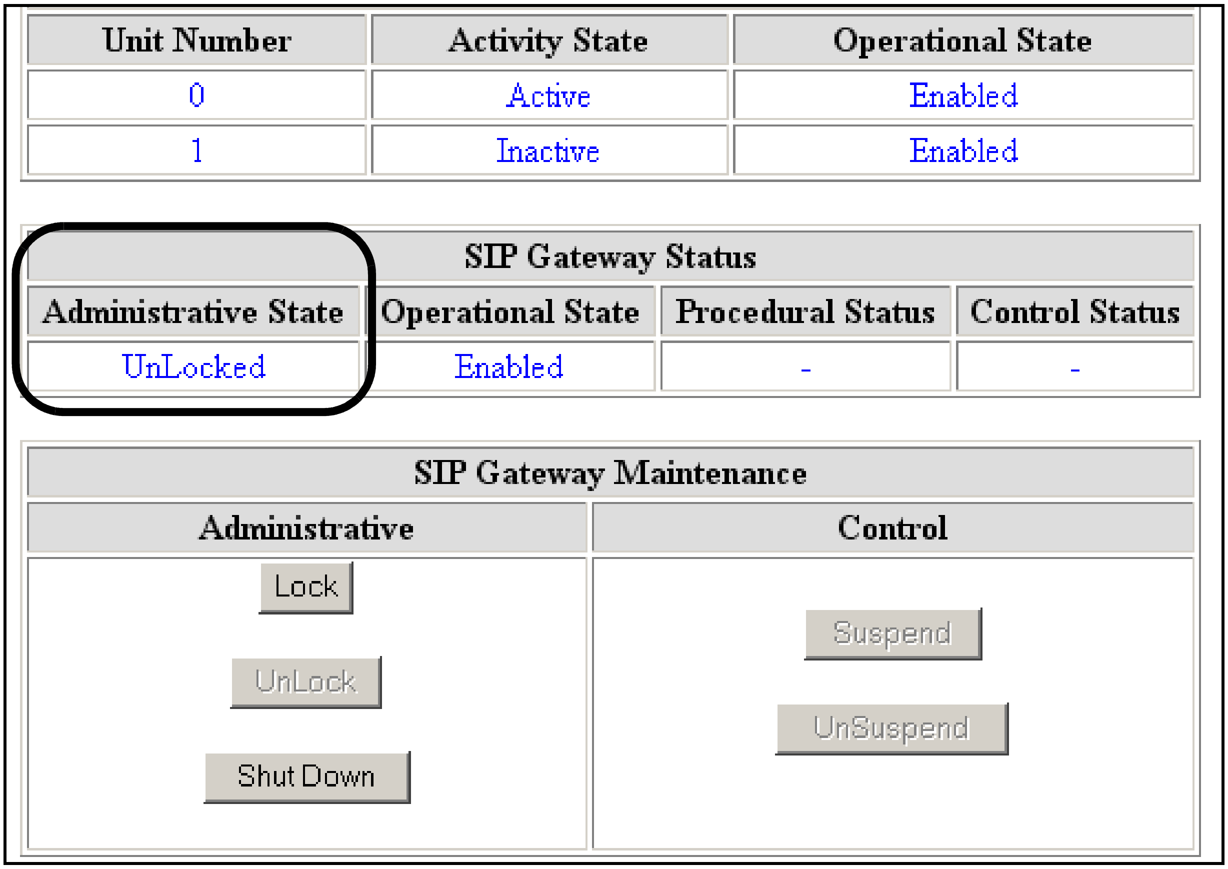
Session Server Status - Connected to Unit #0		
Unit Number	Activity State	Operational State
0	Active	Enabled
1	Inactive	Enabled

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

SIP Gateway Maintenance	
Administrative	Control

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

- 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	-	-

Note: 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 The procedure is complete.

Suspend 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.

> ***Note:*** For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section *Interpreting SIP Gateway application states* in the Session Server Security and Administration NTP, 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**

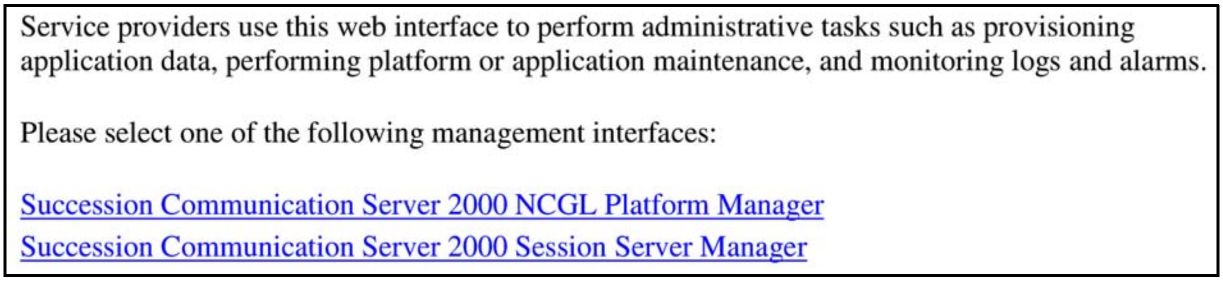
Prerequisites

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 Lock the SIP Gateway application on page 160.

Action

At the Session Server GUI or Integrated EMS client

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

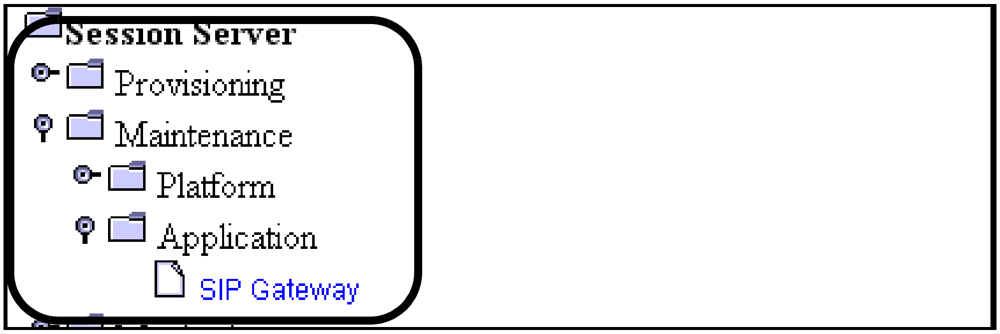


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

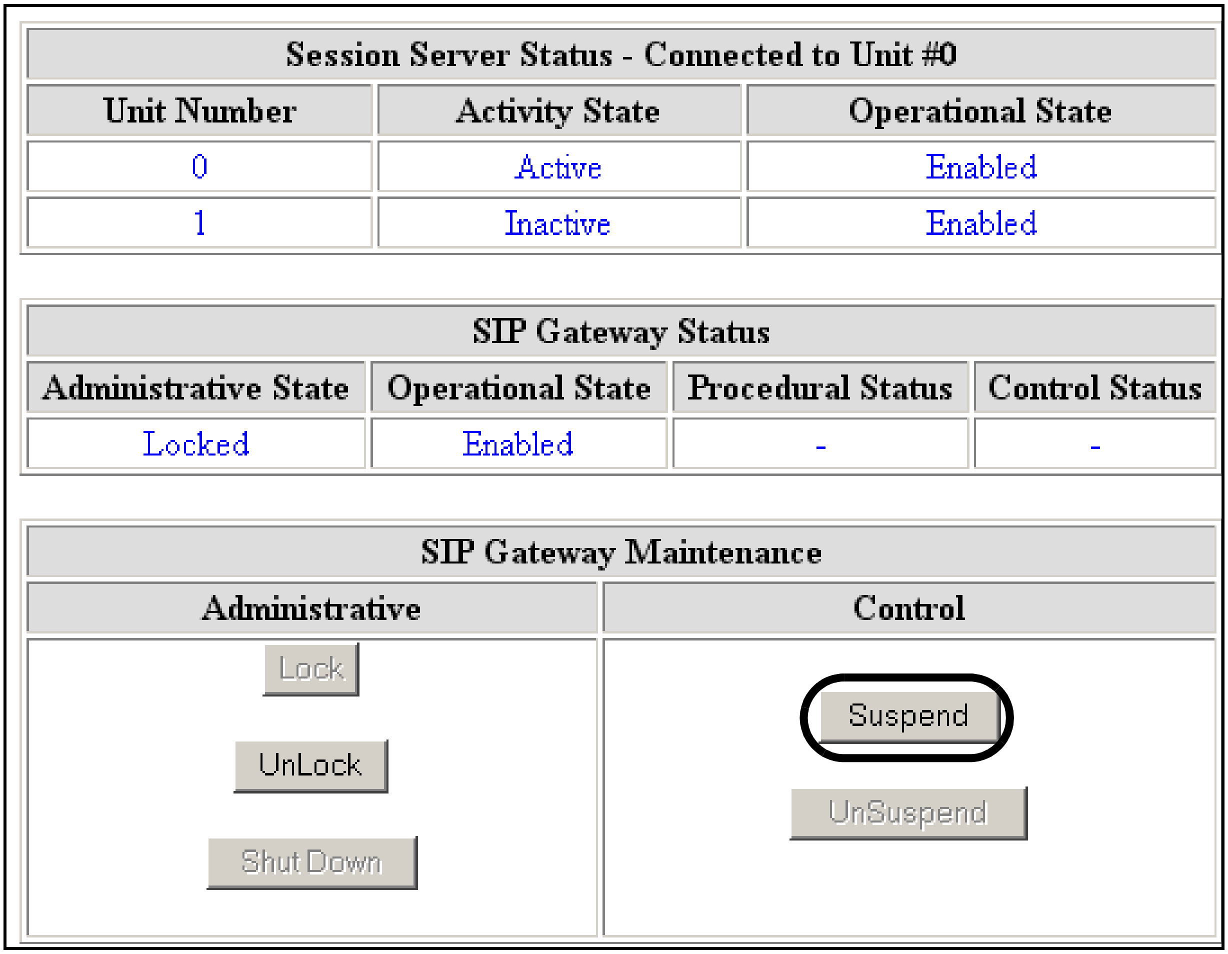
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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



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

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



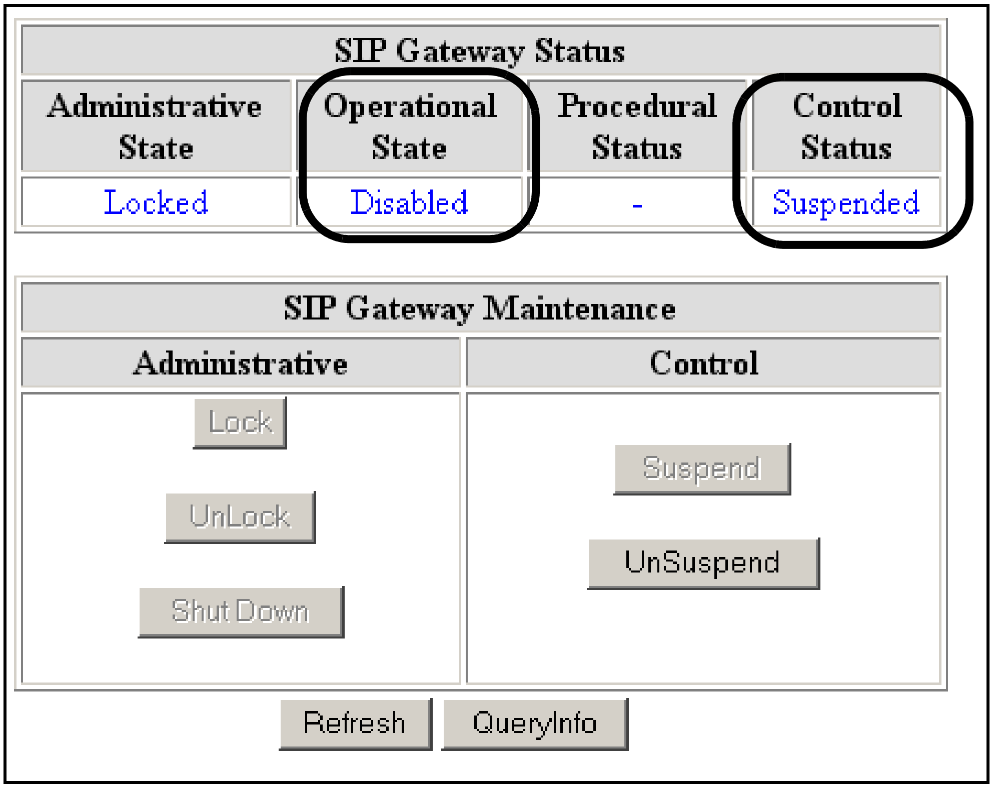
Session Server Status - Connected to Unit #0		
Unit Number	Activity State	Operational State
0	Active	Enabled
1	Inactive	Enabled

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

SIP Gateway Maintenance	
Administrative	Control
Lock UnLock Shut Down	Suspend UnSuspend

5 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**



SIP Gateway Status

Administrative State	Operational State	Procedural Status	Control Status
Locked	Disabled	-	Suspended

6 If applicable, restart the SIP Gateway application by executing procedures Unsuspend the SIP Gateway application on page 169 and Unlock the SIP Gateway application on page 163, in the order shown.

7 The procedure is complete.

Unsuspend 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.

> ***Note:*** For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section *Interpreting SIP Gateway application states,* in the Session Server Security and Administration NTP, 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**

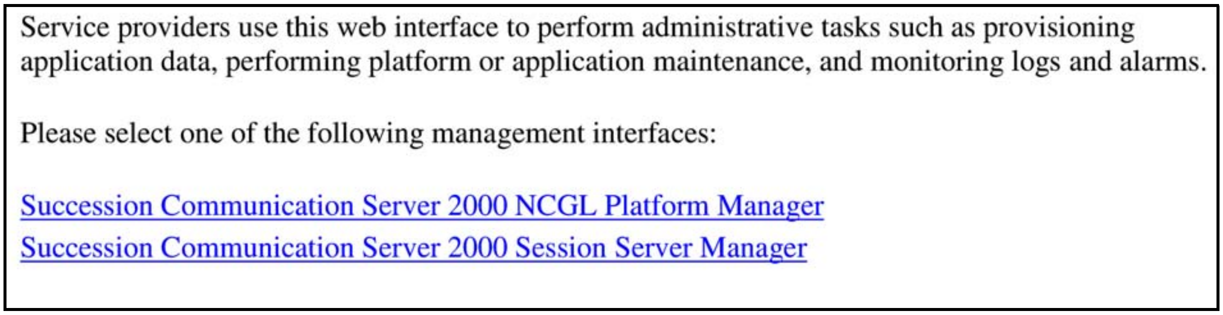
Prerequisites

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 Suspend the SIP Gateway application on page 166.

Action

At the Session Server GUI or Integrated EMS client

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

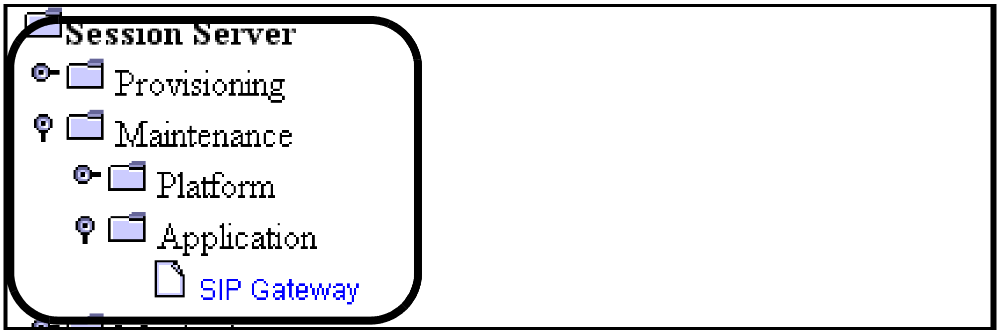


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

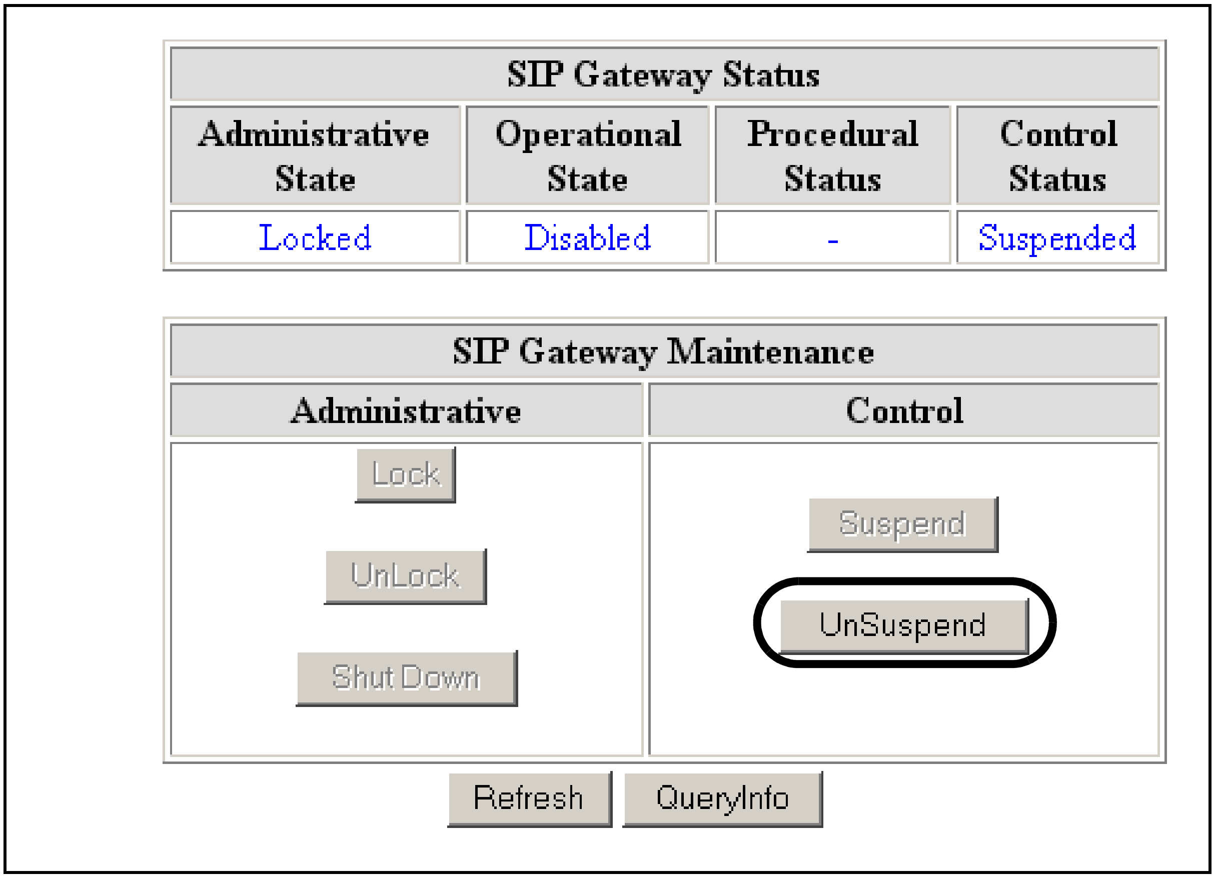
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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



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

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

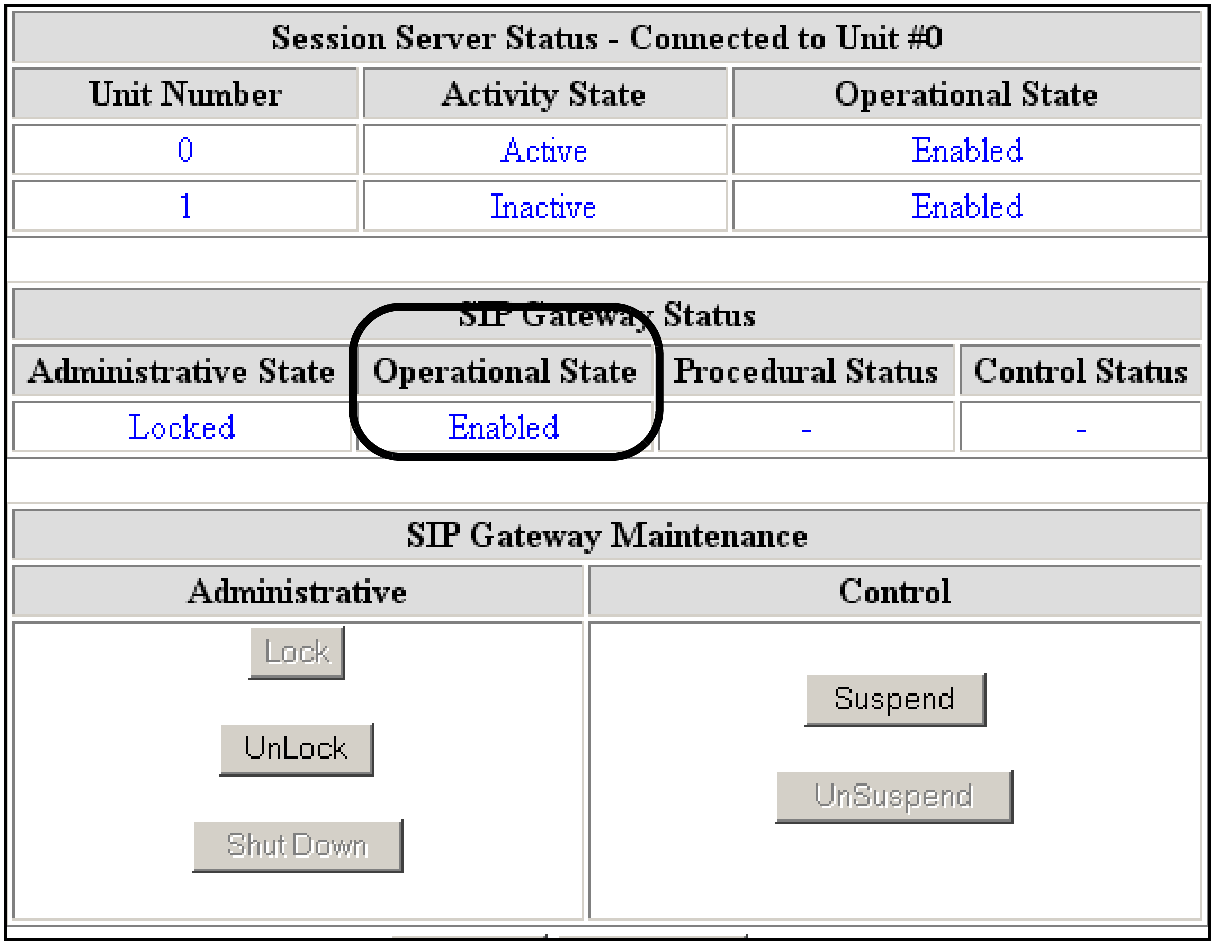


SIP Gateway Status

Administrative State	Operational State	Procedural Status	Control Status
Locked	Disabled	-	Suspended

5 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 **-**



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

6 If necessary, bring the SIP Gateway application back into service by executing procedure Unlock the SIP Gateway application on page 163.

7 The procedure is complete.

Modify 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 Session Server.

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 Management 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 Management NTP applicable to your solution.

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 Modify Session Server maximum DPT call limits on page 173 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.

3 The procedure is complete.

Modify Session Server 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 Session Server.

- 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

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 Configure SIP Gateway application parameters on page 44 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.

3 The procedure is complete.

Add a Session Server node to the SSPFS server web proxy

Purpose of this procedure

Use the following activity to add web proxy services to the SSPFS server, (part of the CS 2000 Management Tools server) for supporting a Session Server node or to replace an existing web proxy entry for a Session Server 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 ATM/IP Solution-level Configuration Management NTP, 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 tagnames for an existing Session Server 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.

Refer to section Understanding Session Server node IP addressing on page 10 for more information about Session Server 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

At the applicable network element interface

1 Verify that an HTTPS Certificate has been installed on the CS 2000 Management Tools Server SSPFS platform. For assistance use procedure *Installing an HTTPS certificate on a Sun server* found in the IP Solution Upgrades NTP, NN10344-450/IP or the Solution level Security and Administration NTP, NN10402-600.

2 Log onto the CS 2000 Management Tools server and complete the following sub-steps to add the Session Server node to the proxy. If needed, you can refer to procedure *Configuring the Apache Web Server for HTTPS proxy*, in the ATM/IP Solution-level Configuration Management NTP, NN10409-500, for assistance.

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.

> ***Note:*** For the port number, use “443”.

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.

Note: For the port number, use “443”.

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.

Note: For the port number, use “443”.

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.

> ***Note:*** 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.

> ***Note:*** 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.

Note: 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 SSPFS operating system.

13 Exit the Configuration level by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

14 Exit the CLI by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

15 If applicable, logout from the workstation.

At a Session Server command line interface (CLI)

16 Use procedure Modify NCGL platform provisioning on page 205, found in this NTP to configure the SNMP trap IP address and the web proxy IP address of the Integrated EMS server on the Session Server.

17 The procedure is complete.

Using multiple tag names for multiple Session Server nodes

Starting in SN08, multiple Session Server 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 Session Server 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 Session Server. The use of unique tag names allows multiple Session Server 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/**	

View web proxy settings in SSPFS for Session Server

Purpose of this procedure

Use the following activity to view the configuration of existing Session Server node web proxy services on the SSPFS server (part of the CS 2000 Management Tools server). This procedure may be used as a standalone task or as part of a higher level activity such as a major upgrade activity.

Limitations and restrictions

If the web proxy entry for a particular Session Server 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 Session Server node to the proxy service configuration. To perform this activity, refer to procedure *Add a Session Server node to the SSPFS server web proxy*, found in the Session Server Configuration NTP, NN10338-511.

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.

Refer to section *Understanding Session Server IP addressing*, found in the Session Server Configuration NTP, NN10338-511, for more information about Session Server 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)

If necessary, refer to procedure *Configuring the Apache Web Server for HTTPS proxy*, in the ATM/IP Solution-level Configuration Management NTP, NN10409-500, for assistance.

Action

At the Session Server CLI or Integrated EMS client

1 Verify that a security certificate has been installed on the CS 2000 Management Tools Server SSPFS platform. For assistance use procedure *Installing an HTTPS certificate on a Sun server* found in the NTP, Carrier Voice over IP Network Upgrade Overview, NN10440-450.

2 Log onto the CS 2000 Management Tools server. If necessary, refer to procedure *Configuring the Apache Web Server for HTTPS proxy*, in the ATM/IP Solution-level Configuration Management NTP, NN10409-500, for assistance.

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 List the current Apache Proxy Configuration entries by typing

3

and pressing the Enter key.

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 GUI used by the CS 2000 Session Server Manager GUI. 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 Session Server active unit.

ATTENTION

If necessary, please refer to section Selecting and using tag names in SN08 and beyond on page 188 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 Session Server node when you installed or upgrading it.

11 Exit the Apache Proxy Configuration level by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

12 Exit the Configuration level by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

13 Exit the CLI by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

14 If applicable, logout from the workstation.

Selecting and using tag names in SN08 and beyond

Tag names for the active Session Server unit GUI 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 Session Server GUIs after the SSPFS web proxy services restart.

ATTENTION

If you are upgrading fromSN07, or rolling back to SN07, the SSPFS web proxy server must be using the “prov” tag name.

If the remote tag name for a Session Server 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. To perform this activity, refer to procedure *Add a Session Server node to the SSPFS server web proxy*, found in the Session Server Configuration NTP, NN10338-511.

Reconfigure the Session Server BIOS

Purpose of this procedure

Use the following procedure to make changes to the BIOS settings on the Session Server platform hardware, when you have replaced the Session Server 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 Session Server units. BIOS settings for both units must match.

Limitations and restrictions

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

ATTENTION

Do not use this procedure on an active Session Server unit.

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

Prerequisites

Verify that there are no active alarms on the active Session Server unit.

CAUTION

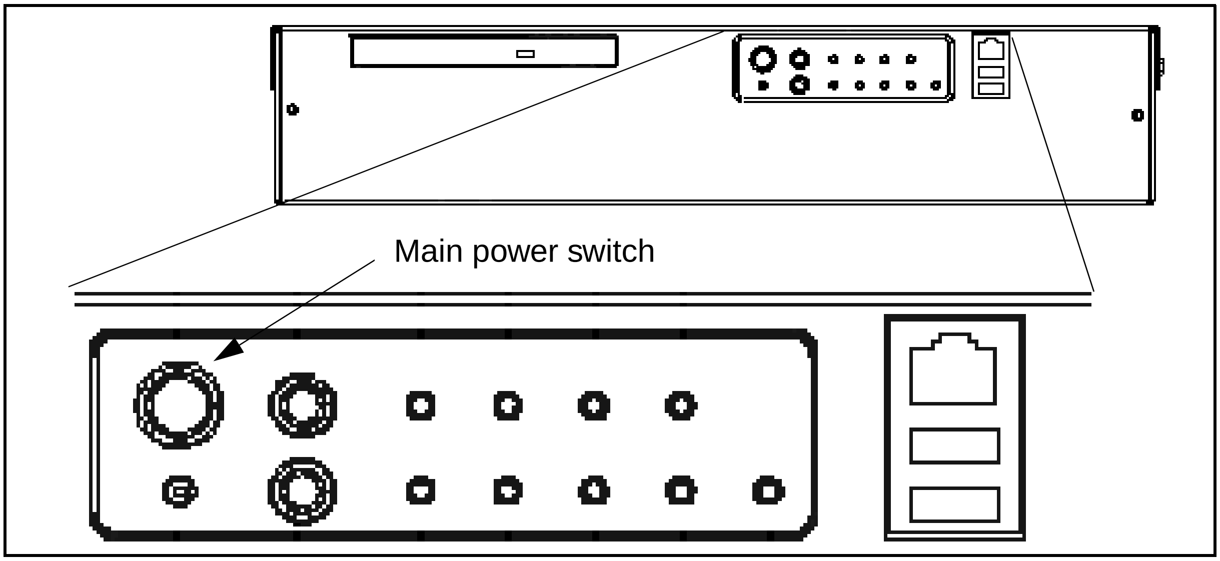
Performing this procedure on a Session Server node performing call processing temporarily affects fault-tolerant capability and overall system performance while the affected unit is offline.

Action

At the Session Server console

1 If necessary, refer to procedure Attach a VT-100 console monitor to the RJ-45 serial port on page 16 or Attach a VGA monitor and keyboard console on page 18 to ensure that you have a console interface connected to the rear of the Session Server you are reprovisioning. Your site may support other connection options.

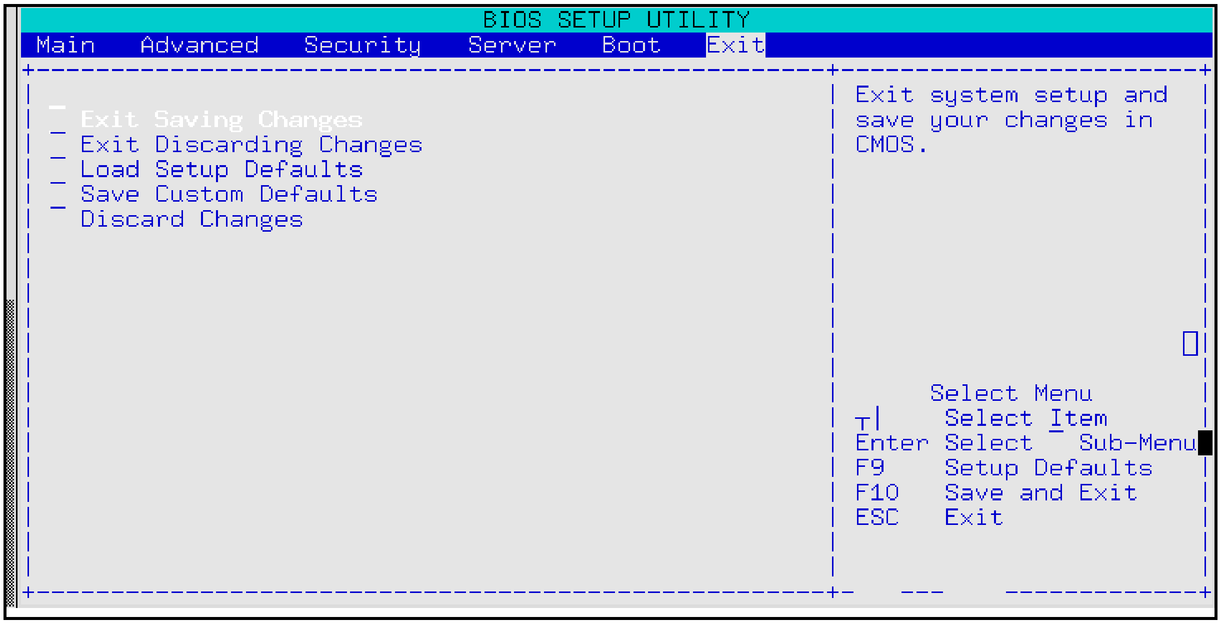
2 If necessary, power on the Session Server using the main power switch located on the front panel, as shown in the following figure.



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.



```
                          BIOS SETUP UTILITY
 Main   Advanced   Security   Server   Boot   Exit
+------------------------------------------------------+------------------------+
|                                                      | Exit system setup and  |
|  Exit Saving Changes                                 | save your changes in   |
|  Exit Discarding Changes                             | CMOS.                  |
|  Load Setup Defaults                                 |                        |
|  Save Custom Defaults                                |                        |
|  Discard Changes                                     |                        |
|                                                      |                        |
|                                                      |      Select Menu       |
|                                                      | T|     Select Item      |
|                                                      | Enter Select   Sub-Menu|
|                                                      | F9     Setup Defaults  |
|                                                      | F10    Save and Exit   |
|                                                      | ESC    Exit            |
|                                                      |                        |
+------------------------------------------------------+-   ---    -------------+
```

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**

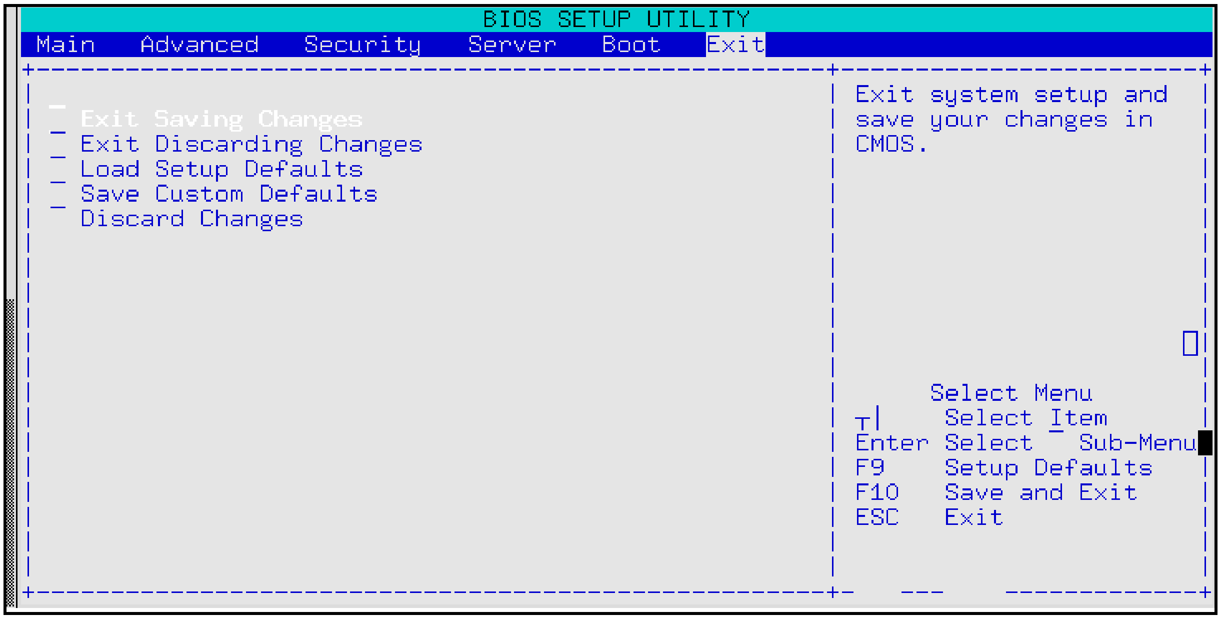
3rd/4th Boot Device: **Disabled**

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.



```
                              BIOS SETUP UTILITY
 Main    Advanced    Security    Server    Boot    Exit
+--------------------------------------------------------+-------------------------+
|                                                        | Exit system setup and   |
|  _ Exit Saving Changes                                 | save your changes in    |
|  _ Exit Discarding Changes                             | CMOS.                   |
|  _ Load Setup Defaults                                 |                         |
|  _ Save Custom Defaults                                |                         |
|    Discard Changes                                     |                         |
|                                                        |      Select Menu        |
|                                                        | ↑↓     Select Item      |
|                                                        | Enter  Select   Sub-Menu|
|                                                        | F9     Setup Defaults   |
|                                                        | F10    Save and Exit    |
|                                                        | ESC    Exit             |
+--------------------------------------------------------+-------------------------+
```

The Session Server unit resets and begins to boot.

14 Once the unit has rebooted, use procedure View the operational status of a Session Server NCGL platform on page 141 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.

16 The procedure is complete.

Reprovision the Session Server NCGL platform software

Purpose of this procedure

Use this procedure when you need to reinstall the Session Server platform software from the NCGL 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 Session Server installation.

If the Session Server 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 procedure Reconfigure the Session Server BIOS on page 189 to ensure that the Boot Device Priority is set so that the DVD/CDROM drive is accessed before the hard drive for booting.

Action

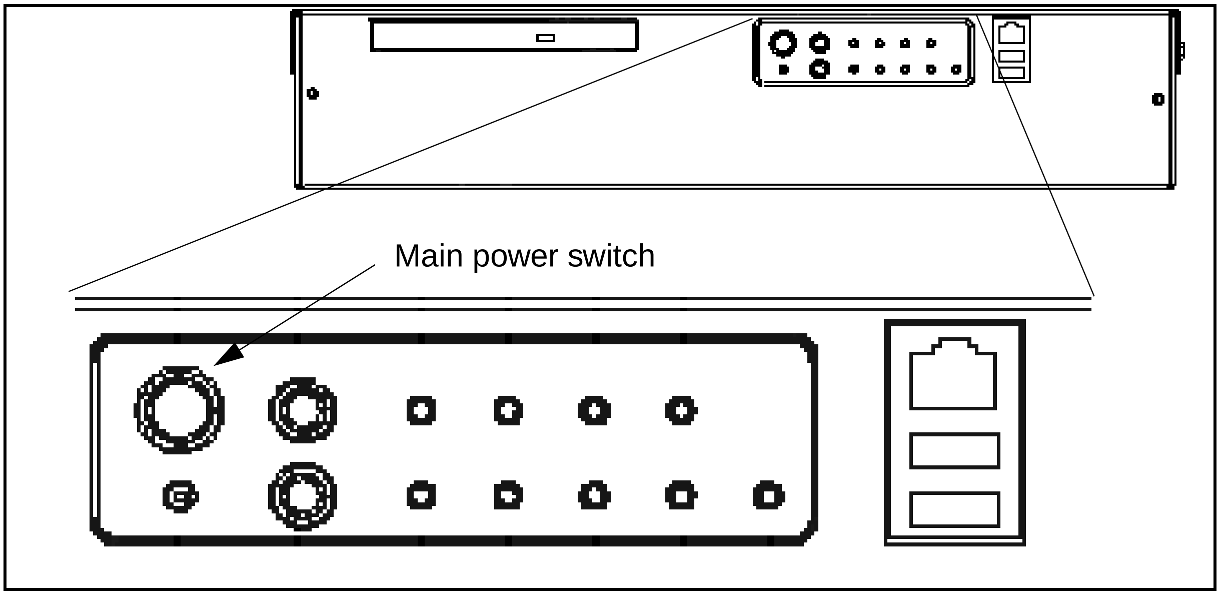
At the Session Server Serial Console

1 If necessary, refer to procedure Attach a VT-100 console monitor to the RJ-45 serial port on page 16 to ensure that you have a console interface connected to the rear of the Session Server you are reprovisioning. Your site may support other connection options. Do not use a VGA console to complete this procedure.

2 If the standby Session Server unit is still operating, shut it down using procedure *Halt (shutdown) a Session Server unit*, found in the Session Server Security and Administration NTP, NN10346-611.

Note: This procedure does not power-off the unit.

3 If necessary, power-off the Session Server using the main power switch located on the front panel.



4 Power-on the Session Server 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:

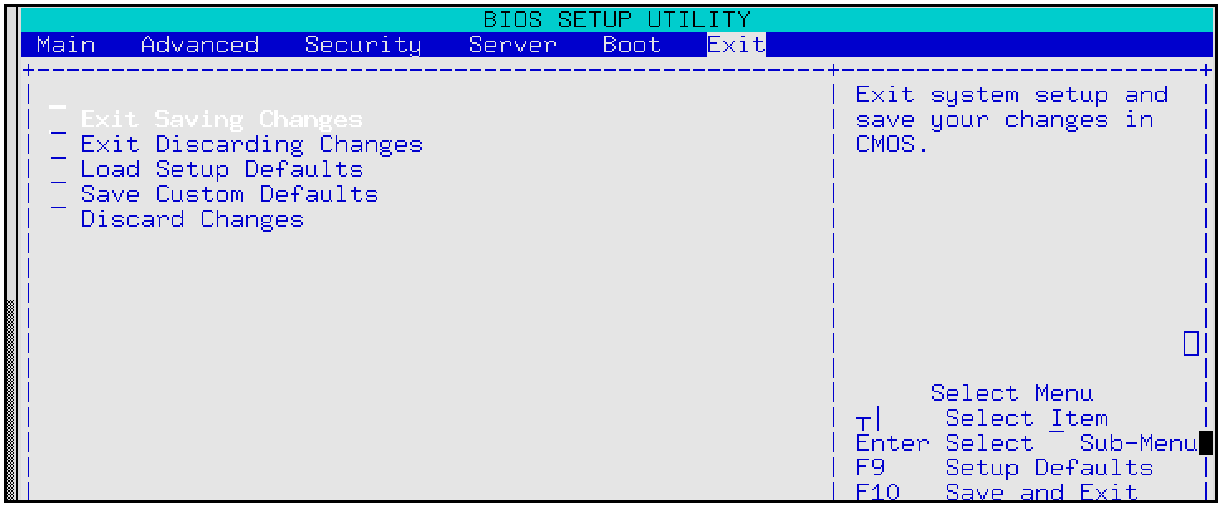
1st Boot Device: ATAPI CD-ROM (the DVD-Rom drive)

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**.



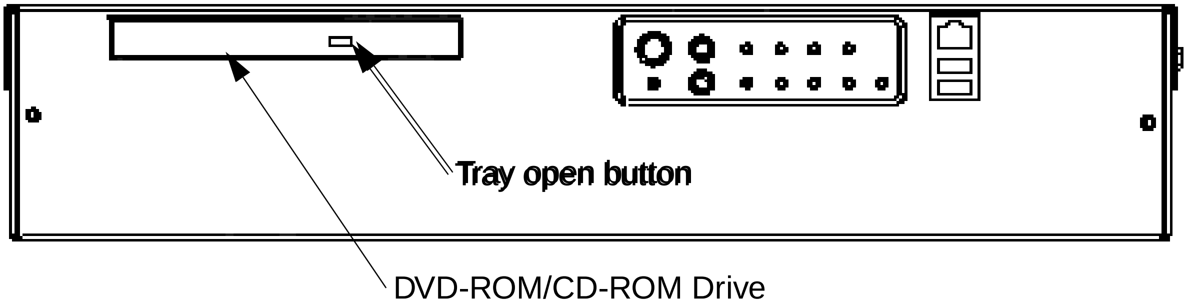
```
                              BIOS SETUP UTILITY
 Main     Advanced     Security     Server     Boot     Exit
+-------------------------------------------------------+-------------------------+
|                                                       | Exit system setup and   |
| _ Exit Saving Changes                                 | save your changes in    |
| _ Exit Discarding Changes                             | CMOS.                   |
| _ Load Setup Defaults                                 |                         |
| _ Save Custom Defaults                                |                         |
|   Discard Changes                                     |                         |
|                                                       |                         |
|                                                       |                         |
|                                                       |                         |
|                                                       |                         |
|                                                       |      Select Menu        |
|                                                       | T|    Select Item        |
|                                                       | Enter Select  Sub-Menu  |
|                                                       | F9    Setup Defaults    |
|                                                       | F10   Save and Exit     |
```

11 Type **Yes** in confirmation dialog box.

The Session Server resets and begins to boot.

12 Immediately press the tray open button on the DVD-ROM and insert the NCGL CD/DVD disk into the DVD-ROM drive.

Session Server Unit Front Panel



13 At the boot prompt, you have 5 seconds to quickly type **NUKE** and press **Enter**.

CAUTION

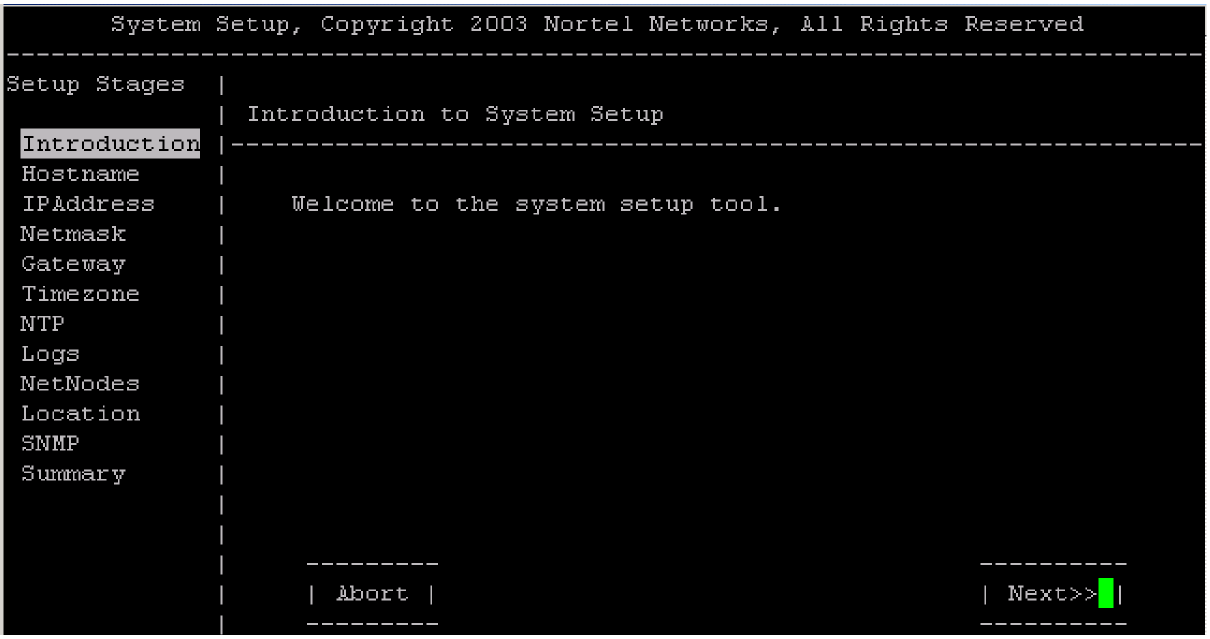
The NUKE command completely erases the drive and initiates a reboot from the CD/DVD disk.

Once the Boot prompt appears, only 5 seconds are given to type NUKE before the Server 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 Session Server completes the boot-up process, the NCGL system setup tool is displayed.

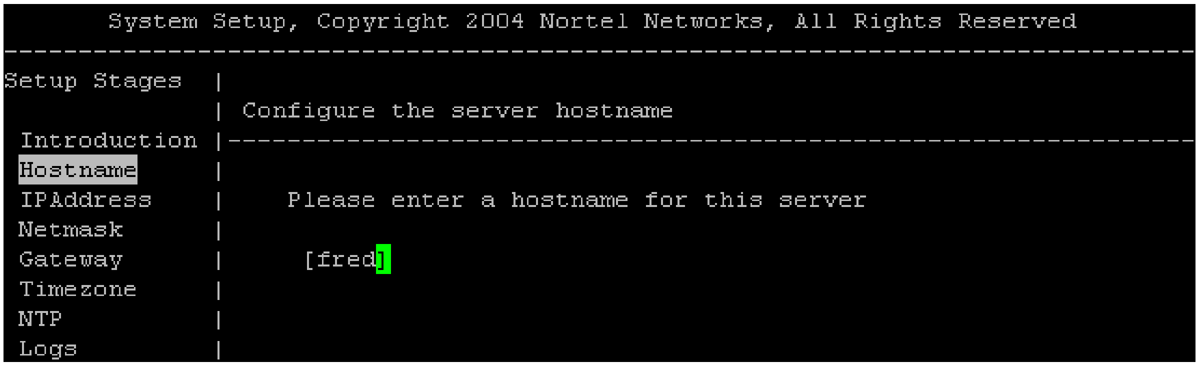


```
       System Setup, Copyright 2003 Nortel Networks, All Rights Reserved
-------------------------------------------------------------------------------
Setup Stages   |
               |  Introduction to System Setup
 Introduction  |----------------------------------------------------------------
 Hostname      |
 IPAddress     |     Welcome to the system setup tool.
 Netmask       |
 Gateway       |
 Timezone      |
 NTP           |
 Logs          |
 NetNodes      |
 Location      |
 SNMP          |
 Summary       |
               |
               |
               |      ---------                                      ----------
               |      | Abort |                                      | Next>> |
               |      ---------                                      ----------
```

15 Position the cursor on the Next button and press **Enter**.

> ***Note:*** 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.

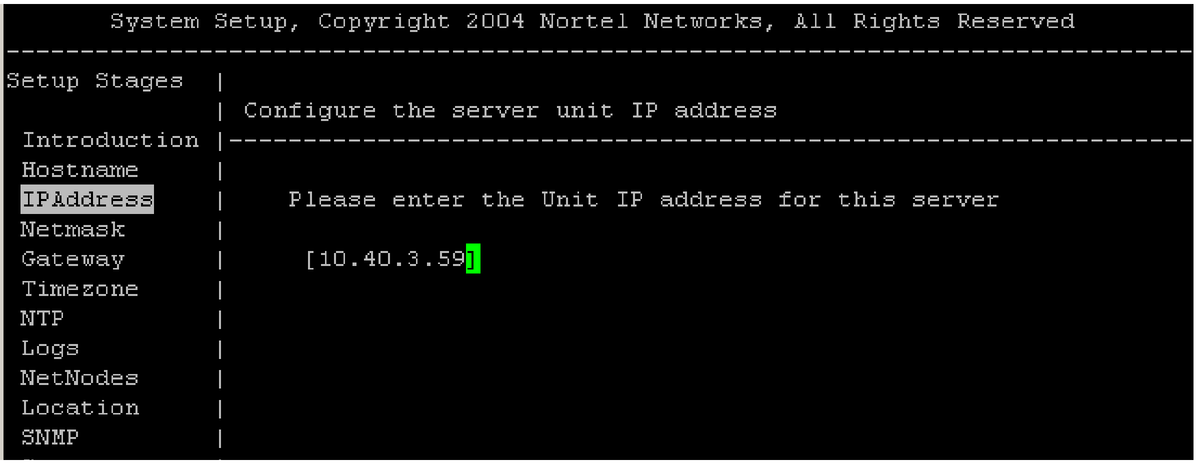


```
      System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server hostname
 Introduction |----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter a hostname for this server
 Netmask      |
 Gateway      |     [fred]
 Timezone     |
 NTP          |
 Logs         |
```

16 If applicable, enter a hostname for this Session Server 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.



```
      System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server unit IP address
 Introduction |----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter the Unit IP address for this server
 Netmask      |
 Gateway      |     [10.40.3.59]
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
 SNMP         |
```

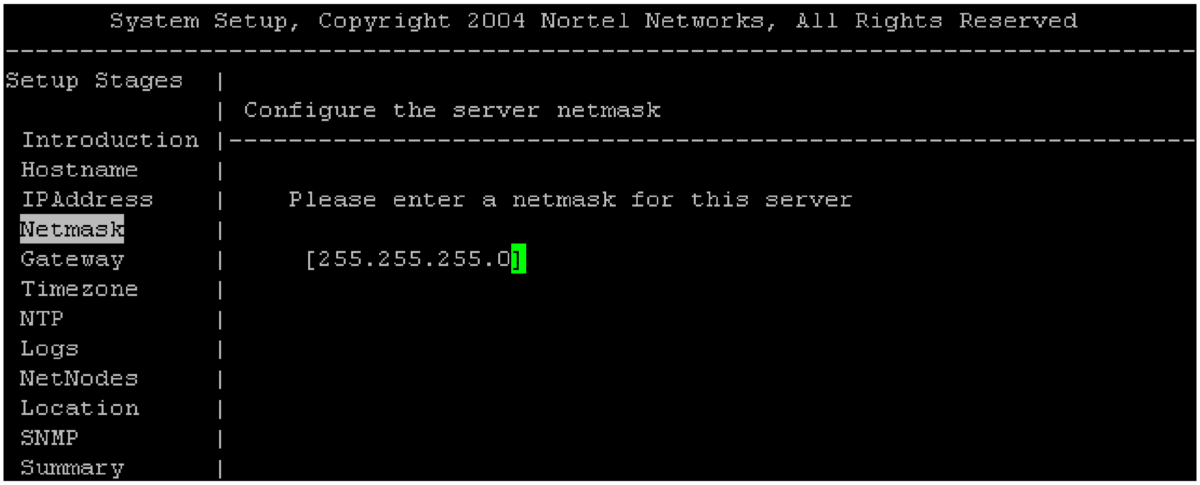
18 If applicable, enter an IP address for this Session Server in the following format:

`10.40.102.112`

> ***Note:*** Refer to section Session Server configuration on page 6 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.



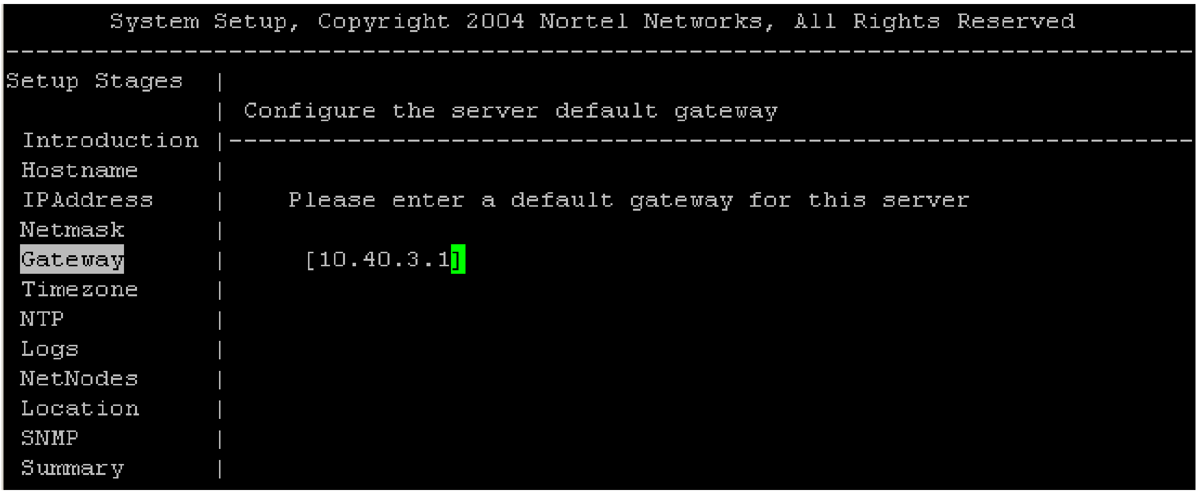
```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the server netmask
 Introduction |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please enter a netmask for this server
 Netmask       |
 Gateway       |     [255.255.255.0]
 Timezone      |
 NTP           |
 Logs          |
 NetNodes      |
 Location      |
 SNMP          |
 Summary       |
```

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.

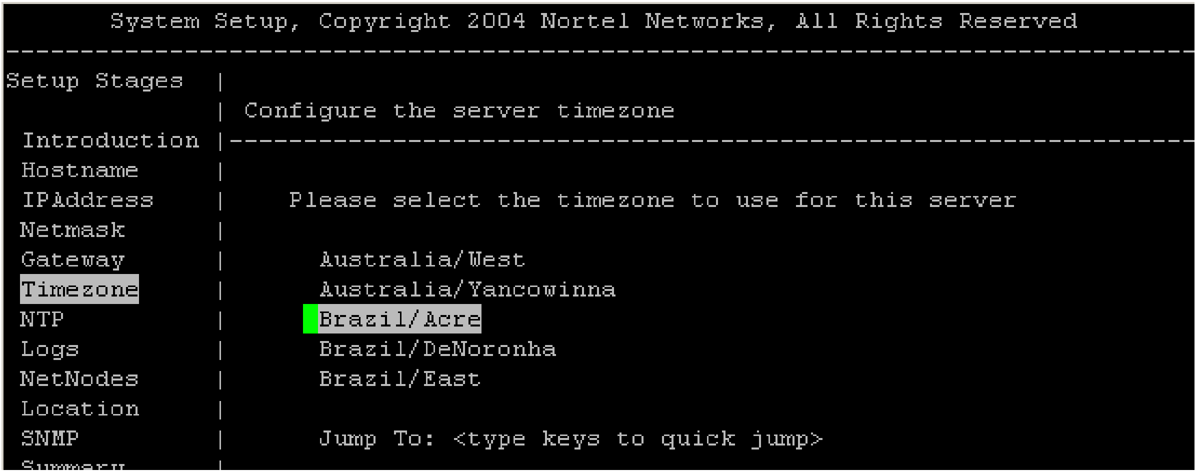


```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the server default gateway
 Introduction |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please enter a default gateway for this server
 Netmask       |
 Gateway       |     [10.40.3.1]
 Timezone      |
 NTP           |
 Logs          |
 NetNodes      |
 Location      |
 SNMP          |
 Summary       |
```

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.



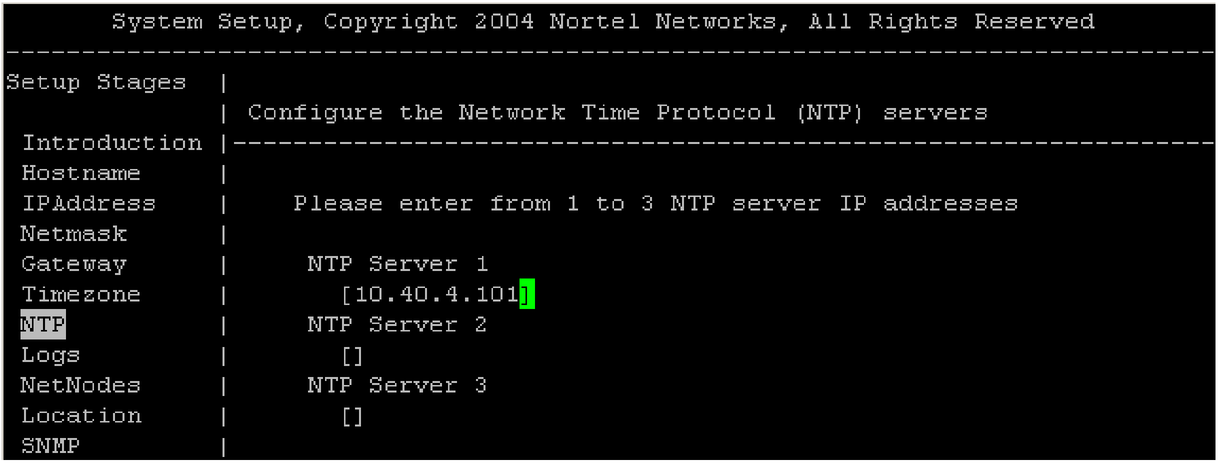
```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the server timezone
 Introduction  |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please select the timezone to use for this server
 Netmask       |
 Gateway       |      Australia/West
 Timezone      |      Australia/Yancowinna
 NTP           |      Brazil/Acre
 Logs          |      Brazil/DeNoronha
 NetNodes      |      Brazil/East
 Location      |
 SNMP          |      Jump To: <type keys to quick jump>
 Summary       |
```

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.

Note: 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.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the Network Time Protocol (NTP) servers
 Introduction  |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please enter from 1 to 3 NTP server IP addresses
 Netmask       |
 Gateway       |     NTP Server 1
 Timezone      |       [10.40.4.101]
 NTP           |     NTP Server 2
 Logs          |       []
 NetNodes      |     NTP Server 3
 Location      |       []
 SNMP          |
```

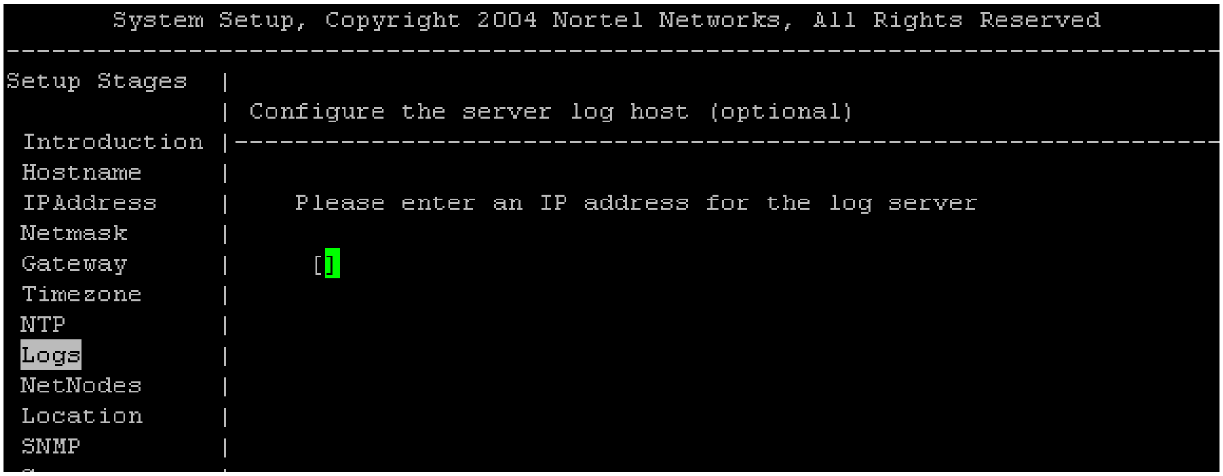
26 If applicable, enter the IP address of at least 1 (up to a maximum of 3) network time protocol servers in the following format:

`10.40.102.112`

> ***Note:*** 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.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the server log host (optional)
 Introduction  |----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please enter an IP address for the log server
 Netmask       |
 Gateway       |      []
 Timezone      |
 NTP           |
 Logs          |
 NetNodes      |
 Location      |
 SNMP          |
```

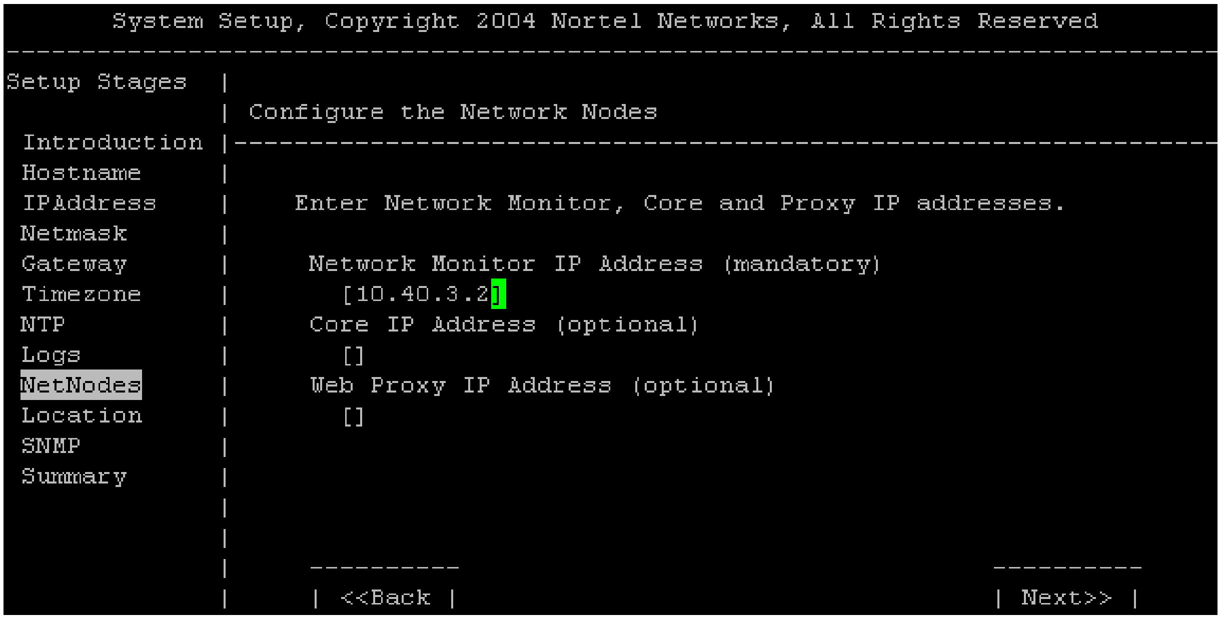
28 Enter the IP address of the log server in the following format:

`192.168.102.112`

> ***Note:*** 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.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the Network Nodes
 Introduction |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Enter Network Monitor, Core and Proxy IP addresses.
 Netmask       |
 Gateway       |     Network Monitor IP Address (mandatory)
 Timezone      |       [10.40.3.2]
 NTP           |     Core IP Address (optional)
 Logs          |       []
 NetNodes      |     Web Proxy IP Address (optional)
 Location      |       []
 SNMP          |
 Summary       |
               |
               |
               |     ----------                                    ----------
               |     | <<Back |                                    | Next>> |
```

30 Use the following sub-steps to complete the Network Nodes screen:

a For networks using sites using PP8600 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.

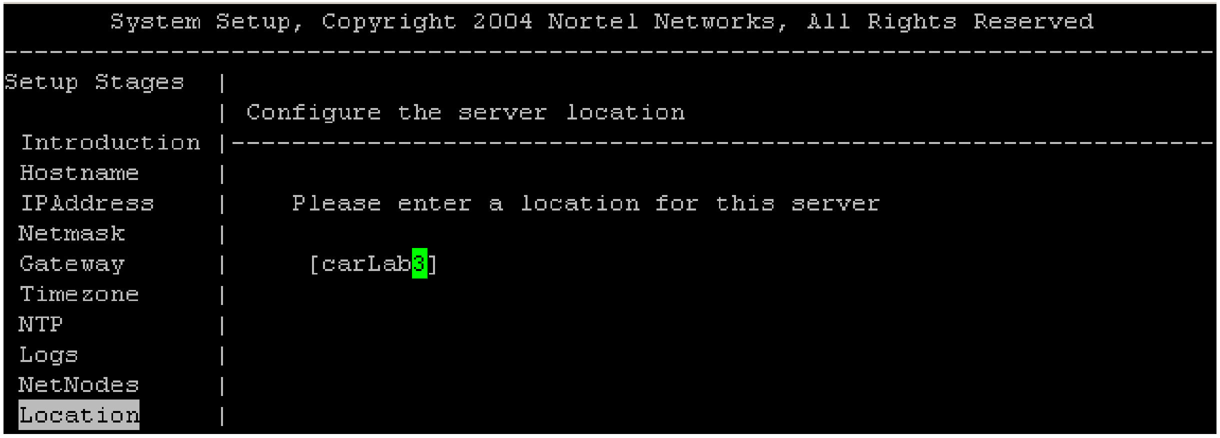
c Enter the IP address of the SSPFS server for the Web Proxy IP Address in the following format:

```
10.40.102.112
```

Note: Use the IP address of the SSPFS 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.

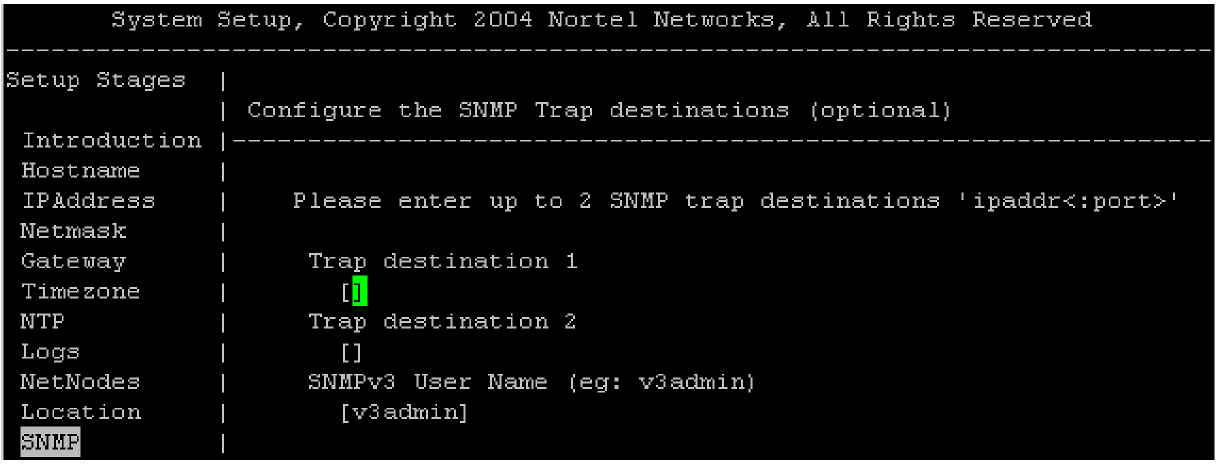


```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the server location
 Introduction |------------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please enter a location for this server
 Netmask       |
 Gateway       |      [carLab3]
 Timezone      |
 NTP           |
 Logs          |
 NetNodes      |
 Location      |
```

32 If applicable, enter a location identifier for this Session Server location.

33 Position the cursor on the **Next** button and press **Enter**.

The optional SNMP trap destinations page is displayed.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the SNMP Trap destinations (optional)
 Introduction |------------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please enter up to 2 SNMP trap destinations 'ipaddr<:port>'
 Netmask       |
 Gateway       |      Trap destination 1
 Timezone      |        []
 NTP           |      Trap destination 2
 Logs          |        []
 NetNodes      |      SNMPv3 User Name (eg: v3admin)
 Location      |        [v3admin]
 SNMP          |
```

34 If applicable, enter the IP address of the Integrated EMS server for Trap destination 1 in the following format:

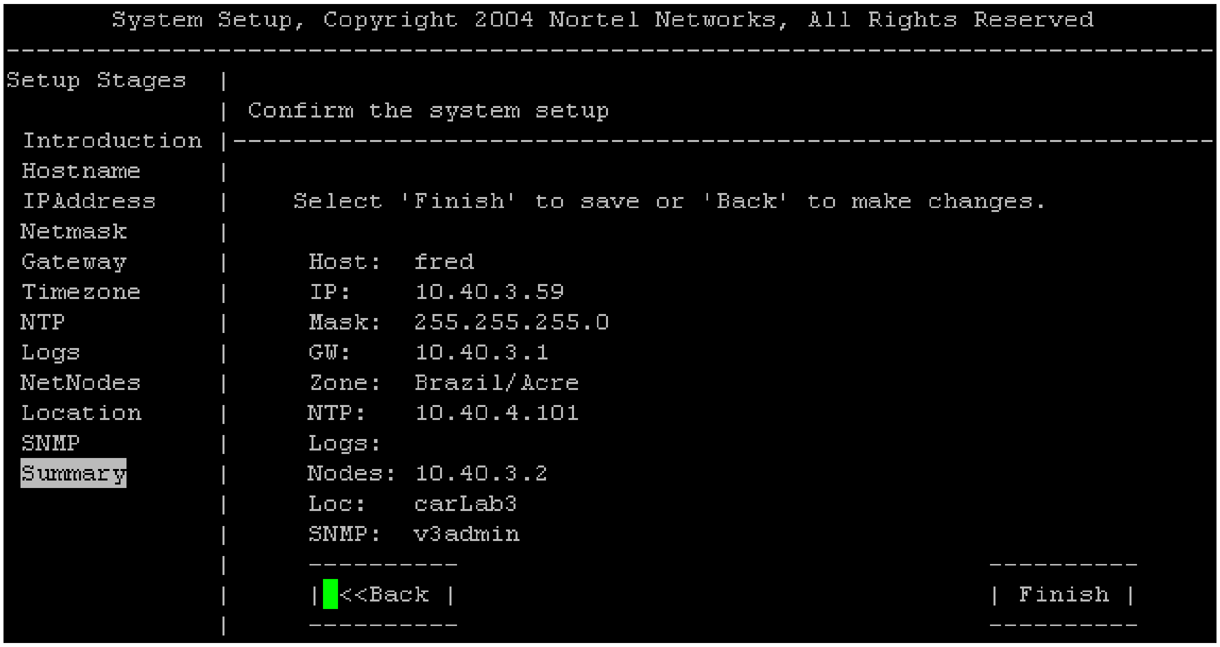
`10.40.102.112`

Note 1: Use the IP address of the Integrated EMS application residing on the CS 2000 Management Tools server.

Note 2: Do not enter values for the Trap destination2 and SNMPv3 User Name fields.

35 Position the cursor on the **Next** button and press **Enter**.

The summary screen is displayed



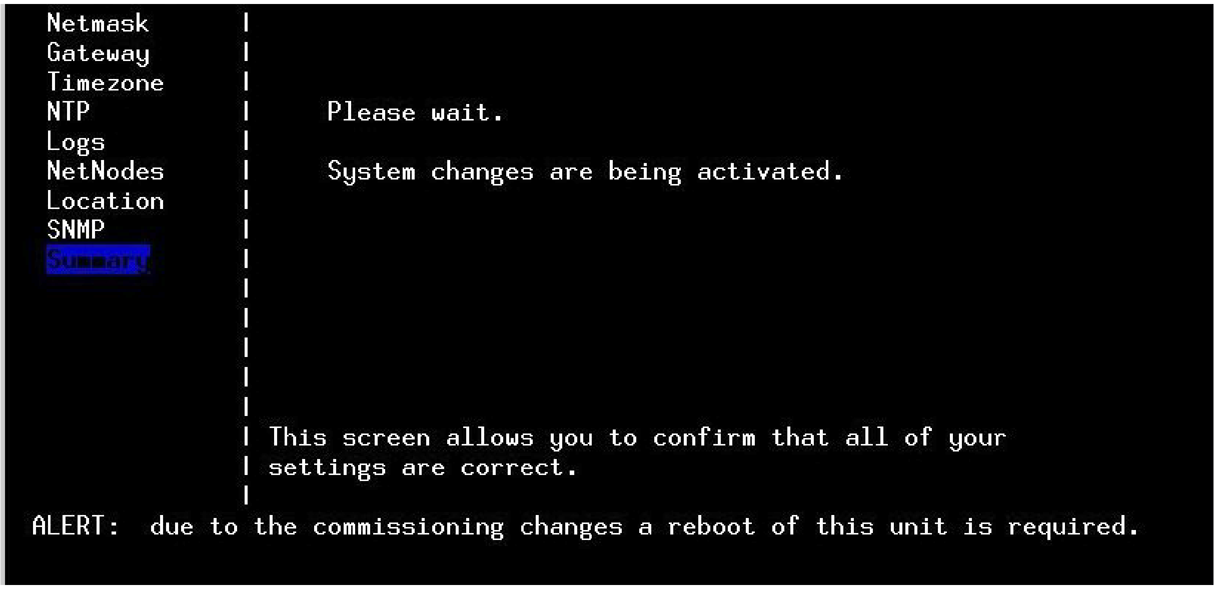
```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Confirm the system setup
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Select 'Finish' to save or 'Back' to make changes.
 Netmask      |
 Gateway      |     Host:  fred
 Timezone     |     IP:    10.40.3.59
 NTP          |     Mask:  255.255.255.0
 Logs         |     GW:    10.40.3.1
 NetNodes     |     Zone:  Brazil/Acre
 Location     |     NTP:   10.40.4.101
 SNMP         |     Logs:
 Summary      |     Nodes: 10.40.3.2
              |     Loc:   carLab3
              |     SNMP:  v3admin
              |     ----------                                   ----------
              |     | <<Back |                                   | Finish |
              |     ----------                                   ----------
```

36 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.

37 Position the cursor on the **Finish** button and press **Enter**.

The system configures itself based upon the supplied settings.

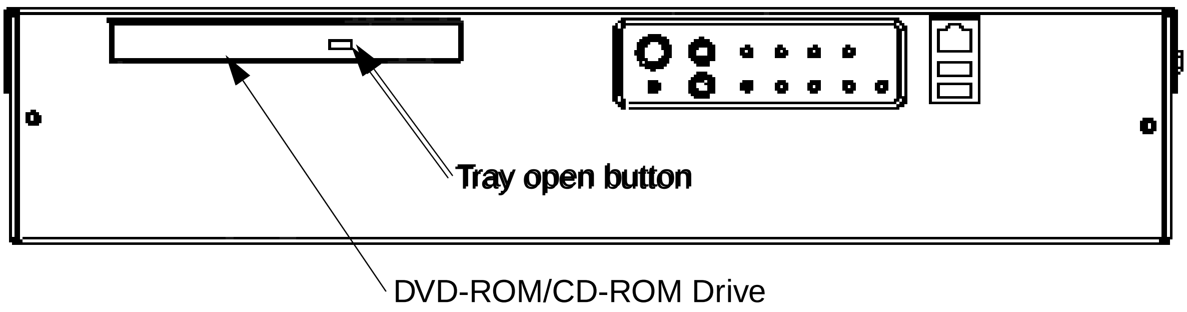
After this procedure is completed, the unit automatically reboots. Allow the unit to boot normally.



```
   Netmask      |
   Gateway      |
   Timezone     |
   NTP          |     Please wait.
   Logs         |
   NetNodes     |     System changes are being activated.
   Location     |
   SNMP         |
   Summary      |
                |
                |
                |
                |
                |
                | This screen allows you to confirm that all of your
                | settings are correct.
                |
 ALERT:  due to the commissioning changes a reboot of this unit is required.
```

38 Press the tray open button on the DVD-ROM drive and remove the NCGL CD/DVD disk.

Session Server Front Panel



39 Verify that the all of the commish settings made for this unit match those of the mate unit.

40 Remove the RJ45 serial cable from the unit. Failure to remove the cable may result in future software upgrade failure.

41 The procedure is complete.

Modify 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 of the Session Server
- change the hostname of the Session Server
- change the time zone setting for the Session Server
- 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 SSPFS web proxy server address
- change the IP addresses to allow access by the Integrated EMS

Limitations and restrictions

ATTENTION
This procedure must be performed on both Session Server units; however, because a reboot and SwAct of the Session Server units is required in order for changes made to take effect, you can only perform this procedure on the standby Session Server 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 Session Server unit must first be jammed using procedure *Inhibit a system SwAct (Jam)*, found in the Session Server Security and Administration, NN10346-611.

If necessary, refer to procedure Attach a VT-100 console monitor to the RJ-45 serial port on page 16 to connect a console interface to the rear of the Session Server for which you are modifying provisioning.

Action

At a Session Server command line interface (CLI)

1 Log onto the standby Session Server unit.

2 At the prompt change to the root user by typing

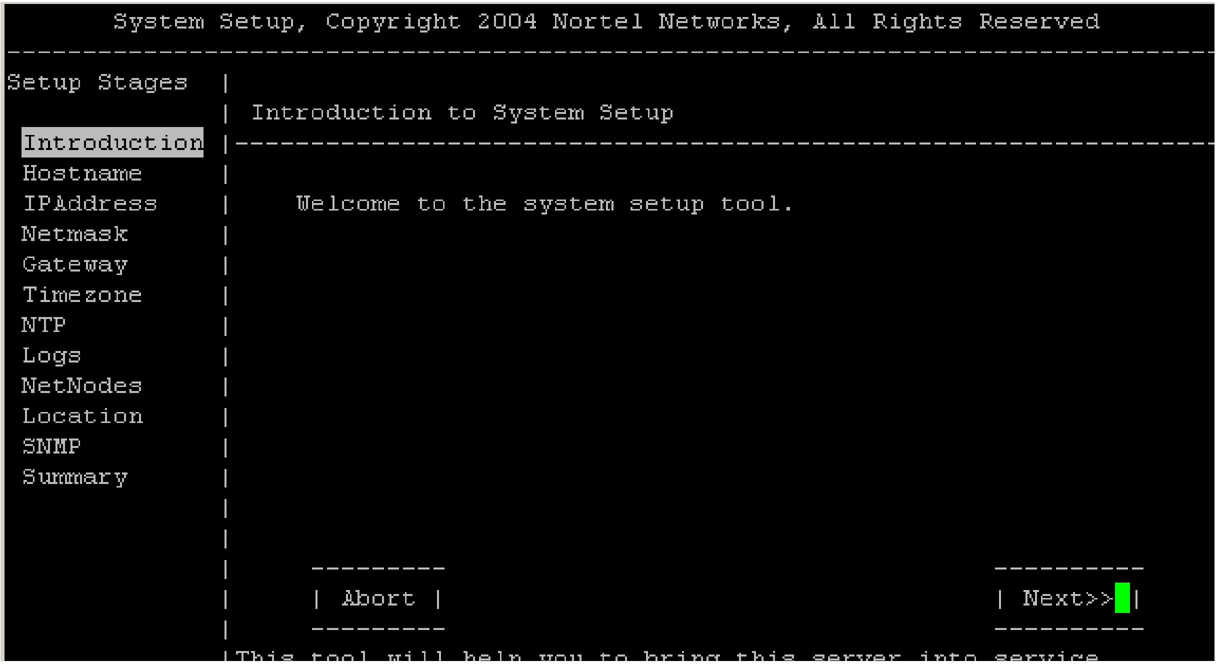
`$ su - root`

and pressing **Enter**.

3 Start the platform commissioning tool by typing

`commish`

After a few seconds the Introduction screen is displayed.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              |  Introduction to System Setup
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Welcome to the system setup tool.
 Netmask      |
 Gateway      |
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
 SNMP         |
 Summary      |
              |
              |
              |     ---------                                  -----------
              |     | Abort |                                  | Next>> |
              |     ---------                                  -----------
              |This tool will help you to bring this server into service
```

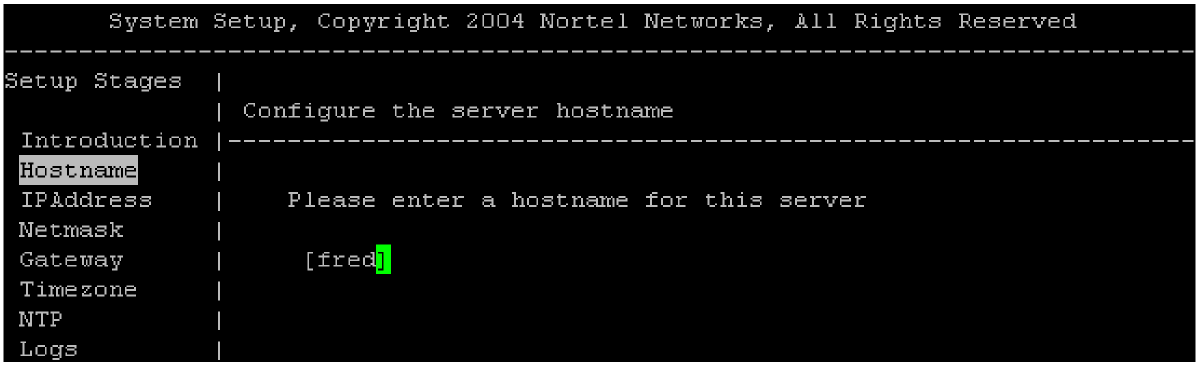
If the commish tool does not start and you receive the following message, complete procedure “Invoke a maintenance SwAct of *the Session Server platform" in the Session Server Security and Administration NTP, NN10346-611.*

```
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**.

> ***Note:*** 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.

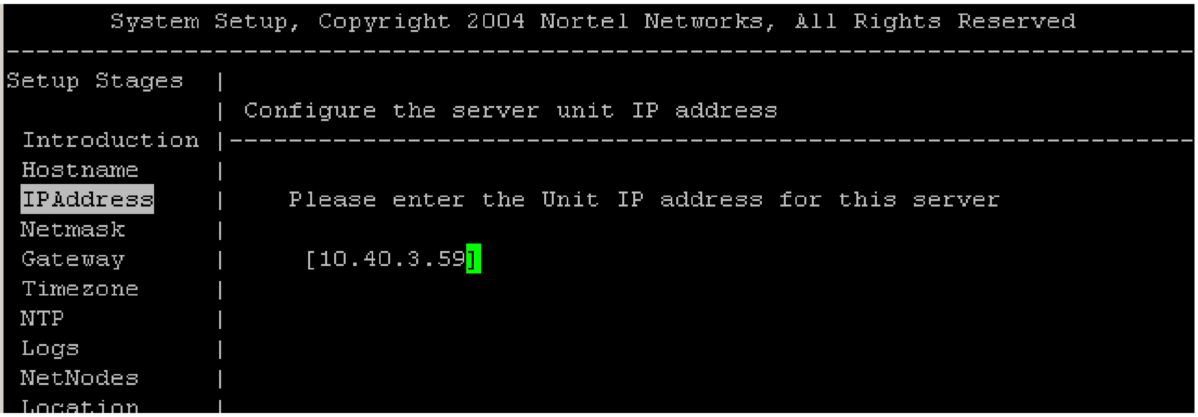


```
      System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server hostname
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter a hostname for this server
 Netmask      |
 Gateway      |     [fred]
 Timezone     |
 NTP          |
 Logs         |
```

5 If applicable, enter a hostname for this Session Server unit using up to 60 alphanumeric characters. Hyphens, underscores are allowed. Periods are not allowed.

6 Position the cursor on the **Next** button and press **Enter**.

The IP address configuration screen appears.



```
      System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server unit IP address
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter the Unit IP address for this server
 Netmask      |
 Gateway      |     [10.40.3.59]
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
```

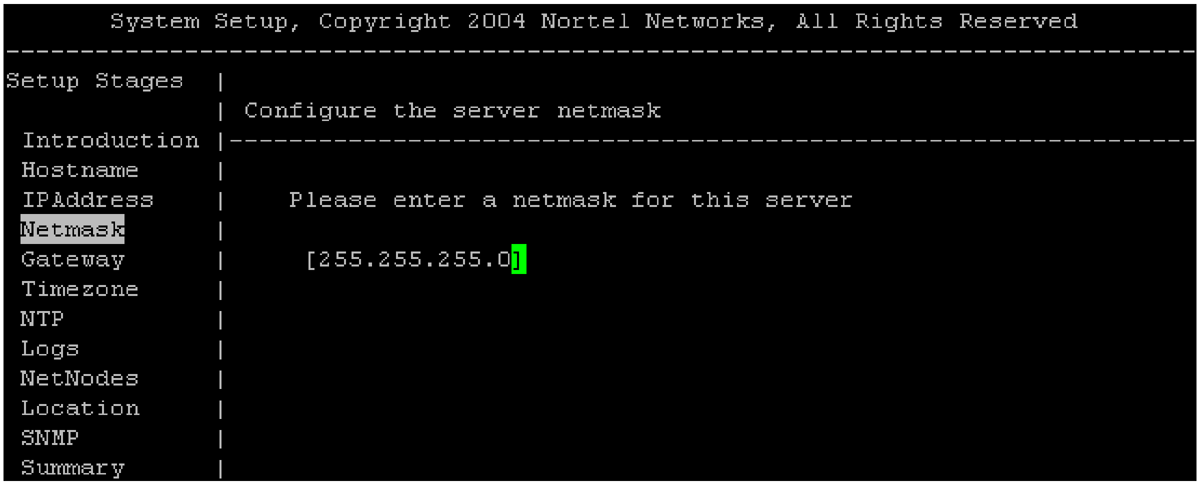
7 If applicable, enter an IP address for this Session Server in the following format:

192.168.102.112

> ***Note:*** Refer to section Session Server configuration on page 6 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.



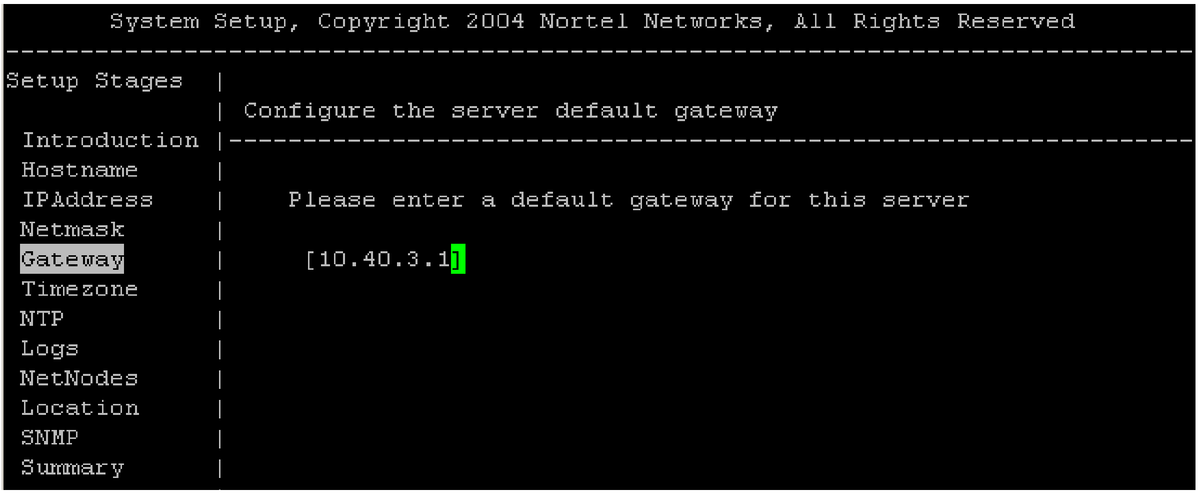
```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server netmask
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter a netmask for this server
 Netmask      |
 Gateway      |     [255.255.255.0]
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
 SNMP         |
 Summary      |
```

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.

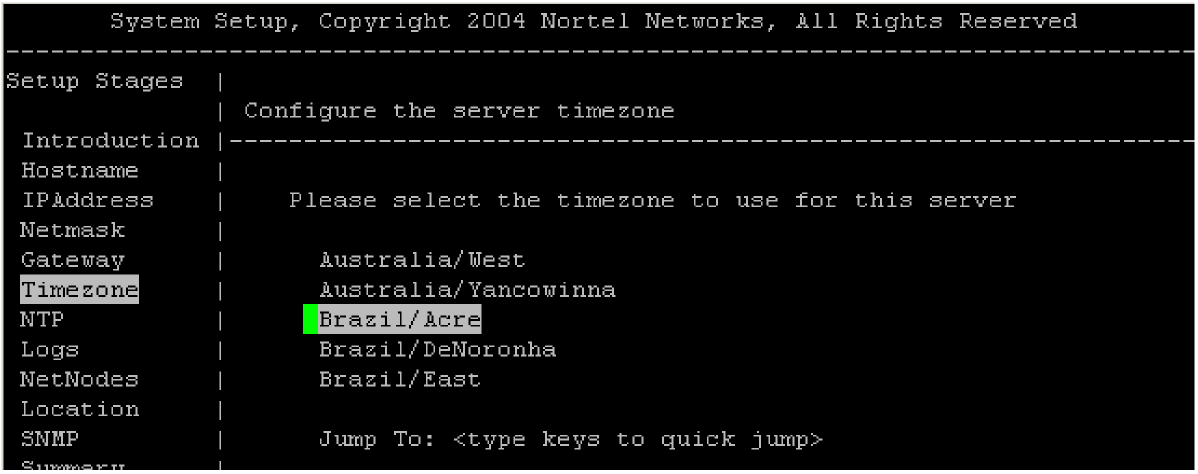


```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages  |
              | Configure the server default gateway
 Introduction |-----------------------------------------------------------------
 Hostname     |
 IPAddress    |    Please enter a default gateway for this server
 Netmask      |
 Gateway      |     [10.40.3.1]
 Timezone     |
 NTP          |
 Logs         |
 NetNodes     |
 Location     |
 SNMP         |
 Summary      |
```

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.



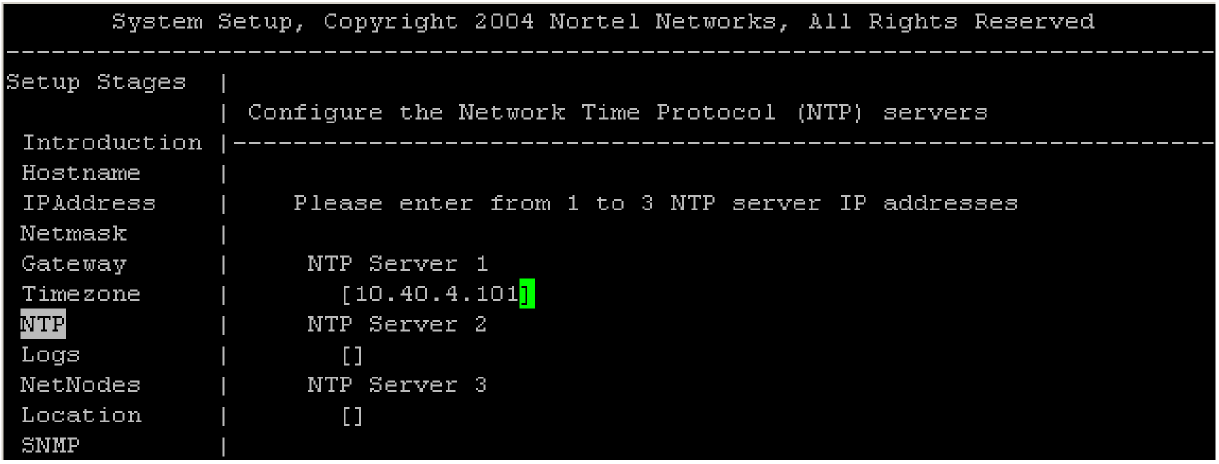
```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the server timezone
 Introduction |----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please select the timezone to use for this server
 Netmask       |
 Gateway       |      Australia/West
 Timezone      |      Australia/Yancowinna
 NTP           |      Brazil/Acre
 Logs          |      Brazil/DeNoronha
 NetNodes      |      Brazil/East
 Location      |
 SNMP          |      Jump To: <type keys to quick jump>
 Summary       |
```

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.

Note: 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.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the Network Time Protocol (NTP) servers
 Introduction |----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please enter from 1 to 3 NTP server IP addresses
 Netmask       |
 Gateway       |     NTP Server 1
 Timezone      |       [10.40.4.101]
 NTP           |     NTP Server 2
 Logs          |       []
 NetNodes      |     NTP Server 3
 Location      |       []
 SNMP          |
```

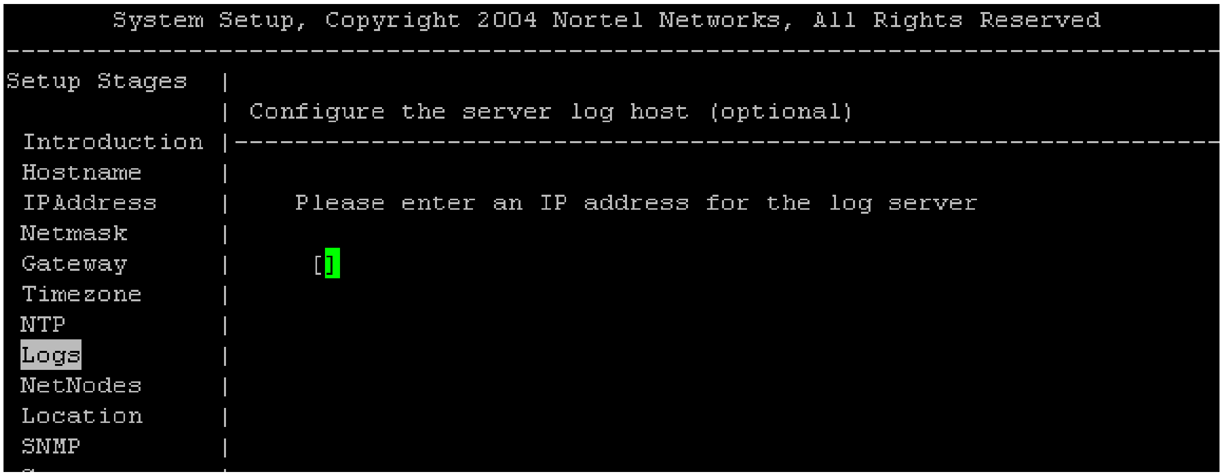
15 If applicable, enter the IP address of at least 1 (up to a maximum of 3) network time protocol servers in the following format:

`192.168.102.112`

> ***Note:*** 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 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.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the server log host (optional)
 Introduction  |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please enter an IP address for the log server
 Netmask       |
 Gateway       |      []
 Timezone      |
 NTP           |
 Logs          |
 NetNodes      |
 Location      |
 SNMP          |
```

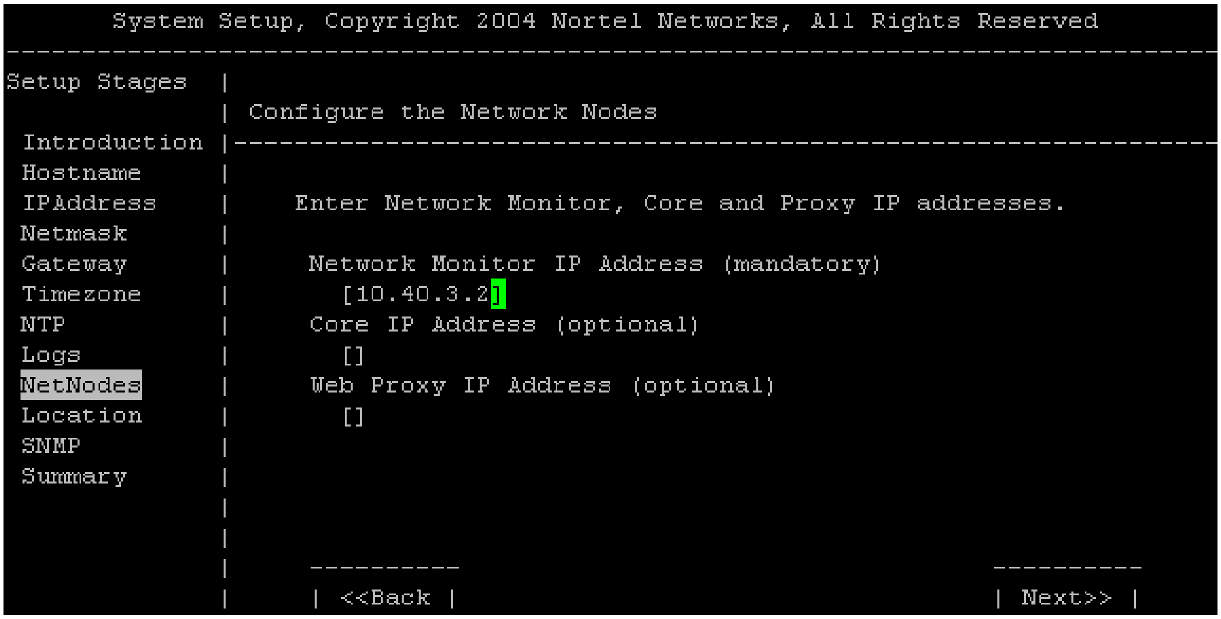
17 Enter the IP address of the log server in the following format:

`192.168.102.112`

> ***Note:*** 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.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the Network Nodes
 Introduction  |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Enter Network Monitor, Core and Proxy IP addresses.
 Netmask       |
 Gateway       |     Network Monitor IP Address (mandatory)
 Timezone      |       [10.40.3.2]
 NTP           |     Core IP Address (optional)
 Logs          |       []
 NetNodes      |     Web Proxy IP Address (optional)
 Location      |       []
 SNMP          |
 Summary       |
               |
               |
               |     ----------                                ----------
               |     | <<Back |                                | Next>> |
```

19 Use the following sub-steps to complete the Network Nodes screen:

a For networks using sites using PP8600 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.

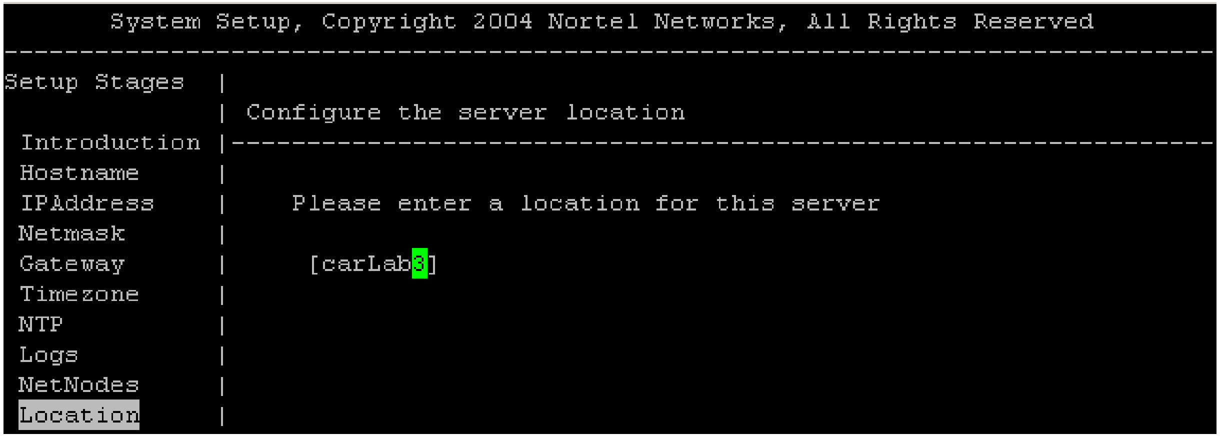
c Enter the IP address of the SSPFS server for the Web Proxy IP Address in the following format:

`192.168.102.112`

Note: Use the IP address of the SSPFS 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.

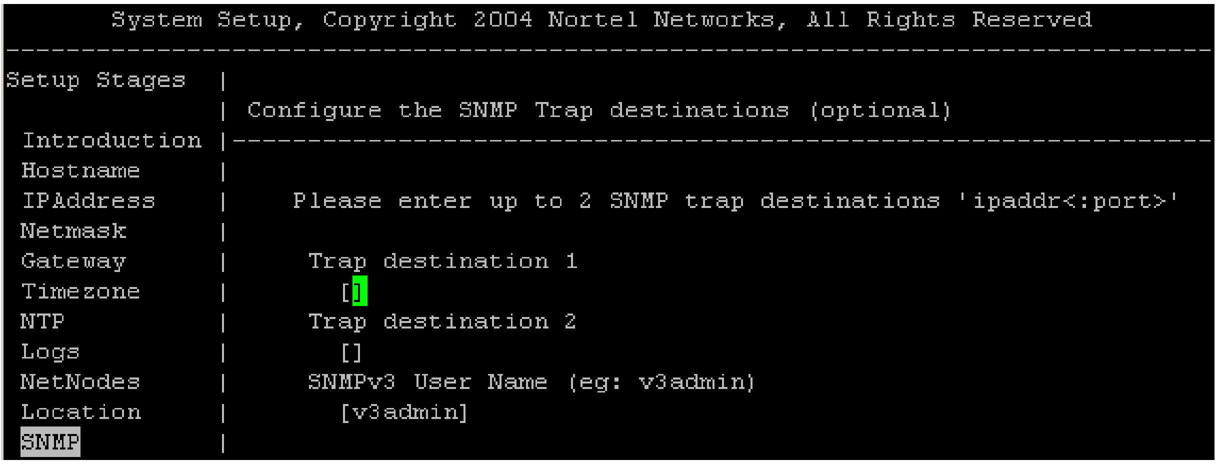


```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the server location
 Introduction |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please enter a location for this server
 Netmask       |
 Gateway       |      [carLab3]
 Timezone      |
 NTP           |
 Logs          |
 NetNodes      |
 Location      |
```

21 If applicable, enter a location identifier for this Session Server location.

22 Position the cursor on the **Next** button and press **Enter**.

The optional SNMP trap destinations page is displayed.



```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Configure the SNMP Trap destinations (optional)
 Introduction |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Please enter up to 2 SNMP trap destinations 'ipaddr<:port>'
 Netmask       |
 Gateway       |      Trap destination 1
 Timezone      |        []
 NTP           |      Trap destination 2
 Logs          |        []
 NetNodes      |      SNMPv3 User Name (eg: v3admin)
 Location      |        [v3admin]
 SNMP          |
```

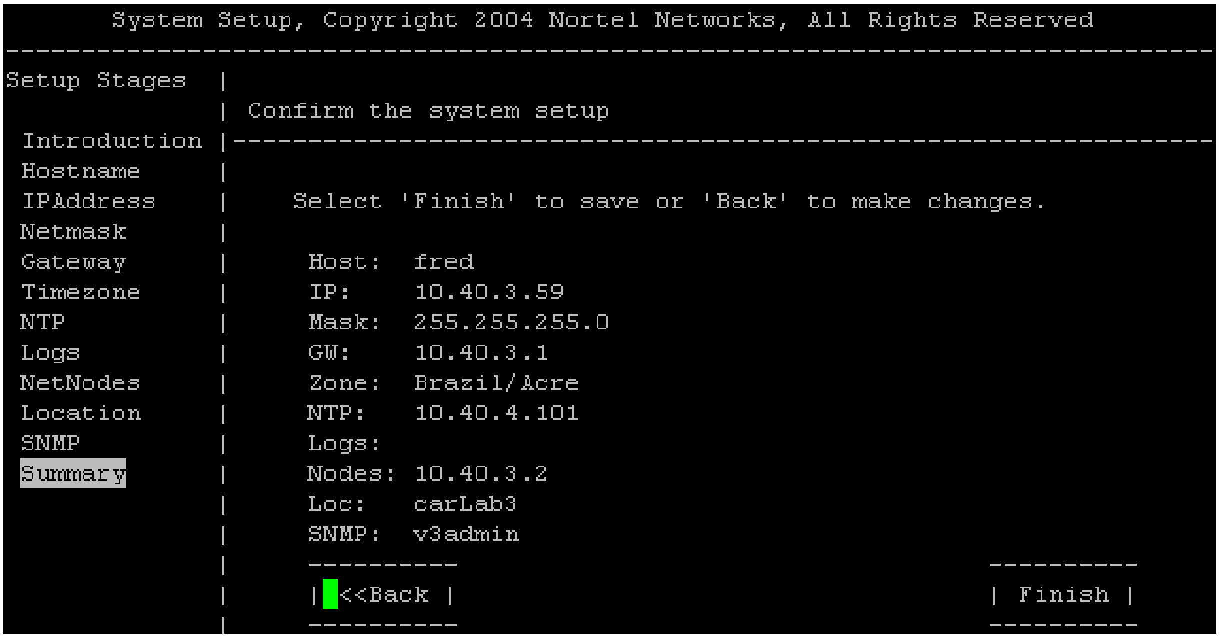
23 If applicable, enter the IP address of the Integrated EMS server for Trap destination 1 in the following format:

```
192.168.102.112
```

> ***Note 1:*** Use the IP address of the Integrated EMS application residing on the CS 2000 Management Tools server.
>
> ***Note 2:*** 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

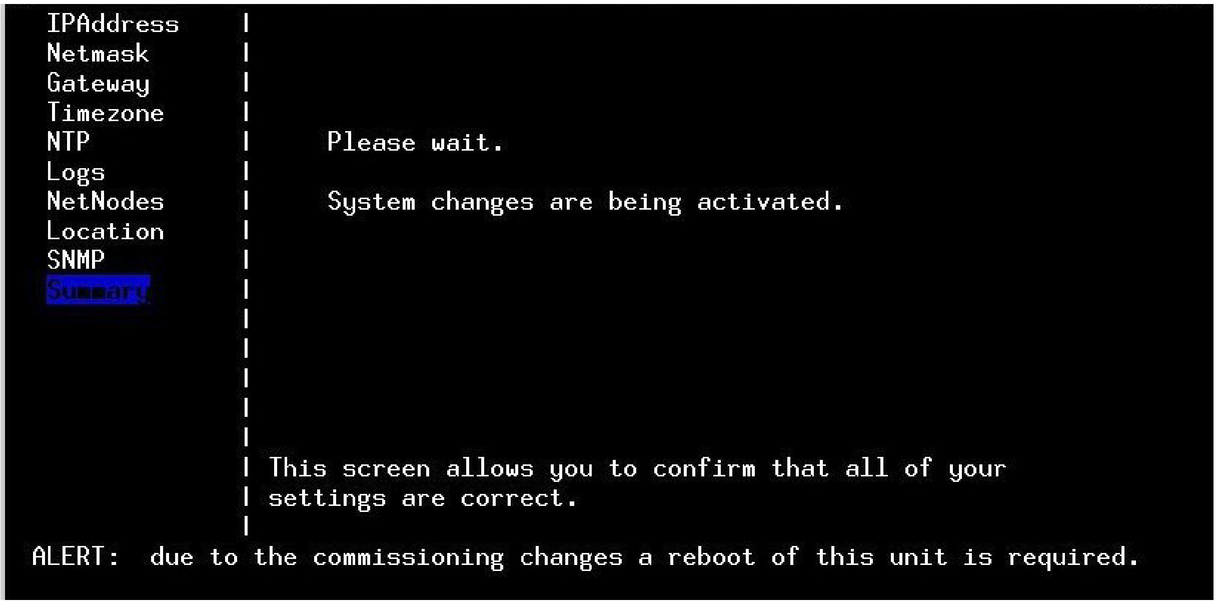


```
       System Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Setup Stages   |
               | Confirm the system setup
 Introduction  |-----------------------------------------------------------------
 Hostname      |
 IPAddress     |    Select 'Finish' to save or 'Back' to make changes.
 Netmask       |
 Gateway       |     Host:  fred
 Timezone      |     IP:    10.40.3.59
 NTP           |     Mask:  255.255.255.0
 Logs          |     GW:    10.40.3.1
 NetNodes      |     Zone:  Brazil/Acre
 Location      |     NTP:   10.40.4.101
 SNMP          |     Logs:
 Summary       |     Nodes: 10.40.3.2
               |     Loc:   carLab3
               |     SNMP:  v3admin
               |     ----------                                        ----------
               |     | <<Back |                                      | Finish |
               |     ----------                                        ----------
```

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.



```
   IPAddress     |
   Netmask       |
   Gateway       |
   Timezone      |
   NTP           |     Please wait.
   Logs          |
   NetNodes      |     System changes are being activated.
   Location      |
   SNMP          |
   Summary       |
                 |
                 |
                 |
                 |
                 |
                 | This screen allows you to confirm that all of your
                 | settings are correct.
                 |
 ALERT:  due to the commissioning changes a reboot of this unit is required.
```

26 After the unit has rebooted, verify the Session Server unit is unjammed using procedure *Enable a system SwAct (Unjam)*, found in the Session Server Security and Administration NTP, NN10346-611.

27 SwAct the units by performing procedure *Invoke a maintenance SwAct of the Session Server platform* found in the Session Server Security and Administration NTP, NN10346-611.

28 Repeat this procedure on the other, now in standby, Session Server unit.

29 Use procedure View the operational status of a Session Server NCGL platform on page 141 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.

31 The procedure is complete.

Start 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 Session Server units in the node.

> **ATTENTION**
> Nortel Networks recommends monitoring all filesystems.

Limitations and restrictions

There are no limitations for performing this procedure

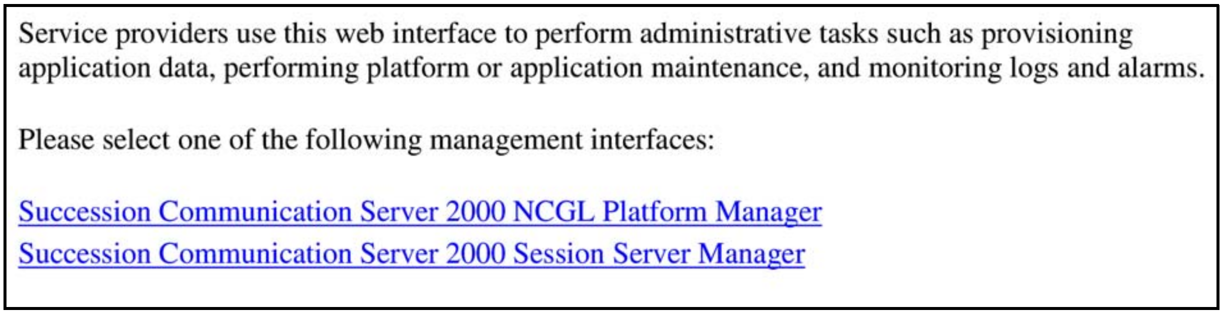
Prerequisites

There are no prerequisites for this procedure.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

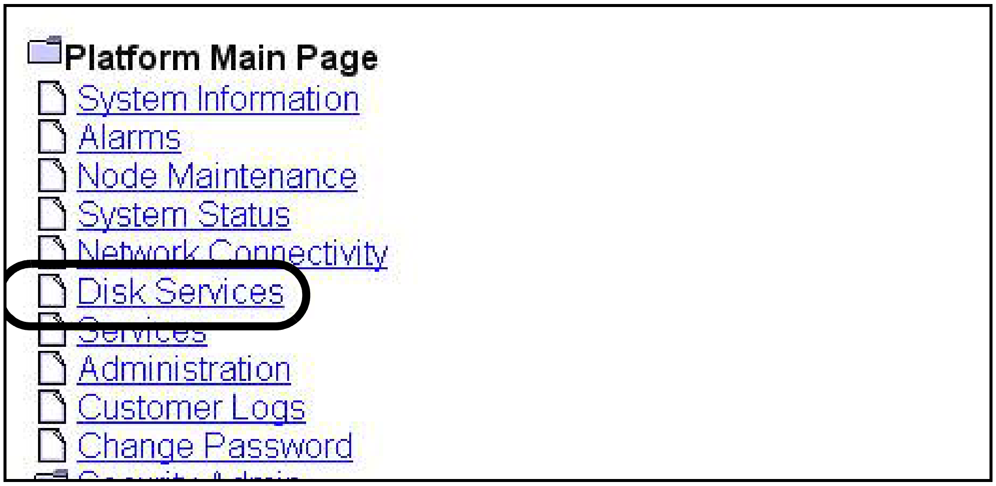


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

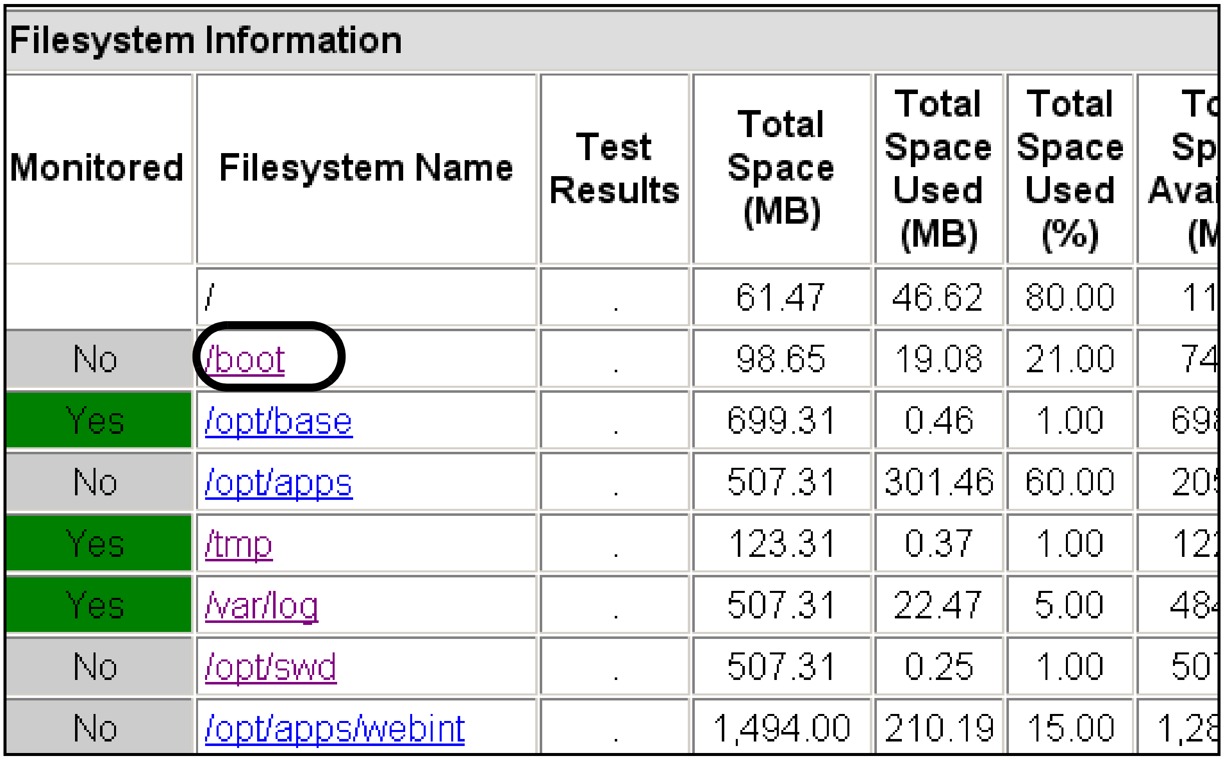
2 Click the **Disk Services** link.



Platform Main Page
- System Information
- Alarms
- Node Maintenance
- System Status
- Network Connectivity
- Disk Services
- Services
- Administration
- Customer Logs
- Change Password

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

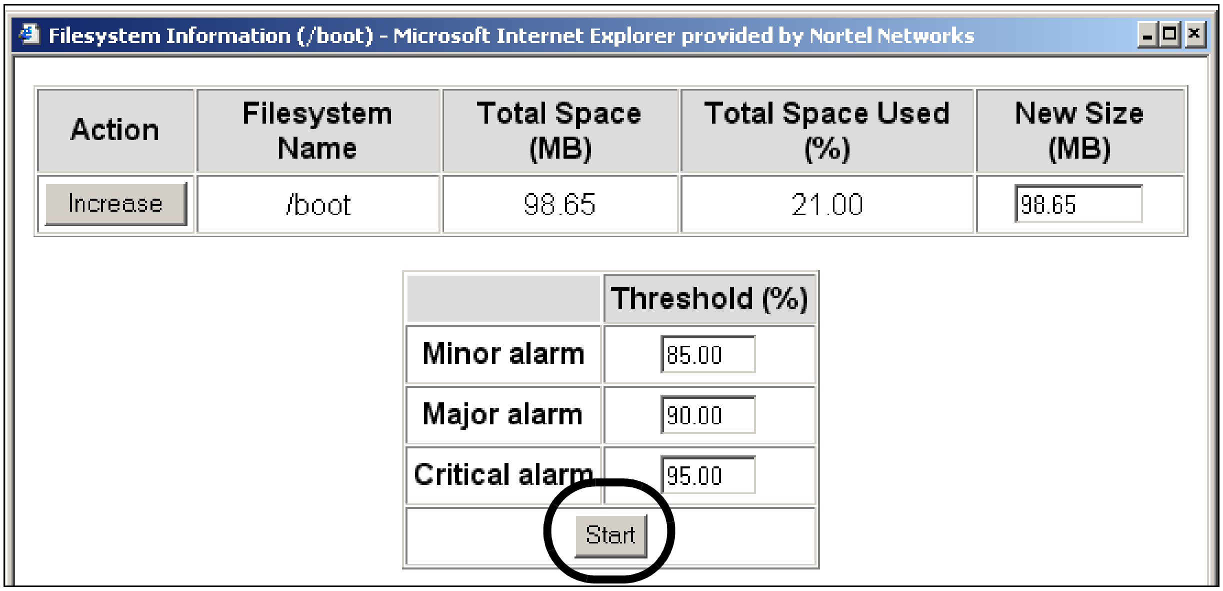
Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	To Sp Avai (M
	/	.	61.47	46.62	80.00	11
No	/boot	.	98.65	19.08	21.00	74
Yes	/opt/base	.	699.31	0.46	1.00	69
No	/opt/apps	.	507.31	301.46	60.00	20
Yes	/tmp	.	123.31	0.37	1.00	12
Yes	/var/log	.	507.31	22.47	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 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 step 5.

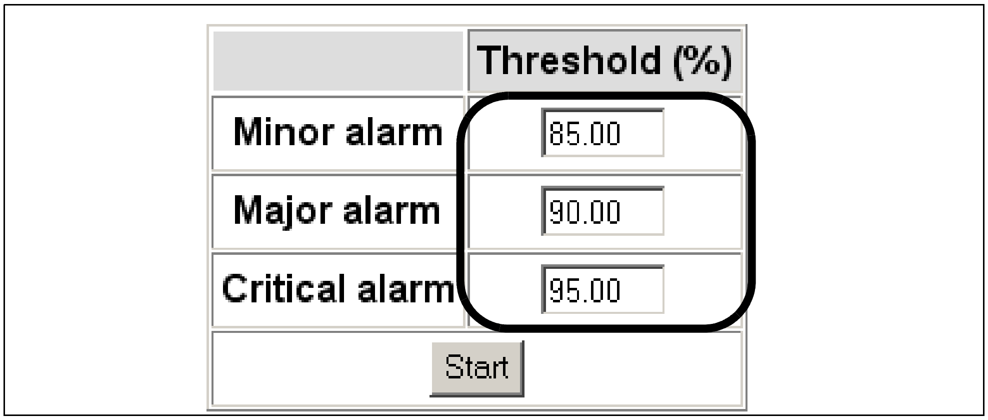

Filesystem Information (/boot) - Microsoft Internet Explorer provided by Nortel Networks

Action	Filesystem Name	Total Space (MB)	Total Space Used (%)	New Size (MB)
Increase	/boot	98.65	21.00	98.65

	Threshold (%)
Minor alarm	85.00
Major alarm	90.00
Critical alarm	95.00
Start	

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 done 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.



	Threshold (%)
Minor alarm	85.00
Major alarm	90.00
Critical alarm	95.00
Start	

6 Repeat this procedure for the same filesystem on the second (mate) Session Server unit.

7 This procedure is complete.

Stop 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 Session Server 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.

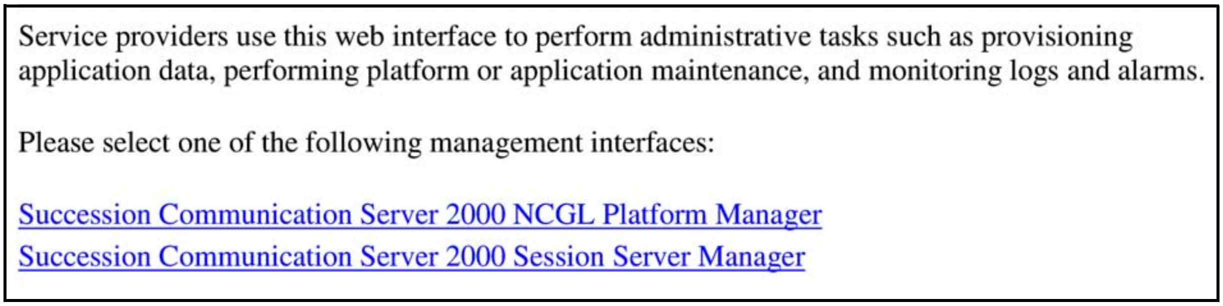
Prerequisites

There are no prerequisites for this procedure.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

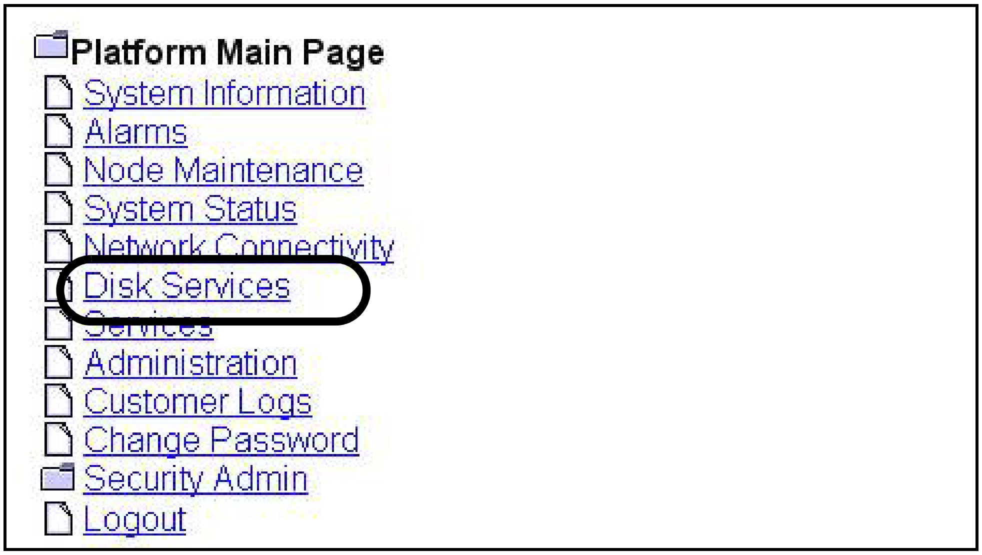


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

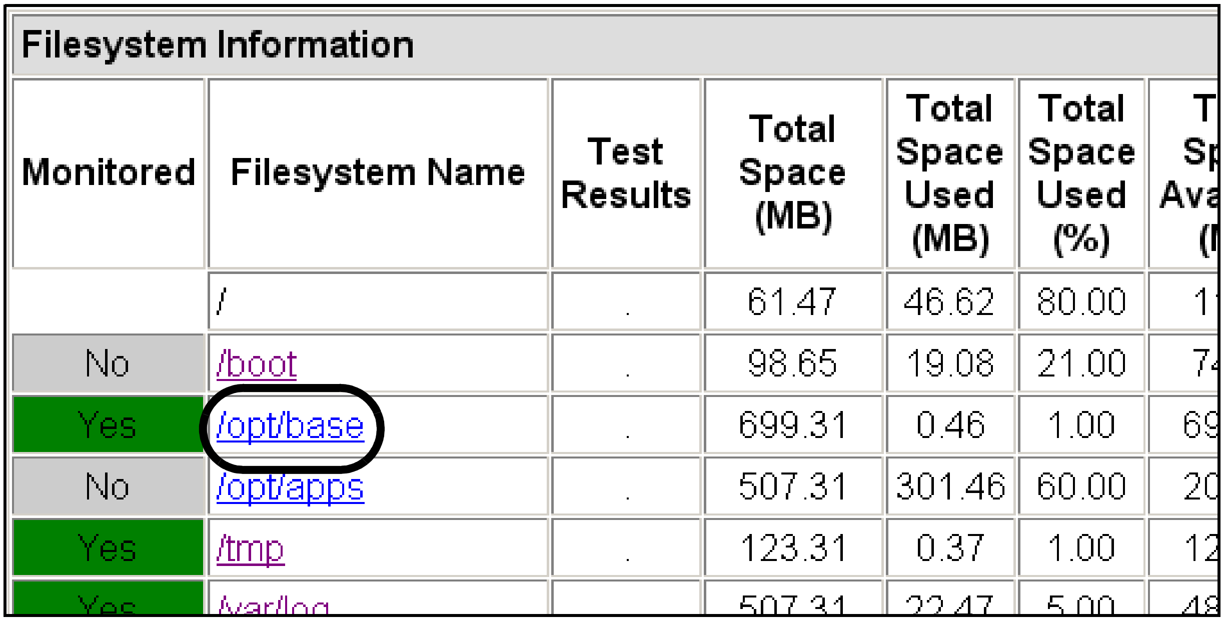
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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.



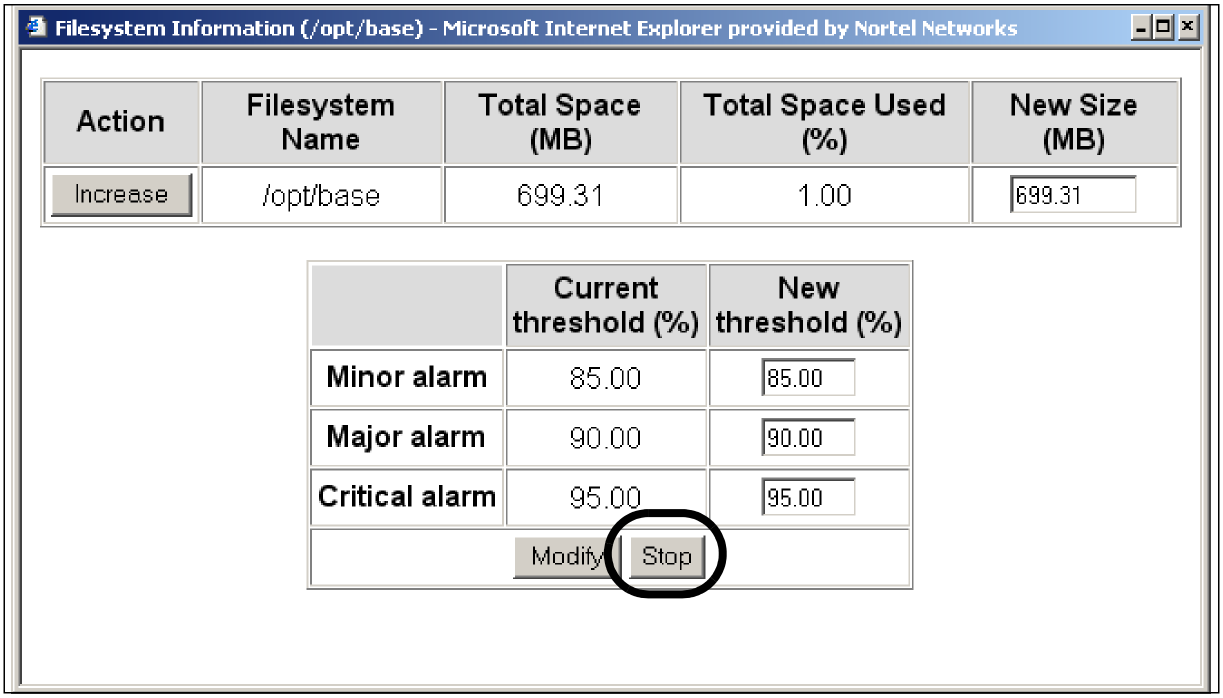
Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	T Sp Ava (I
	/	.	61.47	46.62	80.00	1
No	/boot	.	98.65	19.08	21.00	7
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

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.


Filesystem Information (/opt/base) - Microsoft Internet Explorer provided by Nortel Networks

Action	Filesystem Name	Total Space (MB)	Total Space Used (%)	New Size (MB)
Increase	/opt/base	699.31	1.00	699.31

	Current threshold (%)	New threshold (%)
Minor alarm	85.00	85.00
Major alarm	90.00	90.00
Critical alarm	95.00	95.00

5 Repeat this procedure for the same filesystem on the second (mate) Session Server unit.

6 This procedure is complete.

Modify filesystem monitoring thresholds

Purpose of this procedure

Use this procedure to modify the thresholds for monitoring disk and filesystem usage. Session Server 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 Session Server 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.

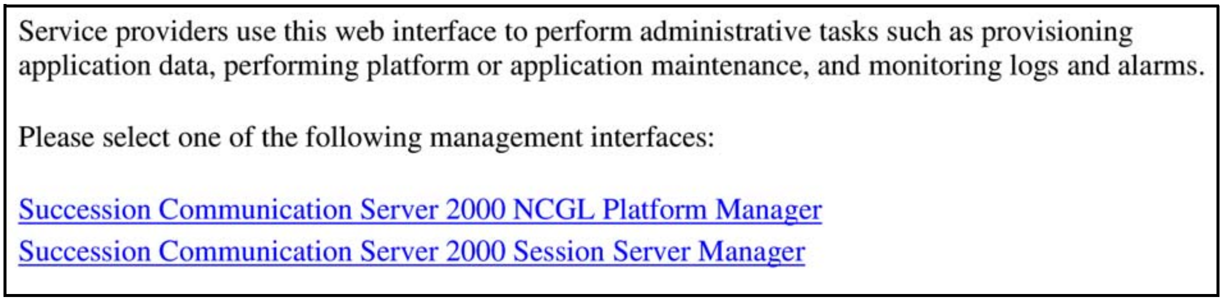
Prerequisites

There are no prerequisites for this procedure.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

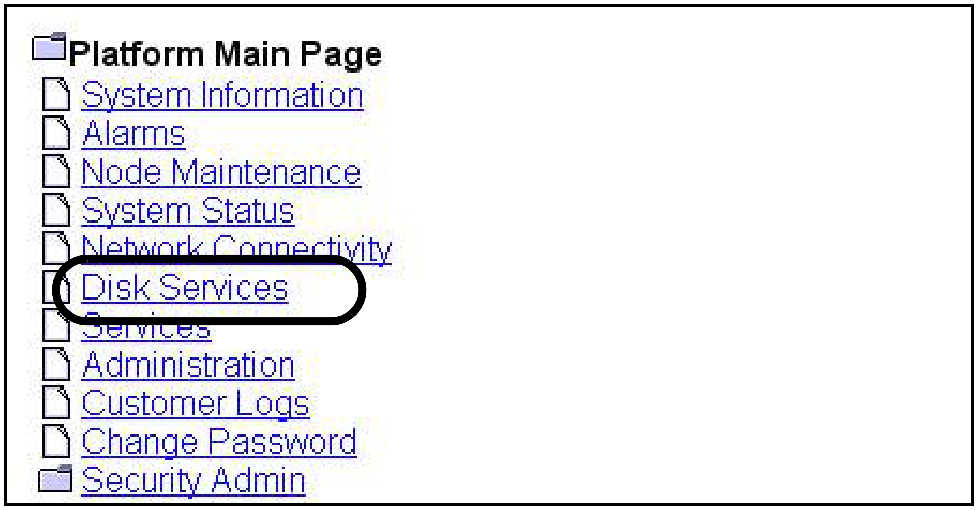


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Disk Services** link.

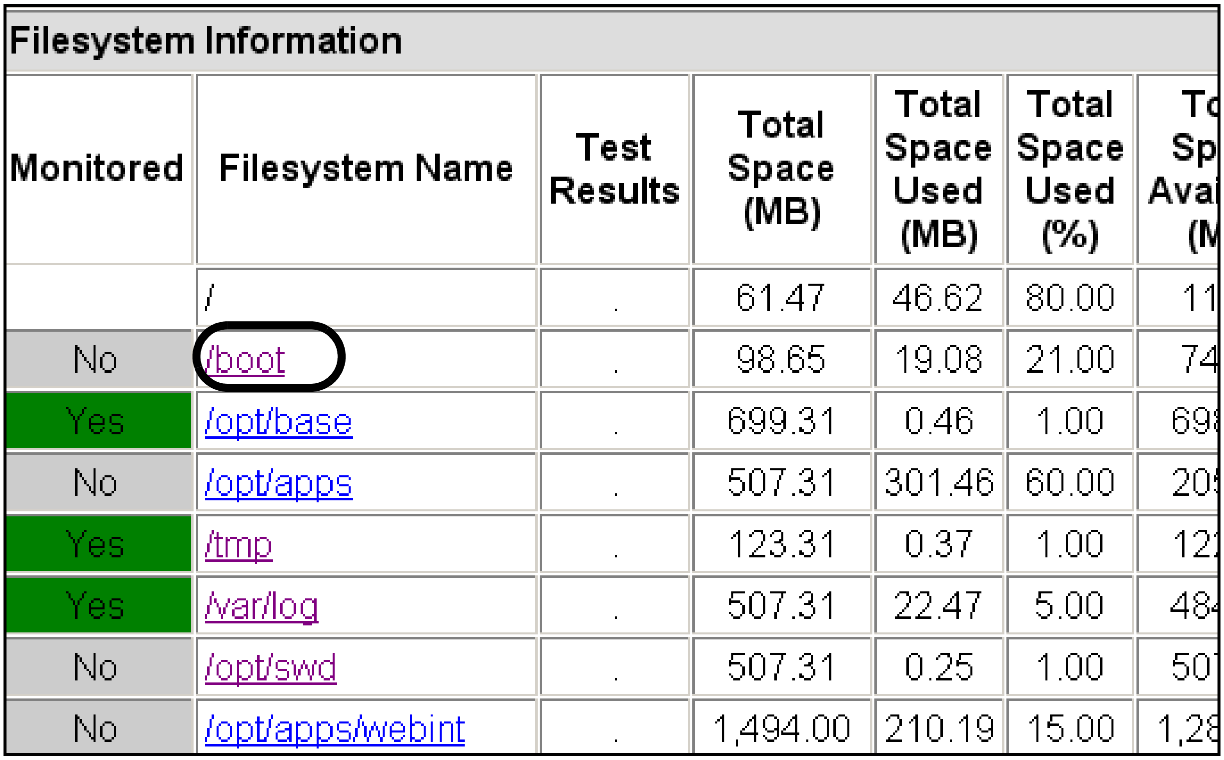


Platform Main Page

- System Information
- Alarms
- Node Maintenance
- System Status
- Network Connectivity
- Disk Services
- Services
- Administration
- Customer Logs
- Change Password
- Security Admin

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.



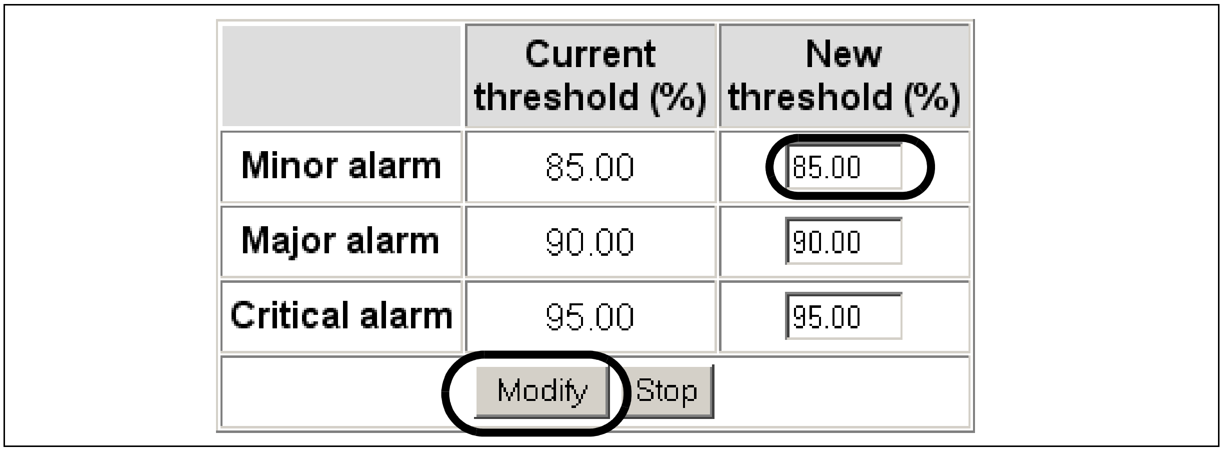
Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	To Sp Avai (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 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

5 Repeat this procedure for the same filesystem on the second (mate) Session Server unit.

6 This procedure is complete.

Remove a filesystem

Purpose of this procedure

This procedure is used to remove an entire filesystem from the Session Server hard drives. This procedure must be performed on both of the Session Server 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.

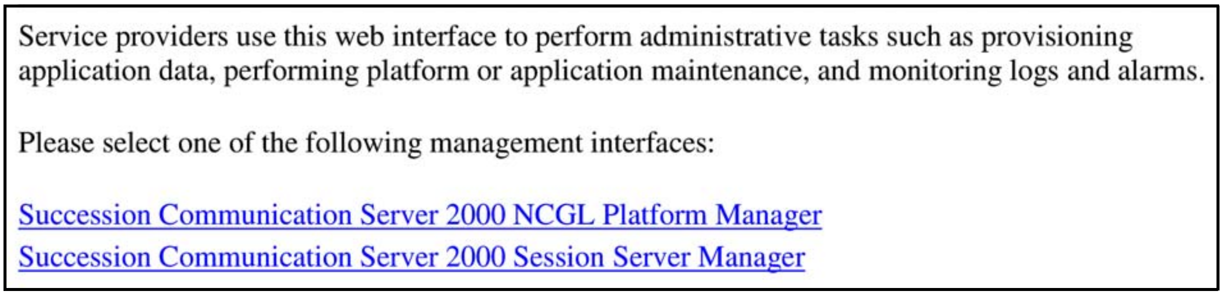
Prerequisites

Refer to procedures *Configure database backups for the Session Server* and *Perform a data backup of the Session Server* found in the Session Server Security and Administration NTP, NN10346-611, for information about backing up filesystems.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



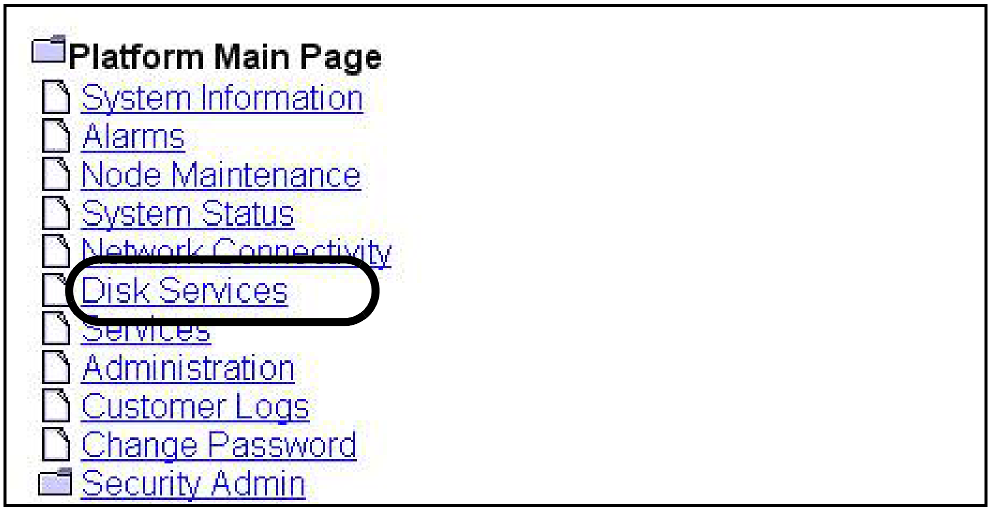
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

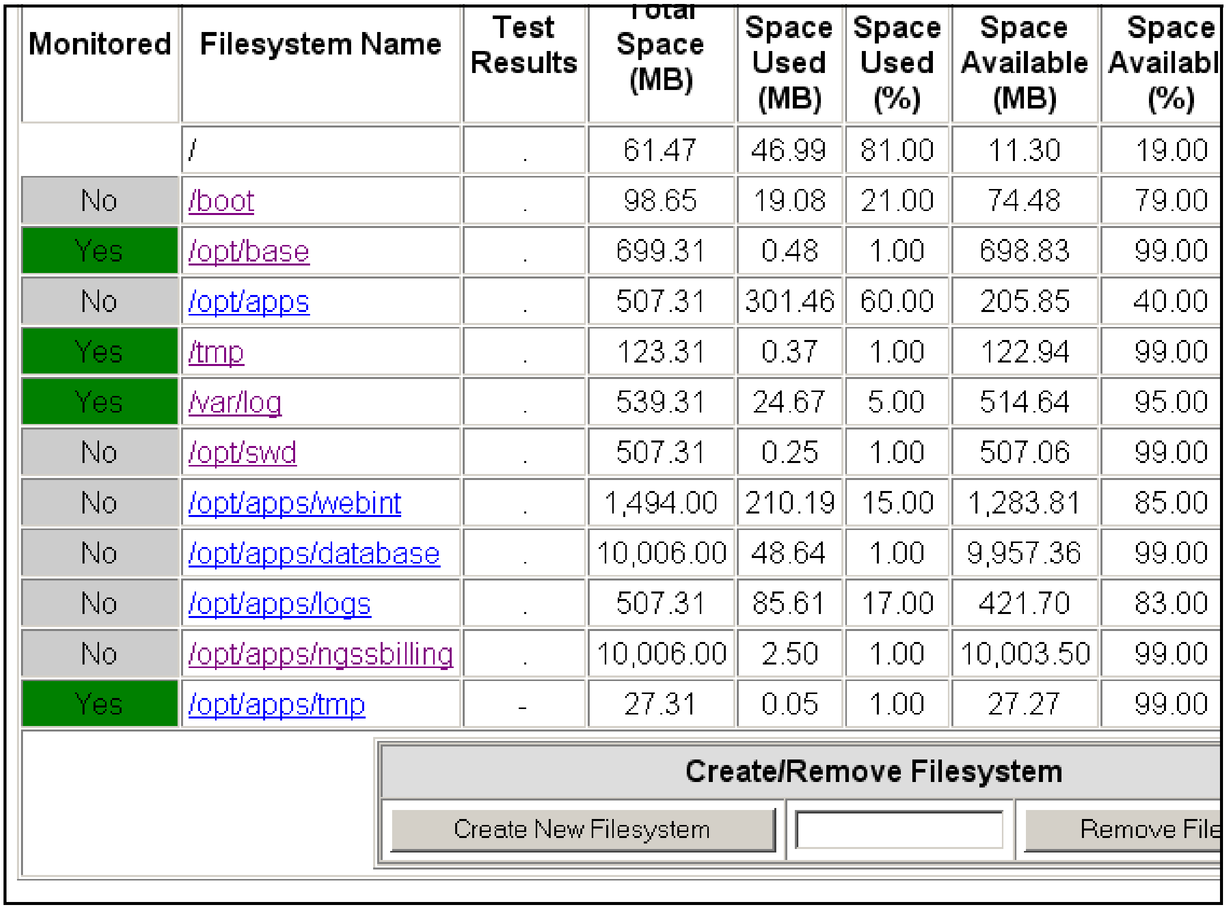
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Disk Services** link.

The Disk Services page is displayed.



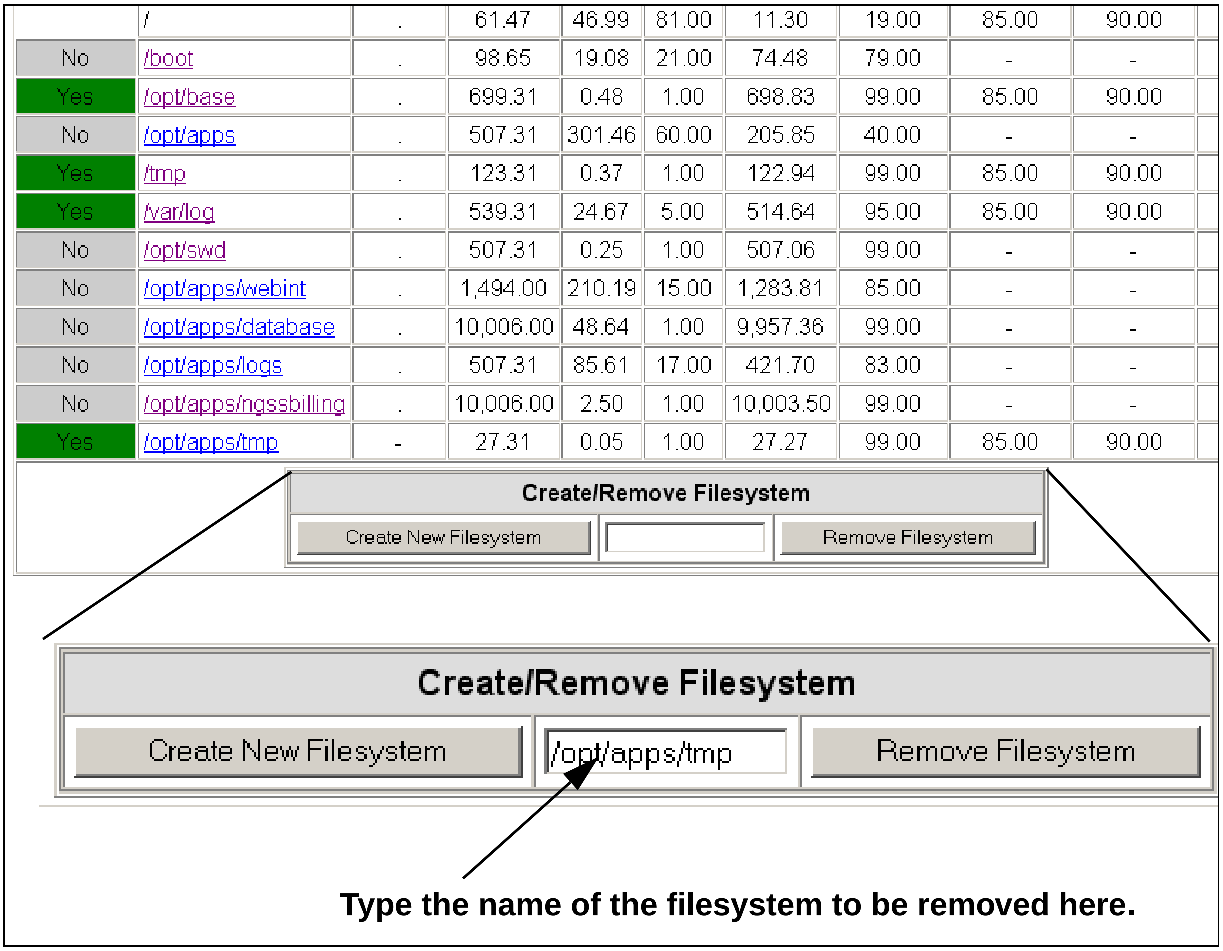
3 Locate the name of the filesystem that you want to remove in the *Filesystems Information* view.



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

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.

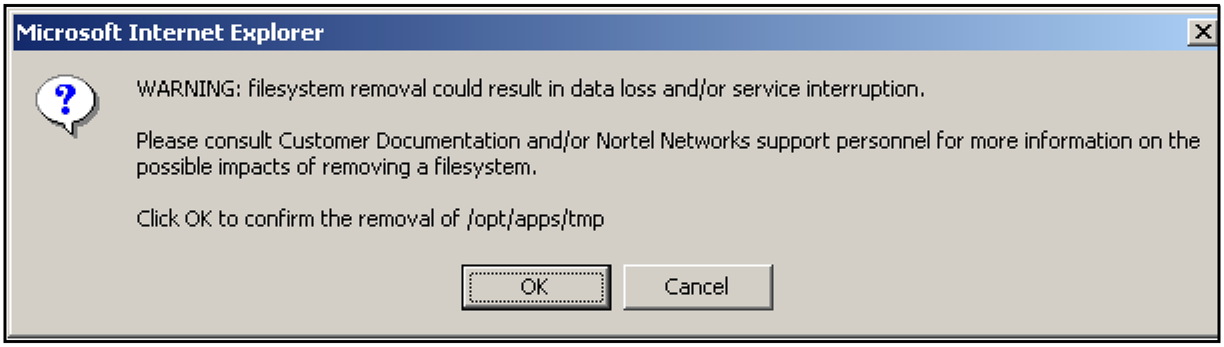


	/	.	61.47	46.99	81.00	11.30	19.00	85.00	90.00
No	/boot	.	98.65	19.08	21.00	74.48	79.00	-	-
Yes	/opt/base	.	699.31	0.48	1.00	698.83	99.00	85.00	90.00
No	/opt/apps	.	507.31	301.46	60.00	205.85	40.00	-	-
Yes	/tmp	.	123.31	0.37	1.00	122.94	99.00	85.00	90.00
Yes	/var/log	.	539.31	24.67	5.00	514.64	95.00	85.00	90.00
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	85.00	90.00

/opt/apps/tmp

Type the name of the filesystem to be removed here.

5 Confirm that you want to remove the filesystem by clicking **OK**.



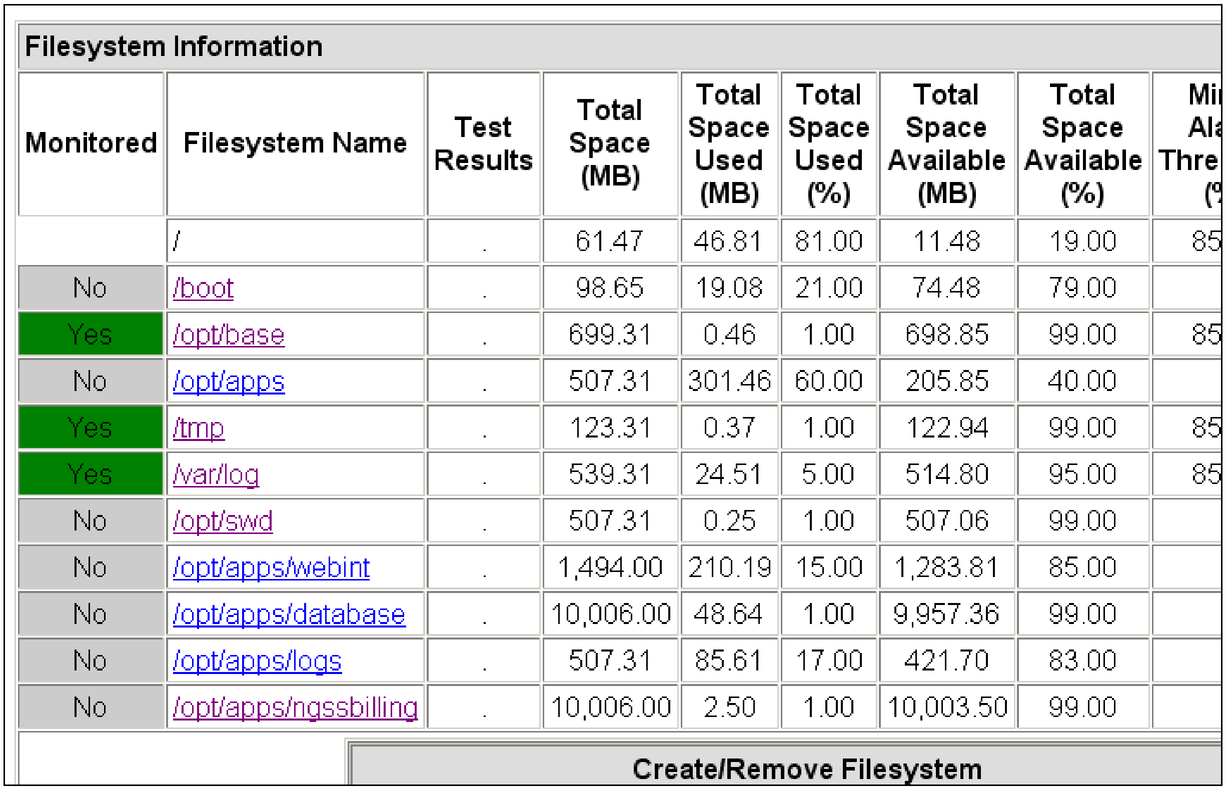
Microsoft Internet Explorer

WARNING: filesystem removal could result in data loss and/or service interruption.

Please consult Customer Documentation and/or Nortel Networks support personnel for more information on the possible impacts of removing a filesystem.

Click OK to confirm the removal of /opt/apps/tmp

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 Ala 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	

7 Repeat this procedure for the other (mate) Session Server unit, using the same values and settings as you did for the first unit.

8 This procedure is complete.

Increase filesystem size

Purpose of this procedure

This procedure is used to increase the size (in MB) of an existing filesystem on the Session Server hard drives. This procedure must be performed on both of the Session Server 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 Remove a filesystem on page 225, then recreate the filesystem, using a smaller amount of disk space, using procedure Create a filesystem on page 233.

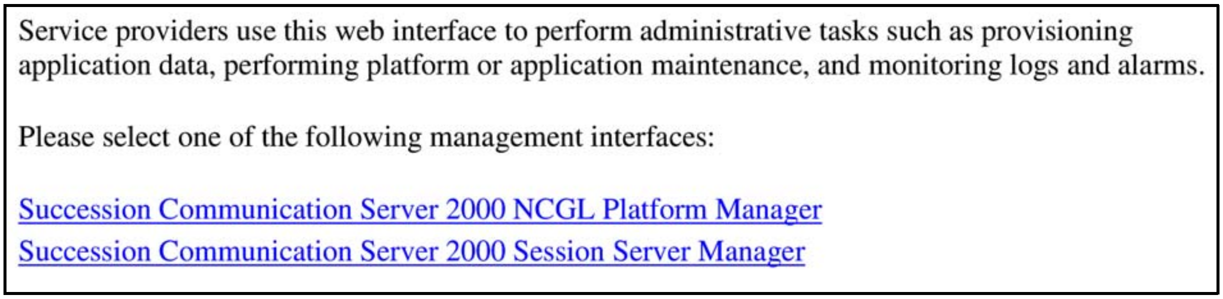
Prerequisites

There are no prerequisites for this procedure.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



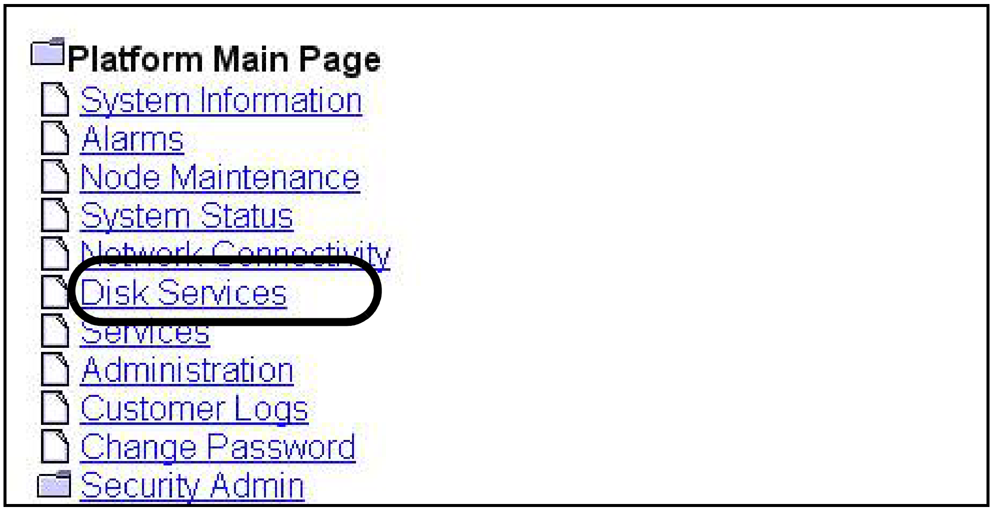
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Disk Services** link.

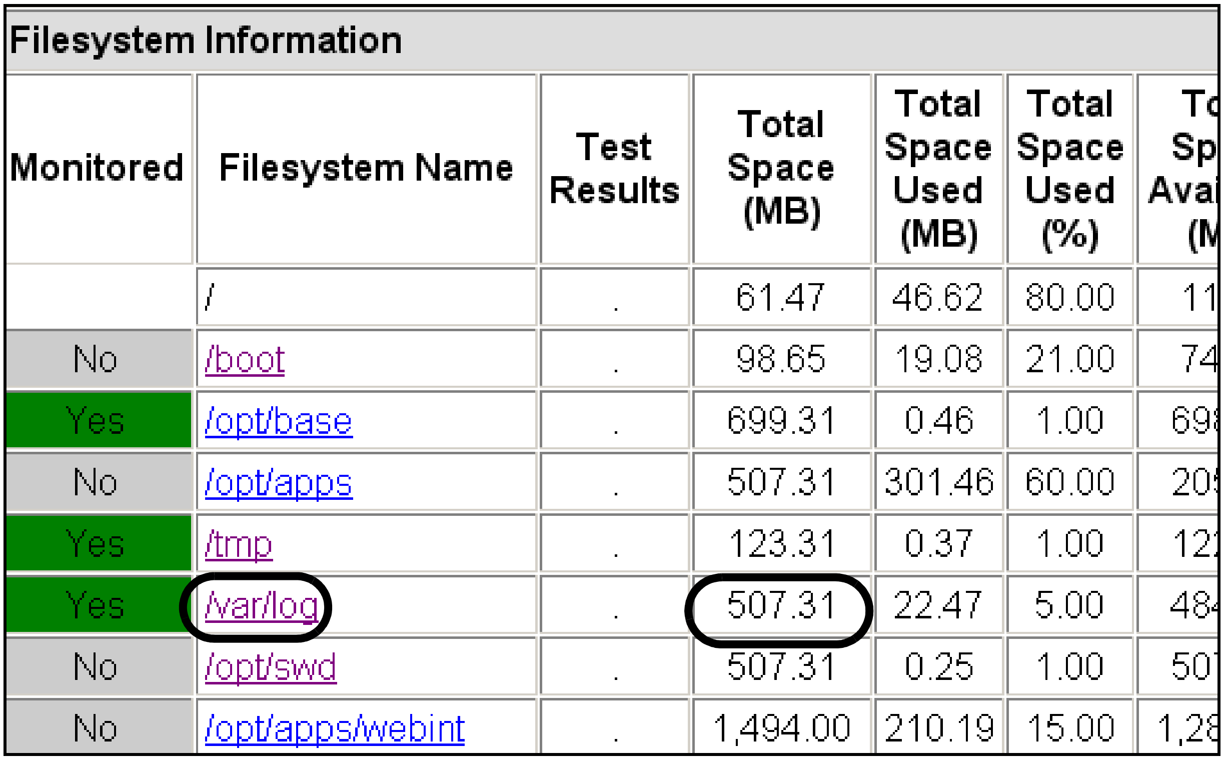
The Disk Services page is displayed.



Platform Main Page
- System Information
- Alarms
- Node Maintenance
- System Status
- Network Connectivity
- Disk Services
- Services
- Administration
- Customer Logs
- Change Password
- Security Admin

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.



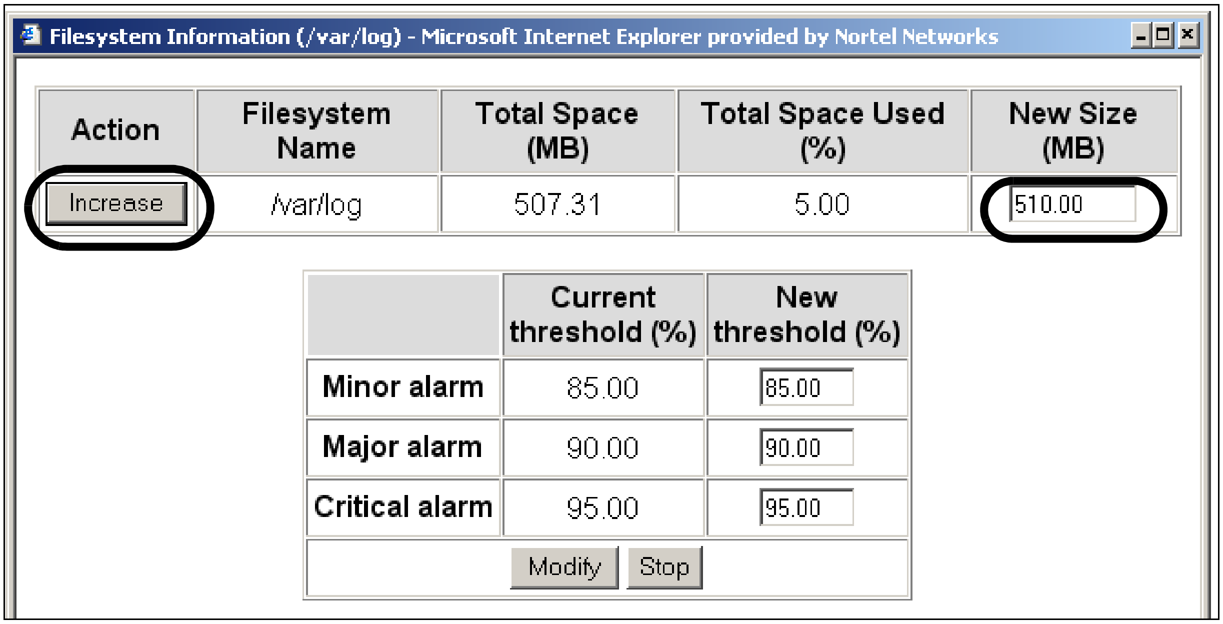
Filesystem Information

Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	To Sp Avai (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.

Note: Enter a value that is larger than the value shown in the Total Space (MB) field.



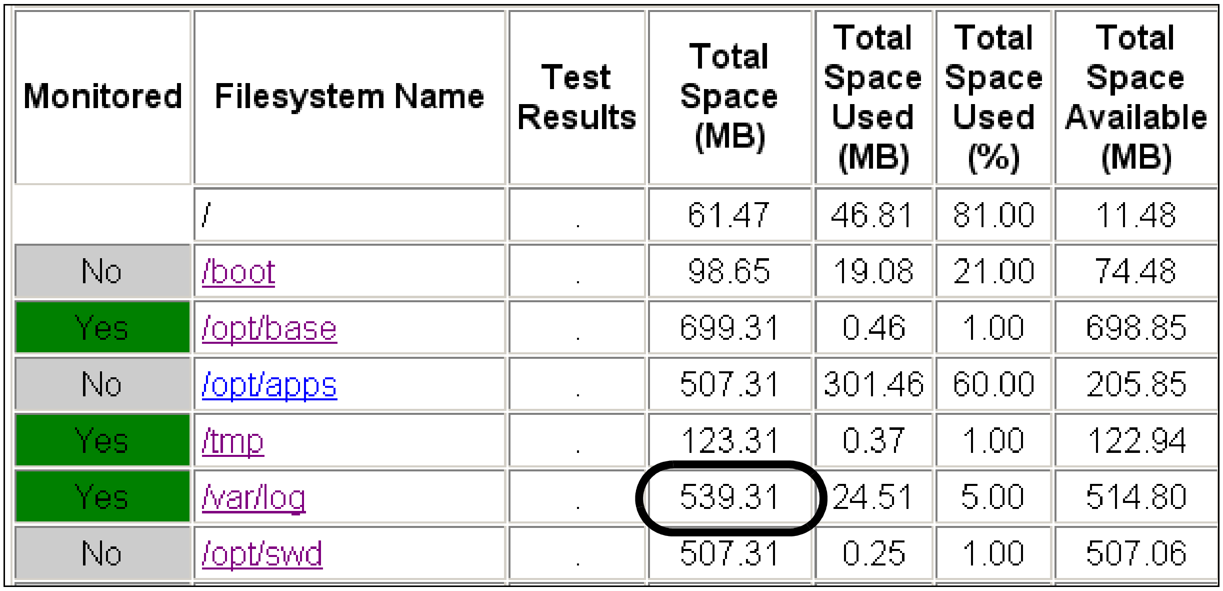
Filesystem Information (/var/log) - Microsoft Internet Explorer provided by Nortel Networks

Action	Filesystem Name	Total Space (MB)	Total Space Used (%)	New Size (MB)
Increase	/var/log	507.31	5.00	510.00

	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 Verify that the increase is indicated in the Total Space (MB) column of the *Filesystem Information* panel.

Note: 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) Session Server unit.

7 This procedure is complete.

Create a filesystem

Purpose of this procedure

This procedure is used to add a new filesystem to the Session Server hard drives. This procedure must be performed on both of the Session Server 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.

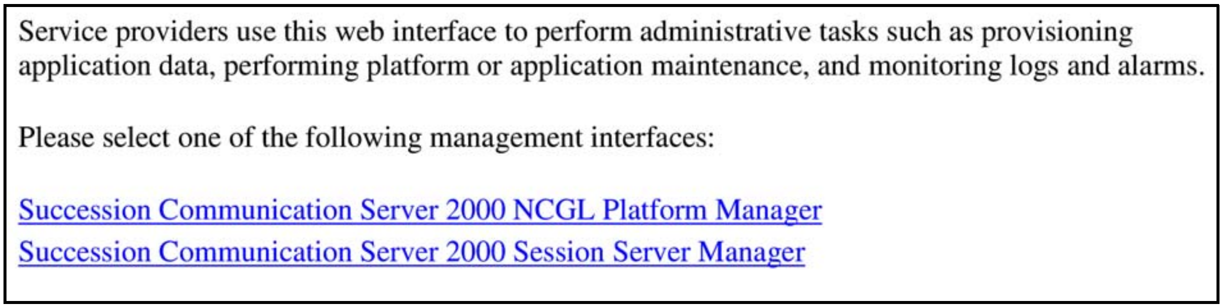
Prerequisites

There are no prerequisites for this procedure.

Action

At the CS 2000 Session Server Launch Point

1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.



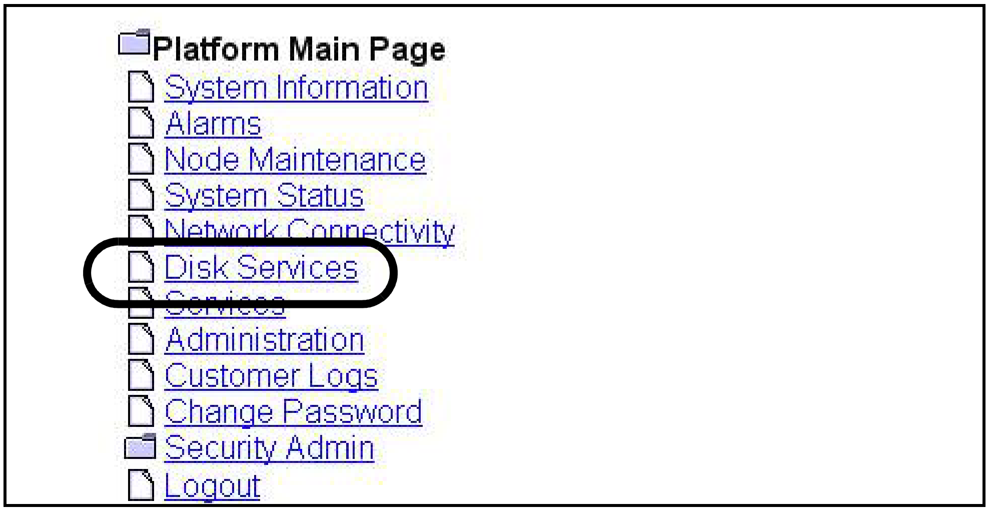
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

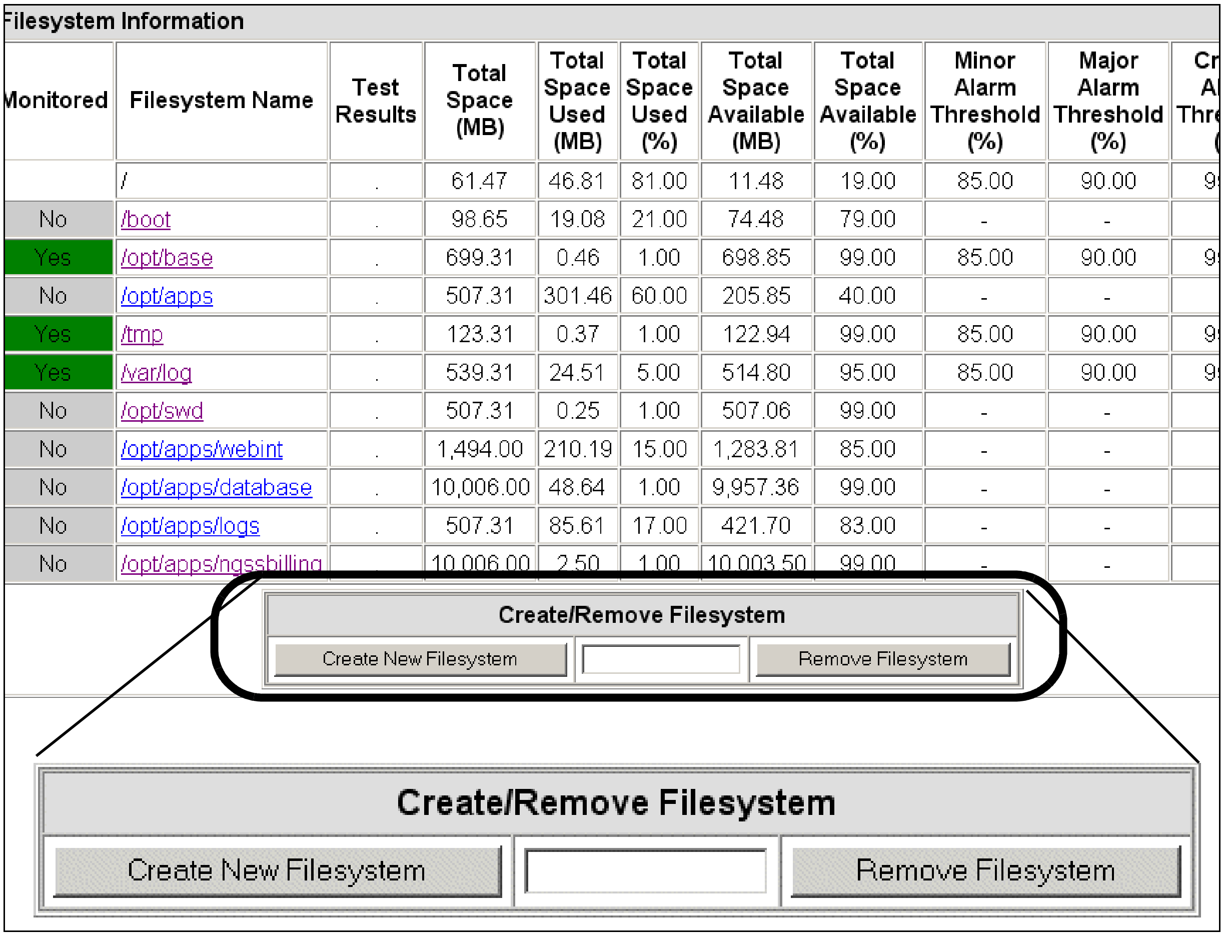
2 Click the **Disk Services** link.

The Disk Services page is displayed.



Platform Main Page
System Information
Alarms
Node Maintenance
System Status
Network Connectivity
Disk Services
Services
Administration
Customer Logs
Change Password
Security Admin
Logout

3 Scroll to the *Create/Remove Filesystem* section.



ilesystem Information

onitored	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 (%)	Cr Al Thre (
	/	.	61.47	46.81	81.00	11.48	19.00	85.00	90.00	9
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	9
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	85.00	90.00	9
Yes	/var/log	.	539.31	24.51	5.00	514.80	95.00	85.00	90.00	9
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

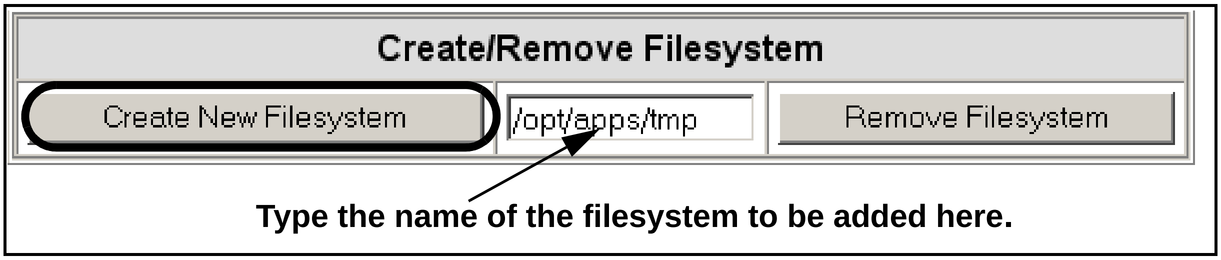
Create New Filesystem | Remove Filesystem

Create/Remove Filesystem

Create New Filesystem | Remove Filesystem

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.

> ***Note 1:*** The name entered for the new filesystem must be fully qualified from the root level (/) and must begin with a forward slash (/) character.
>
> ***Note 2:*** 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)
>
> ***Note 3:*** New filesystem names must be unique from existing filesystem names currently in the system.

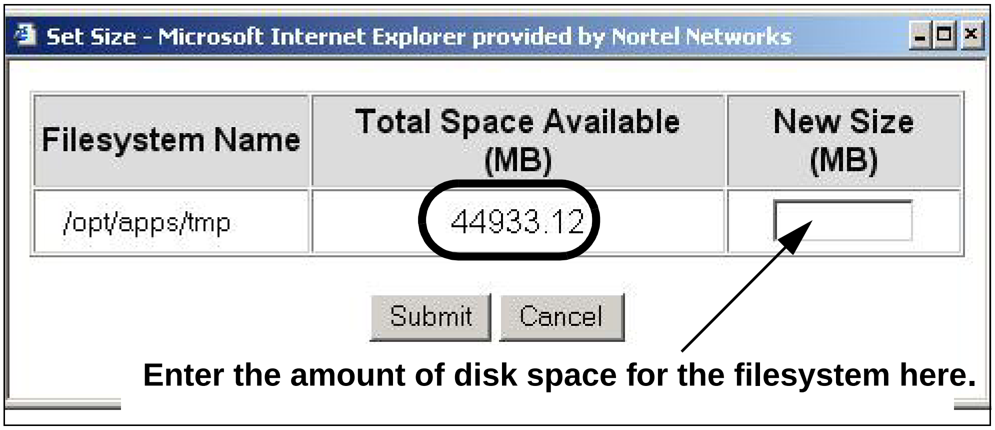


Create/Remove Filesystem

Type the name of the filesystem to be added here.

5 Enter the size of the filesystem to create in the New Size field then click the **Submit** button.

> ***Note:*** 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.



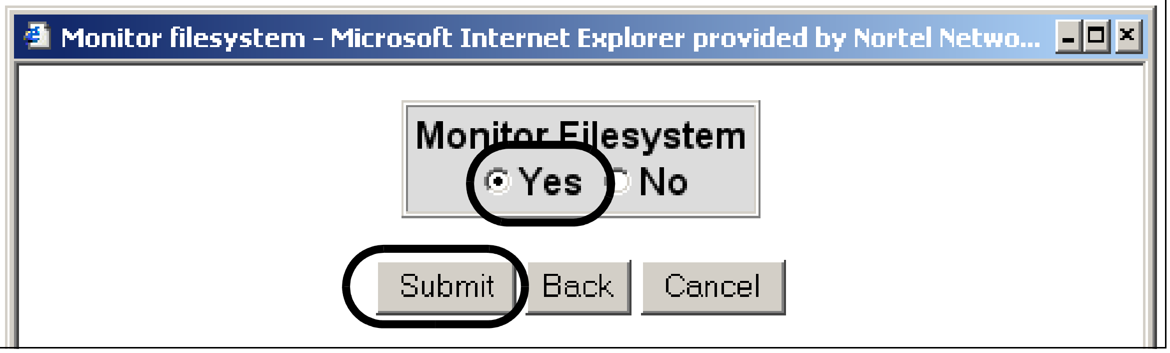
Set Size - Microsoft Internet Explorer provided by Nortel Networks

Filesystem Name	Total Space Available (MB)	New Size (MB)
/opt/apps/tmp	44933.12	

Enter the amount of disk space for the filesystem here.

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.

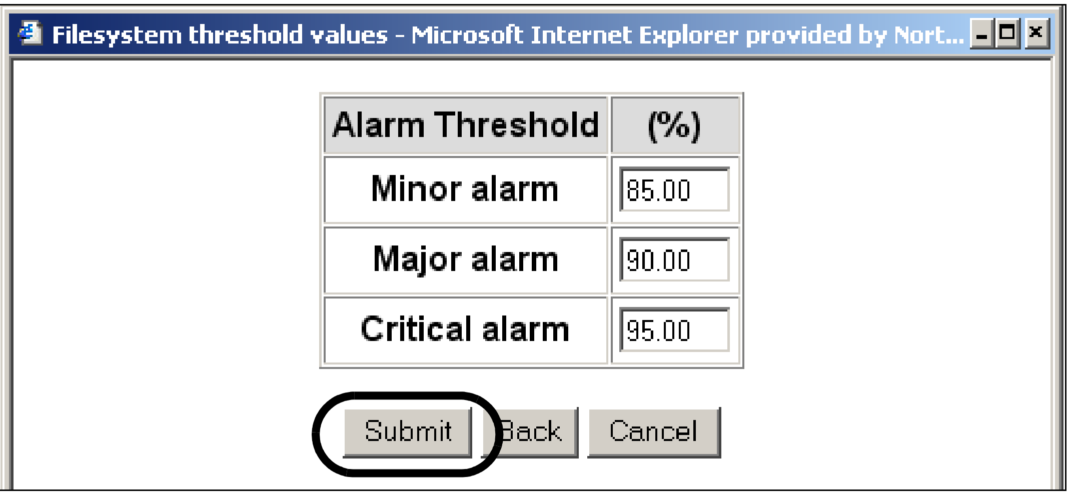

Monitor filesystem - Microsoft Internet Explorer provided by Nortel Netwo...

Monitor Filesystem
● Yes ○ No

7 If desired, change the alarm threshold values, then click **Submit**.

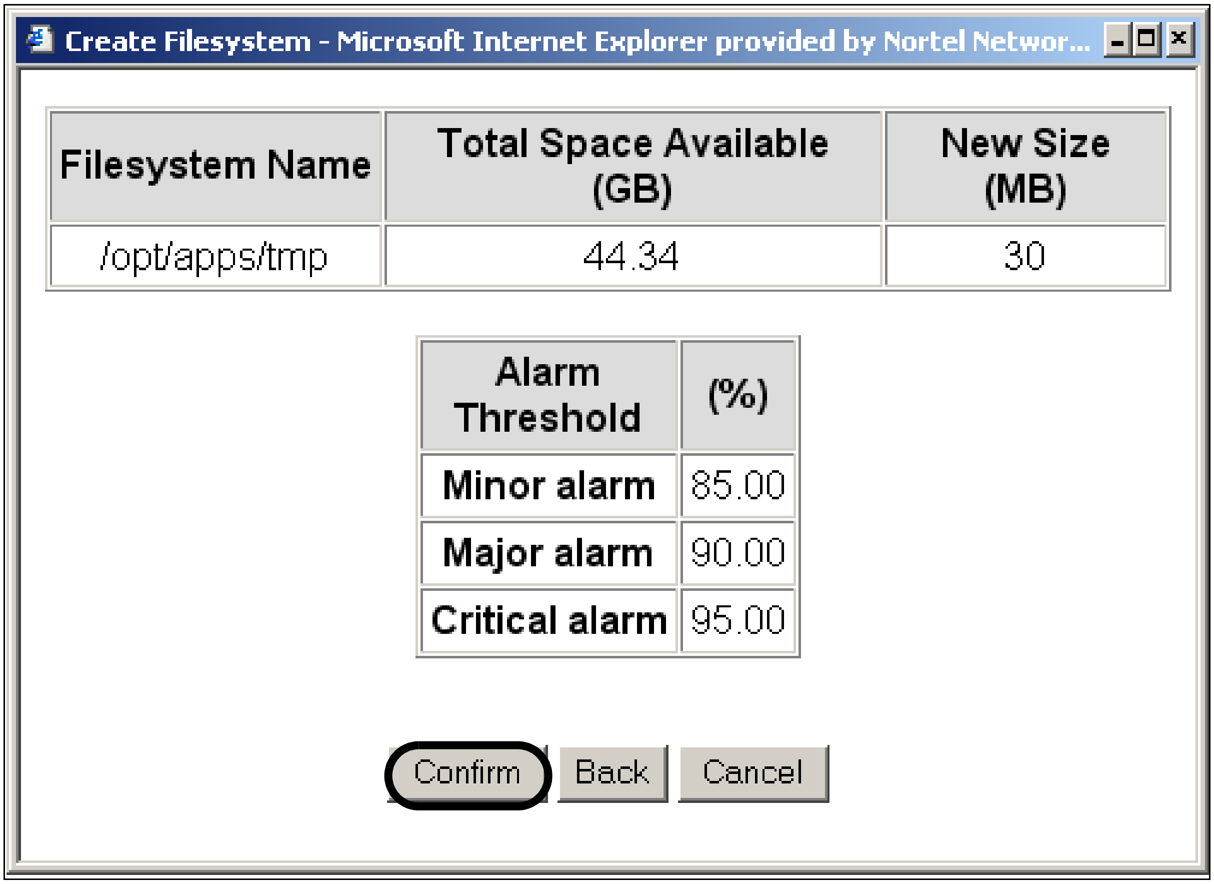
ATTENTION
Ensure that you enter the highest threshold value for the critical alarm and the lowest value or the minor alarm.

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.


Filesystem threshold values - Microsoft Internet Explorer provided by Nort...

Alarm Threshold	(%)
Minor alarm	85.00
Major alarm	90.00
Critical alarm	95.00

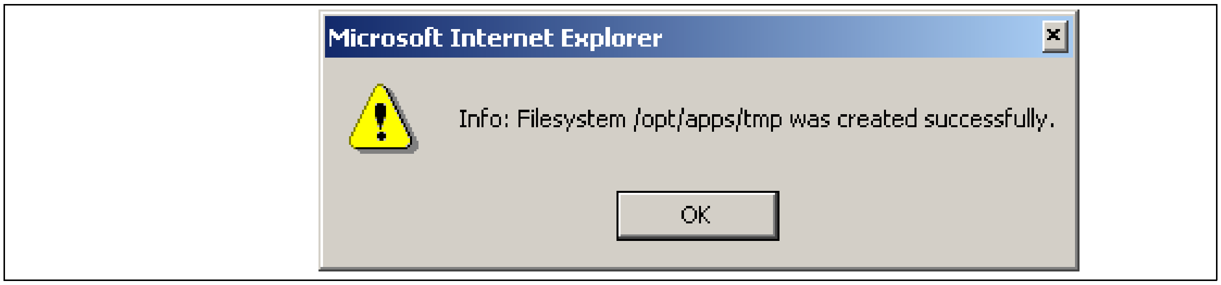
8 Review the provisioning data for the new filesystem and click **Confirm** to create the new filesystem, or click **Back** to make changes.


Create Filesystem - Microsoft Internet Explorer provided by Nortel Networ...

Filesystem Name	Total Space Available (GB)	New Size (MB)
/opt/apps/tmp	44.34	30

Alarm Threshold	(%)
Minor alarm	85.00
Major alarm	90.00
Critical alarm	95.00

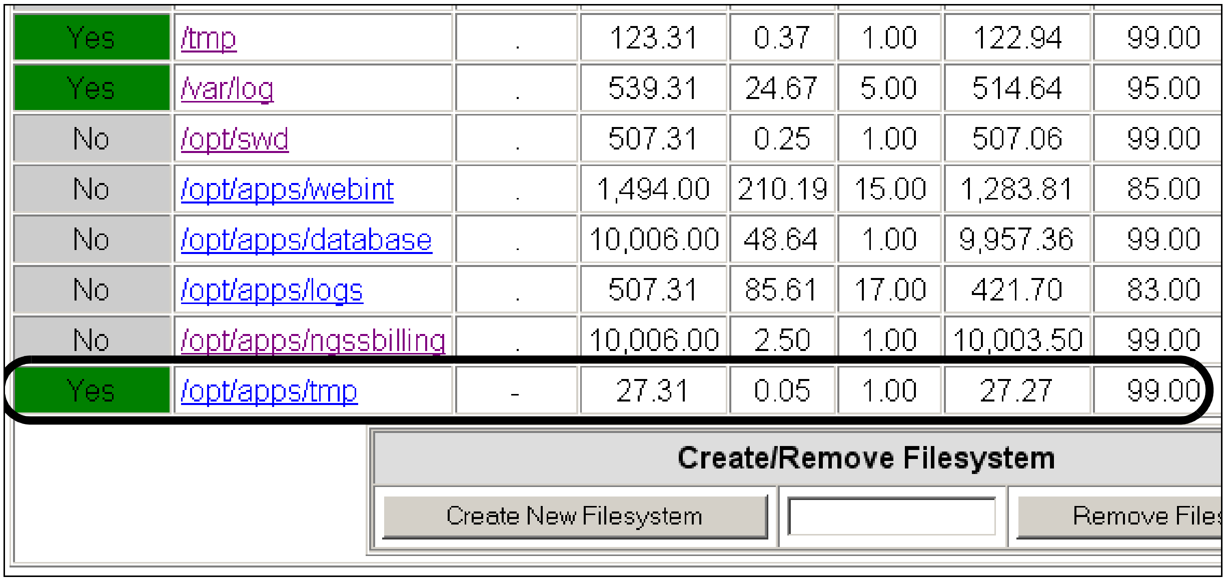
9 When the system indicates that the filesystem was successfully created, click **OK**.



Info: Filesystem /opt/apps/tmp was created successfully.

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) Session Server unit, using the same values and settings as you did for the first unit.

12 This procedure is complete.