Session Server Security and Administration

What's new in the (I)SN08 release?

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

- Features A00008383 and A00007275 - 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.
- Feature A00006893 - TLS Security adds transport layer security (TLS) to the SIP Gateway application. In SN08, TLS is used to secure SIP messaging communications between the SIP Gateway application and a remote SIP device such as an application server.

Security and administration strategy overview

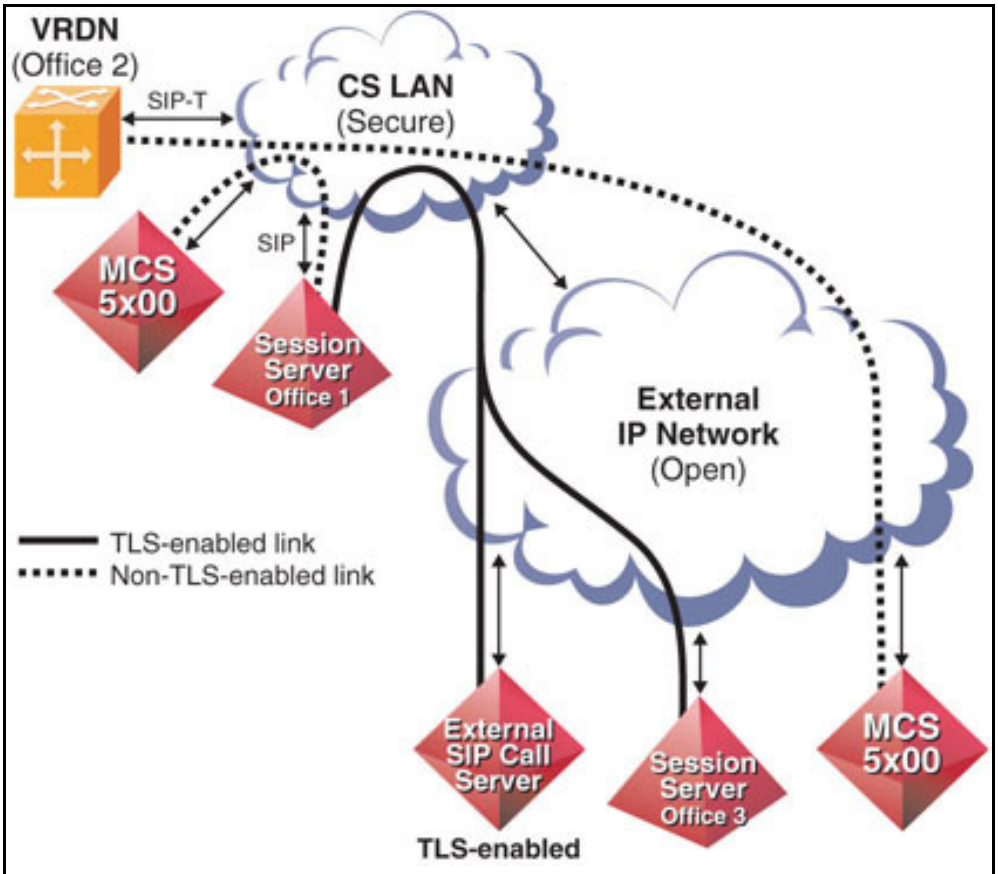
The security and administrative strategy for the Session Server centers around the following primary activities:

- Security administration of the Session Server, which includes managing user IDs and passwords, and acquiring security certificates
- Operational administration and maintenance of the Session Server platform and applications, which includes activities surrounding managing the Session Server platform NCGL (Nortel Carrier-grade Linux) and hardware as well as the SIP Gateway application software running on the platform
- Backing up the SIP Gateway application database, which focuses on maintaining a backup strategy of the SIP Gateway application database.

TLS Security for SIP messaging

In SN08, the TLS Security feature provides security for SIP connections using a security protocol -Transport Layer Security (TLS). This protocol enables secure data transmission for inter-call server communication, such as between the Session Server and a remote SIP application server.

The TLS feature will allow the Session Server to establish TLS sessions with a remote Call Server or SIP application server that is TLS aware. With the support of TLS on the Session Server, connections to a SIP enabled server can be secured over a non-secure network, like the internet, allowing SIP-based client/server applications to communicate with privacy and integrity.



Note: MCS 5x00 will not support TLS in SN08.

Provisioning options enable UDP, TCP or TLS (TCP) connections to be set up and utilized. Refer to the Session Server Configuration Management NTP, NN10338-511, for instructions on configuring TLS security. The TLS Security feature also provides security-related logs,

OMs, and alarms for monitoring security failures, potential attacks, and session establishment. Refer to the Session Server Fault Management NTP, NN10332-911, for instructions on monitoring security-related logs and alarms. Refer to the Session Server Performance Management NTP, NN10342-711, for instructions on monitoring security-related operational measurements.

Tools and utilities

Security administration and operational administration of the Session Server is performed primarily through the two Session Server web interfaces and a command line interface (CLI):

- CS 2000 NCGL Platform Manager
- CS 2000 Session Server Manager

Most system and operations administrative functions and security functions are performed using these interfaces, which are accessed from a single login point.

Backup and restore functions are performed using the Session Server CLI-based (command line interface) console provided by the NCGL.

An online help guide is available for the CS 2000 NCGL Platform Manager GUI only. Clicking the **Help** link opens a help file.

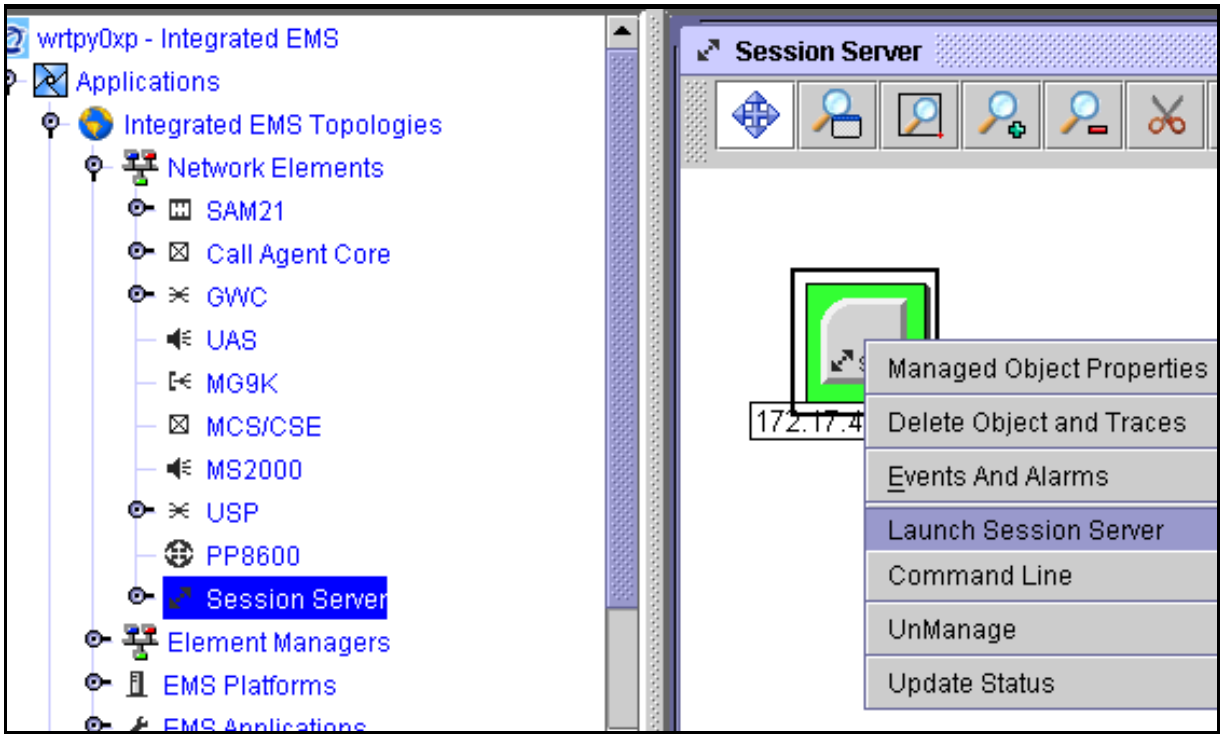
Methods of accessing Session Server GUIs and CLI

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 SSPFS proxy server (running on CS 2000 Management Tools server) on the CS-LAN. For more information, refer to procedure Access Session Server/NCGL GUIs using a proxied client on page 39. Refer to the Session Server Configuration Management NTP, NN10338-511, for more information about configuring a web proxy service on the SSPFS.
- 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.
- For commissioning purposes, 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 the

Session Server Configuration Management NTP, NN10338-511, for more information about using this CLI access method.

Security administration of the Session Server

Users of Nortel Networks operations, administration, maintenance and provisioning (OAM&P) client applications, which include the CS 2000 Session Server Manager and CS 2000 NCGL Platform Manager must belong to the primary group “succssn” for login access, and to one or more secondary user groups to specify the operations the user is authorized to perform.

Note: In SN07 and SN08, the CS 2000 NCGL Platform Manager GUI does not enforce group privileges when making changes. However, the CS 2000 Session Server Manager application GUI does enforce group privileges when making changes. Group privileges are set based on the group names shown in the table “Default groups.”

User and authorization categories

The following table of default groups are used on the Session Server, in similar fashion to the CS 2000 Management Tools Server SSPFS. These user groups are also consistent with the existing Carrier VoIP user categories on other Carrier VoIP component managers.

Default groups

Group Name	Group Number	Description
mgcadm	1011	Equivalent to being the root user
mgcmtc	1014	Can do any non-service impacting platform maint-enance activities. Cannot change provisioning data
mgcsprov	1013	Application provisioning user. Can modify provisioning data, but cannot take any platform maintenance actions.
mgcrw/ mgcro	1012/ 1015	Can view base or provisioning information but cannot initiate any changes
succssn	104	Required for all login access to the Session Server

The following table describes the default user names and associated secondary groups configured on a new Session Server platform.

Default user IDs on a new Session Server installation

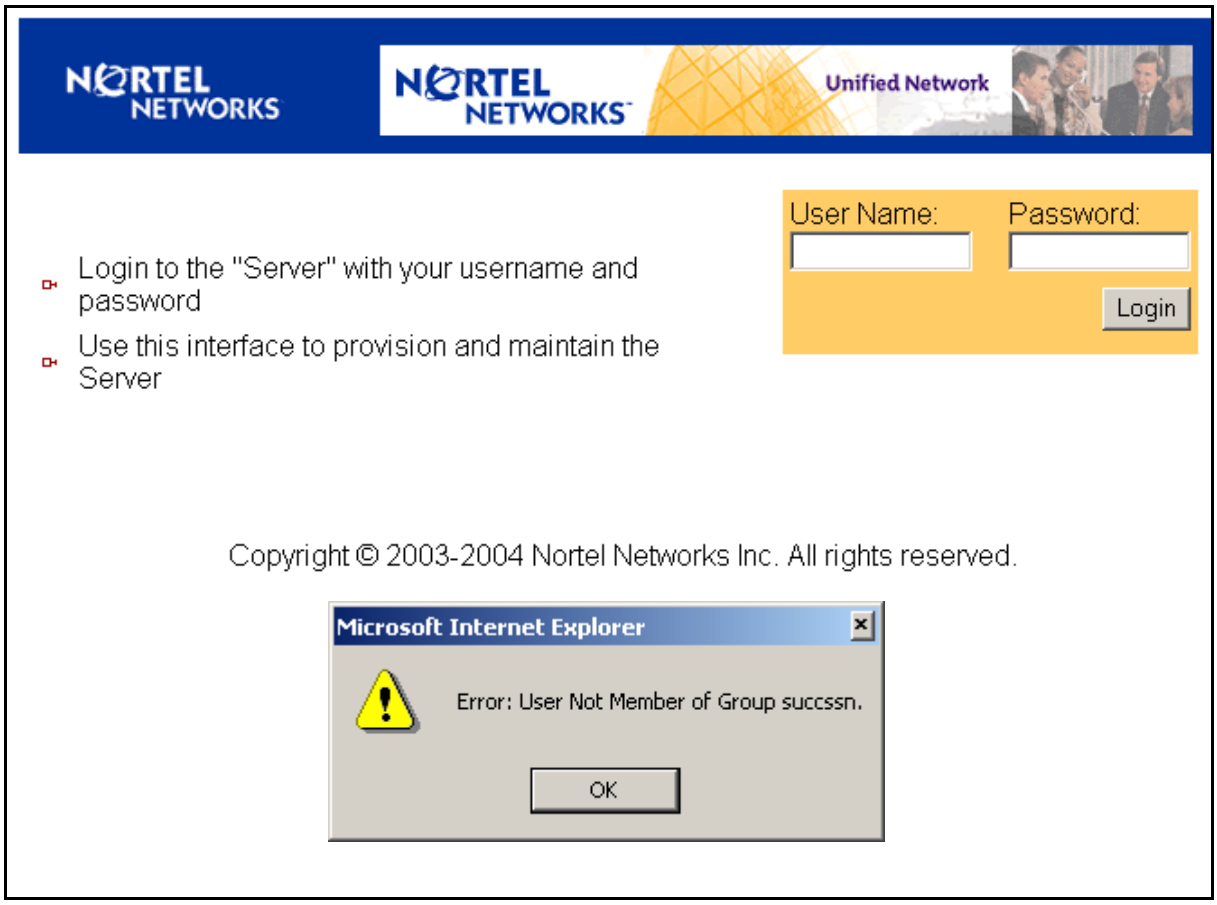
User Name	Groups	Description
root	root bin daemon sys adm disk wheel	System root user is not allowed when logging into the GUIs. Also, you cannot remotely log onto the Session Server console. You must log in as another user, then su (superuser) to the root user. The default root password is “sam39xts.” This password should be changed during commissioning of the Session Server units.
mtc	succssn users mtc mgcadm mgcrw mgcsprov mgcmtc mgcro	Session Server platform NCGL maintenance user. The default password for mtc user is “mtc.” This password should be changed during commissioning of the Session Server units. ***Note:*** The mtc user id should not be deleted. Doing so prevents command line interface (CLI) access from the Integrated EMS and web proxies. Also, the mtc user password must be a shared password account.

Using the root account for Session Server GUI access

Logging in to the Session Server's GUIs is not allowed using the root account. If you attempt to log into the Session Server GUI as root, you receive the error message shown in the following figure. To log in as root, you must access a command line interface at a Session Server console as another user type, then su to root super user. Refer to procedure Remote login using a secure shell (SSH) on page 27 to perform this activity.

Note: In general, Session Server GUI access permissions are controlled by the mgc group type. It is unnecessary to log on to the Session Server GUIs as the root account. For security reasons, it is not recommended that you configure the root account to be part of the primary group "succssn" for login access.

Login screen error message when trying to use the root account



Procedures for managing user accounts and passwords

ATTENTION
User accounts and passwords are not propagated to the Session Server mate unit. Therefore, account management activities such as setting up users, removing users, and changing passwords, must be performed on both servers.

The following is a list of the procedures for managing user accounts and passwords.

User account and password procedures

Procedure
Manage users on the Session Server platform on page 42
Manage user passwords using a Session Server console CLI on page 45
Manage user passwords with the Session Server GUI on page 47

Managing security certificates in SN08

A security certificate enables secure web browser-based communications for both Session Server GUIs and secure SIP signaling for the SIP Gateway application. There are two kinds of certificates that can be provisioned on the Session Server: self-signed certificates and CA-signed certificates (certificates signed by a certificate authority or CA).

For security reasons, Nortel recommends using CA-signed certificates. Whenever you update or change your security certificates, you should purchase a certificate from a trusted certificate authority (CA). If you need to install new security certificates after an upgrade of the Session Server, because you did not keep backup copies of the certificates, it is recommended that you purchase CA-signed certificates. To update or replace your security certificates, on both Session Server units, refer to procedure Renewing unexpired certificates on page 10.

The following files are used in managing security certificates:

- server.crt - Only the local server certificate is in this file. In the self-signed certificate option, this file is created automatically by the

tool. In the CA-signed option, this file will be provided by the customer, and placed in a temporary directory for import by the tool.

- trusted.crt - The certificate chain leading up to the root CA certificate is placed in this file. This file is provided by the customer, and placed in a temporary directory for import by the tool.
- server.key - This file contains the private key corresponding to the certificate in server.crt
- certificate.keystore - This file contains an encoded version of the server.crt, trusted.crt, and server.key file. This file is created automatically by the tool and is used by Tomcat web server.

MIgrating self-signed certificates from SN07 to SN08

Migrating self-signed certificates from SN07 to SN08 is not supported. You must create new self-signed certificates using activity Creating new self-signed certificates on page 11. This also applies to self-signed certificates that are about to expire. Refer to the Session Server Upgrades NTP, NN10349-461, for information about managing security certificates during an upgrade from SN07 to SN08.

Renewing expired CA-signed or self-signed certificates

Nortel always recommends renewing security certificates before they expire; however, if your site's CA-signed or self-signed certificates expire, then you must create new certificates to replace them. Although you can create either new CA-signed or self-signed certificates regardless of the type that expired, Nortel recommends that you replace your expired certificates with new CA-signed certificates.

- To renew expired CA-signed certificates, complete activity Creating new CA-signed certificates on page 10
- To renew expired self-signed certificates, complete activity Creating new self-signed certificates on page 11

ATTENTION

If your Session Server is configured to use TLS for SIP connections and your certificates expire, you will not be able to continue to make TLS-secured SIP calls.

ATTENTION

For security reasons, Nortel recommends that you always use CA-signed certificates. If your self-signed certificates expired, then they should be replaced with CA-signed certificates.

Renewing unexpired certificates

Unexpired certificates may need to be renewed or replaced when existing certificates become corrupted due to a system or database fault. They may also need to be replaced when a system's security is compromised to an unknown extent.

- To renew unexpired CA-signed certificates, complete activity Creating new CA-signed certificates on page 10
- To renew unexpired self-signed certificates, complete activity Creating new self-signed certificates on page 11

ATTENTION
For security reasons, Nortel recommends that you always replace sign-signed certificates with CA-signed certificates.

Migrating from self-signed to CA-signed certificates

If you are currently using unexpired self-signed certificates and want to migrate your Session Server to using CA-signed certificates, refer to section Creating new CA-signed certificates on page 10 and complete the activity for creating new CA-signed certificates, which will replace your self-signed certificates.

Creating new CA-signed certificates

Complete the following procedures, in the order shown, starting on the inactive unit to create new CA-signed security certificates

Step	Procedures
1	Back up your existing security certificates using procedure Back up security certificates on page 140.
2	Complete procedure Generate a certificate signing request on page 154.
3	Send the completed certificate signing request to a Certificate Authority for signing and certificate generation. **Note:** It can take up to several weeks to receive a signed certificate back from a Certificate Authority.
4	Once the CA-signed certificate is received, validate the certificate chain by completing procedure Import certificates and private key on page 166 on the inactive unit.

Step	Procedures
5	Complete procedure Apply security certificates on page 174 to make the new certificates available to applications and GUIs used by the Session Server.
6	SwAct the units. Refer to Invoke a maintenance SWACT of the Session Server - Trunks platform on page 51
7	Complete procedure Copy security certificates to the mate unit on page 172.
8	On the newly inactive unit, perform Apply security certificates on page 174.
9	Back up your existing security certificates using procedure Back up security certificates on page 140.

Creating new self-signed certificates

Complete the following procedures, in the order shown, starting on the inactive unit to create new self-signed security certificates

Step	Procedures
1	Complete procedure Generate self-signed security certificates on page 143 on the inactive unit.
2	Complete procedure Apply security certificates on page 174 to make the new certificates available to applications and GUIs used by the Session Server.
3	SwAct the units. Refer to Invoke a maintenance SWACT of the Session Server - Trunks platform on page 51
4	Complete procedure Copy security certificates to the mate unit on page 172.
5	On the newly inactive unit, perform Apply security certificates on page 174.
6	Back up your existing security certificates using procedure Back up security certificates on page 140.

Using the certificate management tool

New certificates are created and managed using the CS 2000 Session Server Manager GUI and the CLI-based *cert_mgnt* tool. The cert_mgnt tool is run on one Session Server unit only (usually the standby unit), and the certificate files that are created are copied to the mate unit.

The following restrictions apply to using the certificate management tool:

- You must be a root user to use the certificate management tool.
- Only PEM formatted, CA-signed certificates are supported on the Session Server.
- CA chain is required in PEM format in a trusted.crt file, top down with the root CA at the top
- There are additional files (cert_gen.txt and assign_cert.txt) in the /opt/base/share/ssl directory. These files are used by the cert_mgnt tool and should not be removed.

The directory /opt/base/share/ssl, where the security certificates are stored, should be backed up on a regular basis using a secure method, in a physically and logically secure environment, to help prevent unauthorized access to the private keys.

Managing trusted certificates for remote servers

The following are procedures are used for managing trusted security certificates of remote servers known the SIP Gateway application:

Procedures for managing security certificates

Procedure
Display local server certificates on page 182
Manage Trusted Certificates on page 176

Operational administration and maintenance of the Session Server platform and applications

This section provides the procedures available to manage the Session Server and its applications, including:

- Managing operation of the NCGL platform and hardware for each Session Server unit
- Managing operation of the SIP Gateway application on both units to ensure uninterrupted call processing

The following operational administrative and maintenance activities are available to be performed on the Session Server NCGL platform:

- Jam and Unjam - manually prevent a switch of activity (SwAct) to the standby unit. Jam and Unjam are performed in cases where a Session Server unit is faulty and is about to be replaced, when

configuration or maintenance activities are being performed, or when the standby unit is unavailable.

- Switch of Activity (SwAct) - switch the active unit to the standby (mate unit). Refer to section Understanding conditions for a SWACT on page 16 for details about types of SwActs and the conditions required to perform a SwAct.
- Switch active link (Swlink) - switch the active communications links in both the active and standby Session Server units.
- Network ethernet link Lock and Unlock - shut down the ethernet interfaces and isolate a single Session Server unit from the network. Refer to section Managing Session Server ethernet links on page 19 for more information.

The following activities can be performed on the SIP Gateway application to change its operational and administrative state:

- Taking the SIP Gateway application from out-of-service to in-service
- Unsuspend followed by Unlock
- Taking the SIP Gateway application from in-service to out-of-service
- Lock followed by Suspend

Interpreting SIP Gateway application states

SIP Gateway application maintenance uses the CCITT X.731 state and status attributes as well as X.731 commands to be consistent with other Carrier VoIP component platforms. The following table shows the four fields that comprise the CCITT X.731 state of the SIP Gateway application. The last column in the table provides a mapping to legacy DMS-style states to aid in understanding.

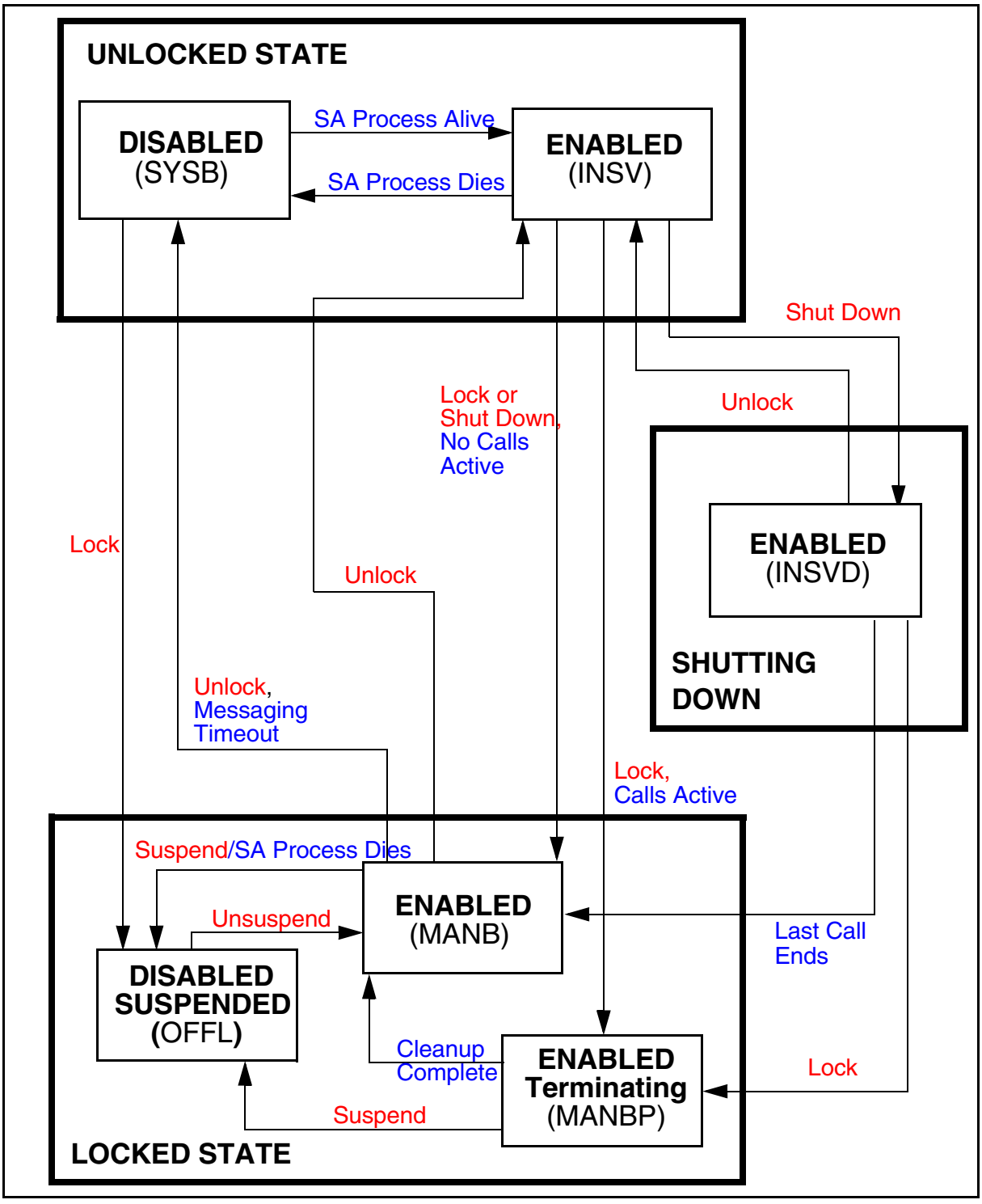
Administrative State	Operational State	Procedural Status	Control Status	DMS Style States
Locked	Disabled	-	Suspended	OFFL
Locked	Enabled	-	-	MANB
Locked	Enabled	Terminating	-	MANBP
Unlocked	Enabled	-	-	INSV
Unlocked	Disabled	-	-	SYSB
Shutting Down	Enabled	-	-	INSVD

The following table explains the controls that are allowed based on the current Admin State, Operational State, and Procedural Status of the SIP Gateway application. Legacy DMS style representation is shown in parentheses to aid in understanding.

Operational State	Admin State	Procedural Status	Control Status	Allowed Controls DMS Style Commands in ()'s
Locked	Disabled	-	Suspended	Admin Control None Control Status Unsuspend (BSY)
Locked	Enabled	-	-	Admin Control Unlock (RTS) Control Status Suspend (OFFL)
Locked	Enabled	Terminating	-	Admin Control None Control Status: Suspend (OFFL)
Unlocked	Enabled	-	-	Admin Control Lock (BSYFORCE) Shut Down (BSY) Control Status None
Unlocked	Disabled	-	-	Admin Control Lock (OFFL) Control Status None
Shutting Down	Enabled	-	-	Admin Control Lock (BSYFORCE) Unlock (RTS) Control Status None

The following state diagram shows how maintenance states transition from one to the other. The legacy DMS system commands are shown in parentheses to aid in understanding. Commands that can be executed are listed in red, while messaging and state transitions are listed in blue.

SIP Gateway application maintenance state diagram



Understanding conditions for a SWACT

There are three types of SwAct supported on the Session Server NCGL platform:

- a manual SwAct (forced or unforced)
- a system initiated SwAct
- an application requested SwAct

Swacts are executed depending on the state of the system and any failure conditions, according to the following rules:

SwActs cannot occur under the following circumstances:

- when the node is running in a simplex configuration; where the inactive unit is unavailable
- when the inactive unit is completely isolated and unreachable or is in a Jammed state
- critical failure conditions exist on the inactive unit that prevent a SwAct
- the SIP Gateway application rejects a SwAct request

SwAct always occur under the following circumstance:

- a forced manual SwAct is initiated
- critical failure conditions on the active side cause a system-initiated swact.

Rules for SwActs are summarized in the following table:

Unit status		Applications accept the SWACT			
Active	**Inactive**	**Manual or Application requested SWACT**	**System Initiated SWACT**	**Application rejects SWACT**	**Manual "Force" SWACT**
Not critical	Not critical	SWACT	not applicable	no action taken	SWACT
Not critical	critical failure	no action taken	not applicable	no action taken	SWACT
critical failure	Not critical	not applicable	SWACT	no action taken	SWACT

Unit status		Applications accept the SWACT			
Active	Inactive	Manual or Application requested SWACT	System Initiated SWACT	Application rejects SWACT	Manual "Force" SWACT
critical failure	critical failure	no action taken	no action taken	no action taken	SWACT

In the previous table discussing rules for a SwAct, "critical failure" conditions are mentioned. Note that the conditions that would initiate a SwAct on the active side are the same conditions that would inhibit a SwAct due to a failed inactive unit. These conditions correspond to the following cases:

- a unit is not available because it has experienced a power loss, or is in the process of rebooting
- the Sanity watchdog timer times out, a kernel panic is generated or critical hardware failure occurs
- critical network monitoring-related alarms are generated, indicating that the active unit is becoming isolated or otherwise no longer responding to its mate
- one or both of the disk drives fails on a unit
- a manual SwAct is initiated to a unit which has a single disk missing/fail alarm

The following events are not included the "critical failure" conditions, even though some alarms for these events may be categorized as "critical" in the alarm view:

- major or minor alarms for connectivity and most hardware faults
- Most hardware failures, including power supply faults, voltage and temperature conditions, fan, CPU and memory
- NCGL operating system faults, including zombie processes, cpu usage and memory usage faults
- disk usage faults

Note 1: The operating system status critical alarm is not symmetrical, in that it prevents a SwAct, but does not cause a system initiated SwAct.

Note 2: For more information about faults, alarms and fault conditions, refer to the Session Server Fault Management NTP, NN10332-911.

Operational administration procedures for the Session Server platform

The following operational administration procedures are available for managing the Session Server NCGL platform and unit hardware:

System administration procedures

Procedure
Power-On and boot a Session Server unit on page 139
Power-Off a Session Server unit on page 137
Halt (shutdown) a Session Server unit on page 80
View the operational status of the NCGL platform on page 99
Reboot a unit on page 84
Access Session Server/NCGL GUIs or CLI using the IEMS on page 28
Access Session Server/NCGL GUIs using a proxied client on page 39

Operational administration procedures for the SIP Gateway application

The following table lists administrative procedures available for controlling the SIP Gateway application.

Operational administration procedures

Procedure
Invoke a maintenance SWACT of the Session Server - Trunks platform on page 51
Invoke a manual cold SwAct of the SIP Gateway application on page 57
Inhibit a system SwAct (Jam) on page 65
Enable a system SwAct (Unjam) on page 70
View the operational status of the SIP Gateway application on page 93
Lock the SIP Gateway application on page 117
Unlock the SIP Gateway application on page 121

Operational administration procedures

Procedure
Suspend the SIP Gateway application on page 124
Unsuspend the SIP Gateway application on page 128
Query current number of SIP calls on page 24
Verify synchronization status on page 90

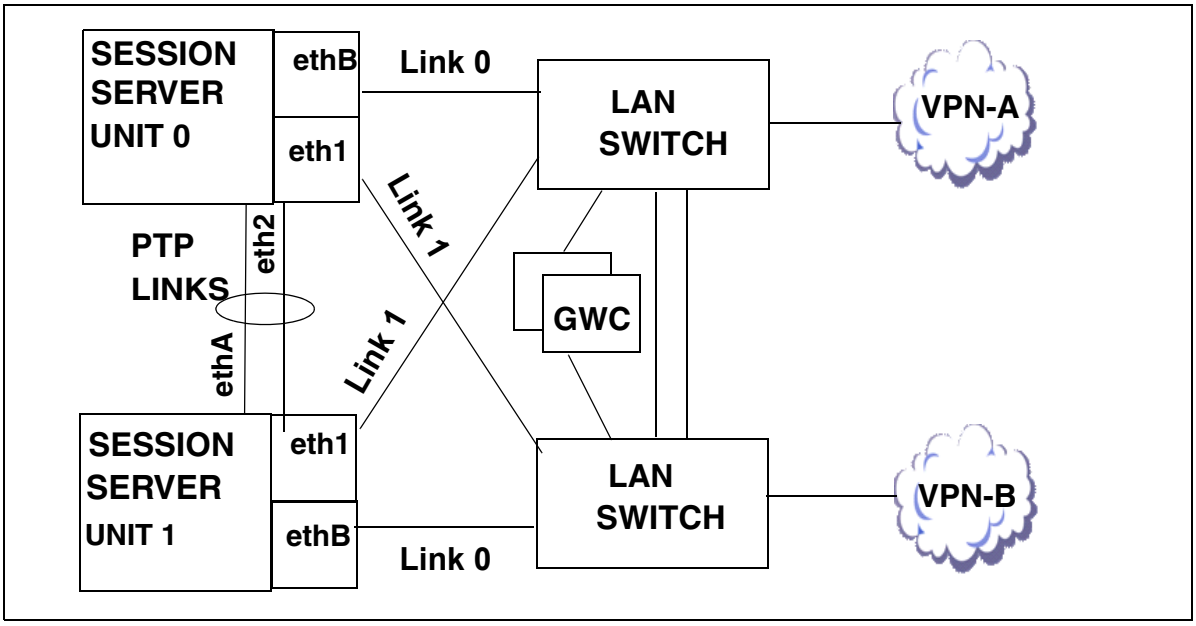
Determining the status of SIP access links

In the XA-Core, the status of an access link can be monitored by posting the associated SIP-T trunk group at the MAPCI;MTC;TRKS;DPTRKS level of the MAP. The association of the trunk group to an access link is defined in CM table SIPLINK, and is used to manage routing of incoming and outgoing SIP calls. Since the XA-Core has no direct communication with the Session Server, it is dependent on receiving link status information from the SIP-T GWCs, which receive access link status messages from the Session Server and pass them on to the XA-Core. Refer to the CS 2000 Security and Administration NTP associated with your solution for more information about posting an associated SIP-T trunk group.

Managing Session Server ethernet links

The following figure shows each Session Server unit to be configured with two gigabit ethernet interfaces (shown as link 0 and link 1). These are directed to the LAN switch that routes call traffic and signalling on the customer's private central office (CO) network. In addition, two ethernet interfaces, acting as Point To Point (PTP) links, connect unit 0 to unit 1.

Map of Session Server ethernet ports and link configuration



Ethernet link management procedures for Session Server

The following table lists the link management procedures:

Operational administration procedures

Procedure
Invoke a manual switch of active links (Swlink) on page 61
Lock network ethernet link on page 74
Unlock network ethernet link on page 77

Performing a controlled shutdown of a Session Server node

Execute the procedures in the following activity to perform a controlled shutdown of a Session Server node. Use this activity in the event of an impending power failure at the physical site or for any other conditions requiring shutting down the entire node.

CAUTION

This is a service affecting procedure. Executing the procedures in this activity releases all SIP calls in progress, regardless of call state, and causes an outage of all SIP media communications and shuts down all DPT trunk communications.

Step	Procedure
1	If necessary, ensure that a backup copy of the SIP Gateway application database has been made using procedure Session Server - Trunks backup on page 131.
2	Perform procedure Lock the SIP Gateway application on page 117 on the active unit.
3	Perform procedure Suspend the SIP Gateway application on page 124 on the active unit.
4	Perform procedure Halt (shutdown) a Session Server unit on page 80 on the inactive unit. ***Note:*** The state of the SIP Gateway application is saved when the unit is powered off. When the unit is powered up, the SIP Gateway application initializes in the same state in which it was powered down.
5	Perform procedure Power-Off a Session Server unit on page 137 on the inactive unit.
6	Perform procedure Halt (shutdown) a Session Server unit on page 80 on the active unit. ***Note:*** The state of the SIP Gateway application is saved when the unit is powered off. When the unit is powered up, the SIP Gateway application initializes in the same state in which it was powered down.
7	Perform procedure Power-Off a Session Server unit on page 137 on the active unit.

Backing up the SIP Gateway application database

Database backups secure the information stored in the SIP Gateway application database. In the event that there is a complete failure of both Session Server units in the node or if an unrecoverable corruption in the database on the active unit occurs, a copy of the database can be restored from a backup.

Ordinarily, there is only one backup copy of the SIP application database. It contains the last or most recently backed up copy (within the last 24 hours) of the database. The backup file is named **solid.db** and is located at the following path on the active Session Server disk drive:

/opt/apps/database/solid/backup/solid.db

There is only a single backup copy of the database saved on each unit. It contains the last or most recently backed up copy (within the last 24 hours) of the database. The database on each unit is automatically backed up at 1:00 AM each day. The time of day for the backup or the content set of the backup cannot be changed by the customer; however, the customer can perform a manual backup of the database on an as-needed basis such as when an upgrade activity is scheduled. It is recommended that manual backups be performed on the active database.

If additional security measures are required, the customer may periodically retrieve the files saved in the backup directory and store them on another system. By regularly saving copies of the backup database, a customer can maintain a history of database changes.

The following table lists the procedures available to backup the SIP Gateway application database.

Database backup procedures

Procedure
Session Server - Trunks backup on page 131

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.

Query current number of SIP calls

Purpose of this procedure

Use this procedure to determine how many SIP calls are currently being processed by the Session Server node.

Limitations and restrictions

Only active calls are reported, including calls in setup and termination.

The SIP Gateway application must be in one of the following states to report the number of active SIP calls. Use the SIP Gateway Status panel (shown below) to determine the state of the application:

- In service (Unlocked, Enabled, -, -)
- In service but shutting down (Shutting Down, Enabled, -, -)
- Locked or ManB (Locked, Enabled, Terminating, -)

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

Prerequisites

There are no prerequisites for performing this procedure.

Action

At the CS 2000 Session Server Launch Point

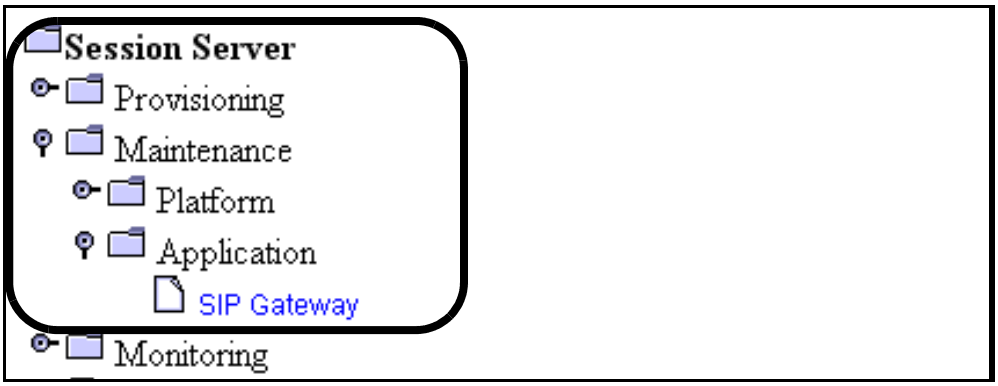
1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.

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:

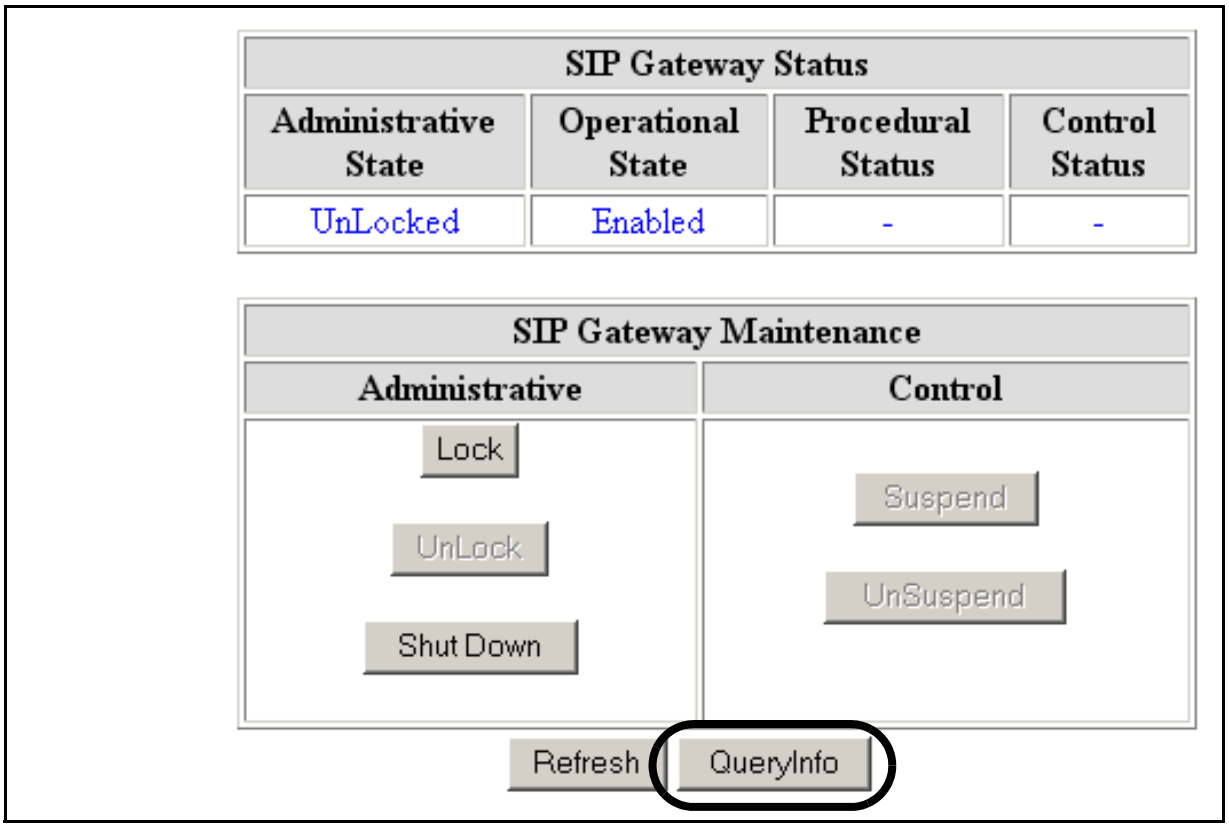
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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



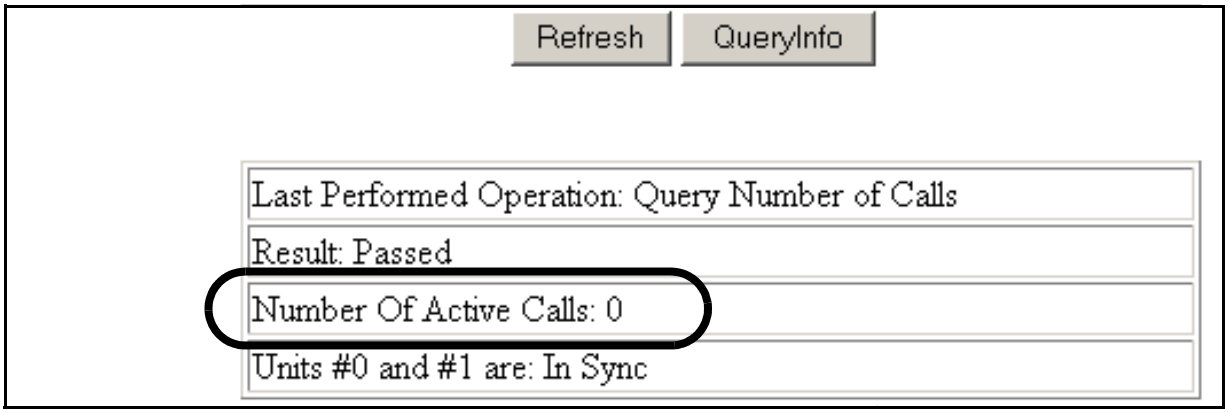
3 Click on the **SIP Gateway** folder to open it.

4 At the bottom of the SIP Gateway Maintenance panel, locate and click the **QueryInfo** button.



5 The number of currently active calls is displayed in the table below the **QueryInfo** button.

Note: The status panel is refreshed according the value shown in the drop down box at the bottom of the status panel. When refresh occurs, the info box disappears. If necessary, to increase the refresh rate, select a larger value from the drop down menu and click the **Refresh Rate** button.



6 The procedure is complete.

Remote login using a secure shell (SSH)

Purpose of this procedure

This procedure is used to log in to the active unit with the CLI (command line interface) from a remote client system that has access to the secure CS LAN and has access permissions as setup on the proxy server running on the CS 2000 Management Tools server.

You can also log in using a console connected to the rear of the active unit.

Limitations and Restrictions

Telnet is not supported.

Prerequisites

The remote client must have access to the secure CS LAN and must have access permissions as setup on the proxy server running on the CS 2000 Management Tools server.

Action

From a remote client that supports SSH on the CS LAN

1 Open a secure shell to the Session Server by typing

> ssh -l <userid> <IP_address>

and pressing the Enter key.

where

userid
is a valid userid (like mtc)

IP_address
is the IP address or host name

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 If applicable, change to the root user by typing

su - root

4 When prompted, enter the root password.

5 You have completed this procedure.

Access Session Server/NCGL GUIs or CLI using the IEMS

Purpose of this procedure

This procedure describes how to access the Session Server web-based GUIs (CS 2000 NCGL Platform Manager and CS 2000 Session Server Manager) or the command line interface (CLI) using the IEMS Java Webstart Client.

For the inactive unit only, you can also use this procedure to access the CS 2000 NCGL Platform Manager GUI and Command Line Interface.

Limitations and Restrictions

This procedure is not a comprehensive guide to using the IEMS for access to the Session Server, for OAM&P activities. For more information about using the IEMS and performing OAM&P activities using IEMS refer to *IEMS Basics*, NN10329-111.

When attempting to access the Session Server GUI, access to the active unit is only supported for non-upgrade activities. Accessing the active Session Server unit GUIs is supported in the methods provided in this document.

You will be required to enter your login information two or more times to access the Session Server GUI through the IEMS as the IEMS and the Session Server each validate login information individually.

Prerequisites

The Session Server must be configured for access from the IEMS.

Action

If you want to access the active Session Server unit user interfaces (the unit currently controlling the node), use procedure Accessing the active Session Server unit user interfaces on page 28

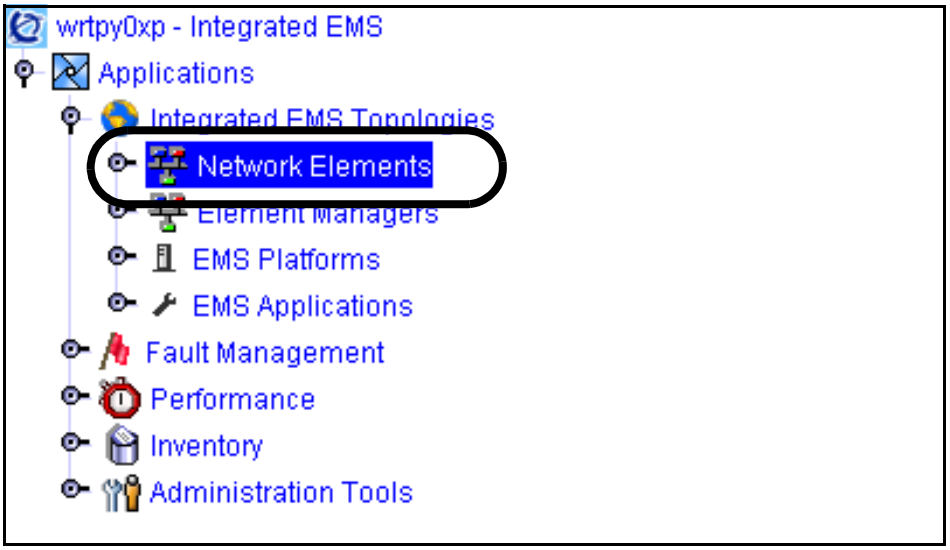
If you want to access the inactive Session Server unit user interfaces, use procedure Accessing the inactive Session Server unit user interfaces on page 32

Accessing the active Session Server unit user interfaces

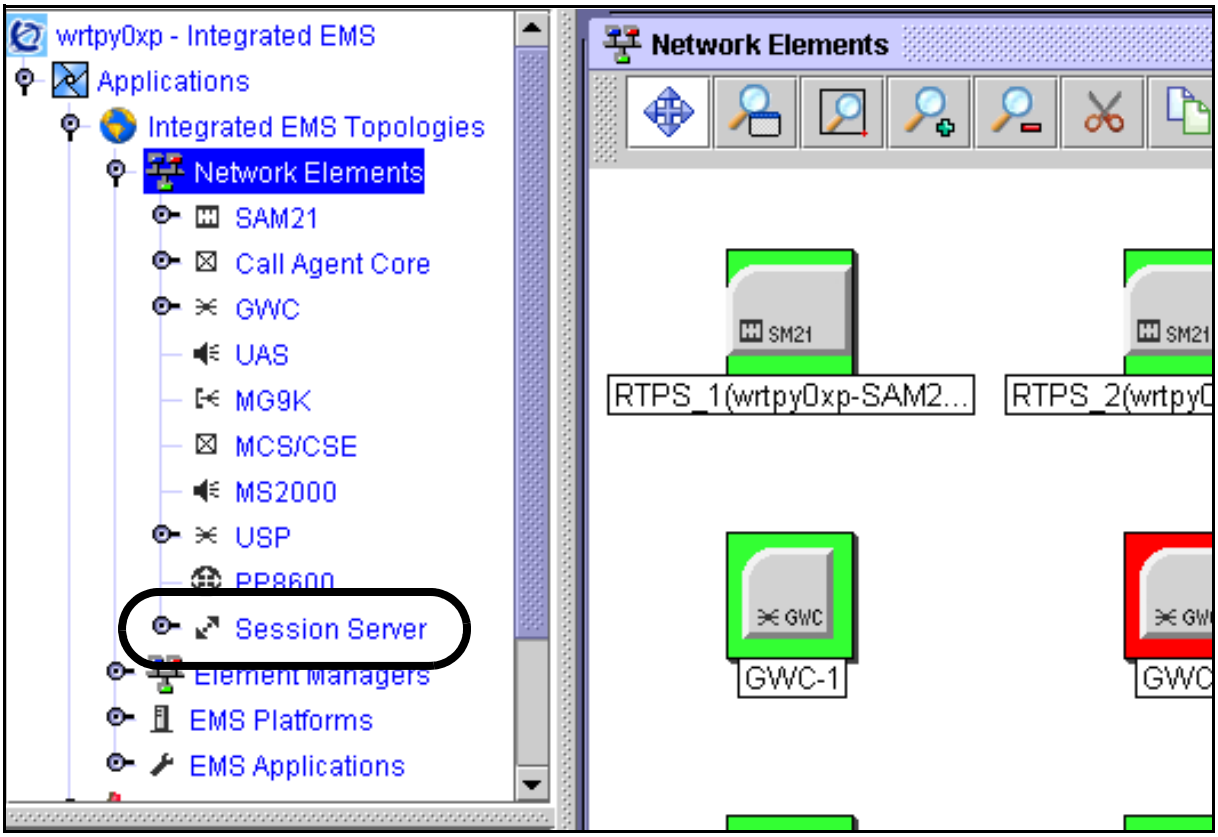
At a workstation or console running the IEMS client

1 If necessary, log into the IEMS Java Webstart Client.

2 Select the **Network Elements** view.



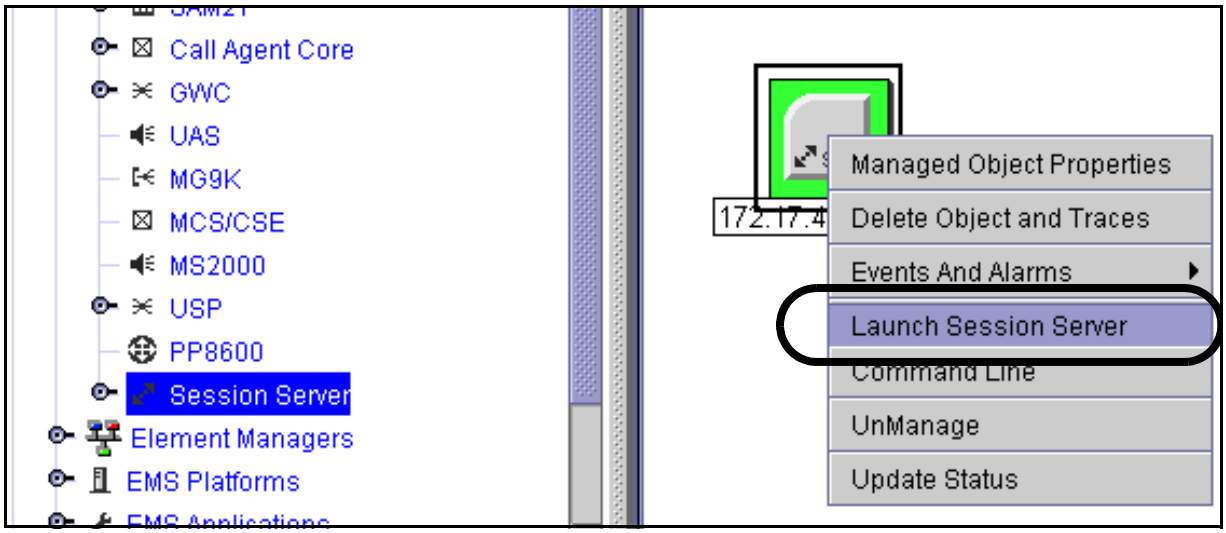
3 In the Network Elements view locate and click the Session Server element.



4 Use the following table to determine your next step.

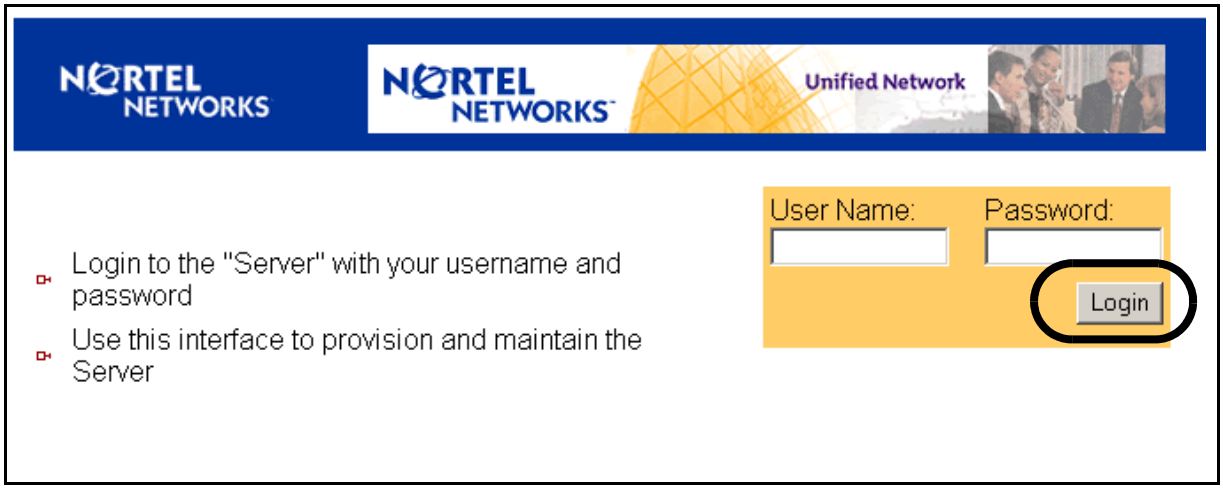
If	Do
you want to launch a Command Line (CLI) session	step 10
you want to launch either of the active unit GUIs	step 5

5 To launch either of the active unit Session Server GUIs, right-click on the Session Server Node icon and select **Launch Session Server.**



6 Confirm any security alerts.

7 At the login screen enter your user id and password, then click the **Login** button.



8 Select the GUI you want to launch 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:

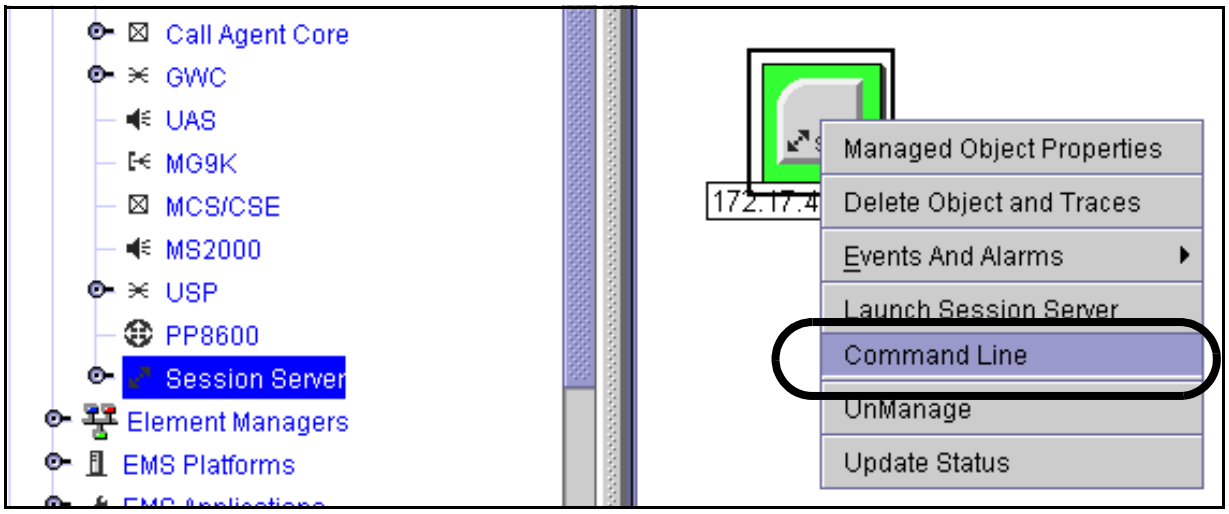
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

or

Logout

9 Skip to step step 13.

10 To launch a Session Server Command Line session, right-click on the Session Server Node icon and select **Command Line** from the menu.



A secure shell (SSH) command line login window is presented.

11 If prompted to log onto the CS 2000 Management Tools server, enter the user id and password for the maintenance user.

12 At the login prompt enter the Session Server mtc user id and password.

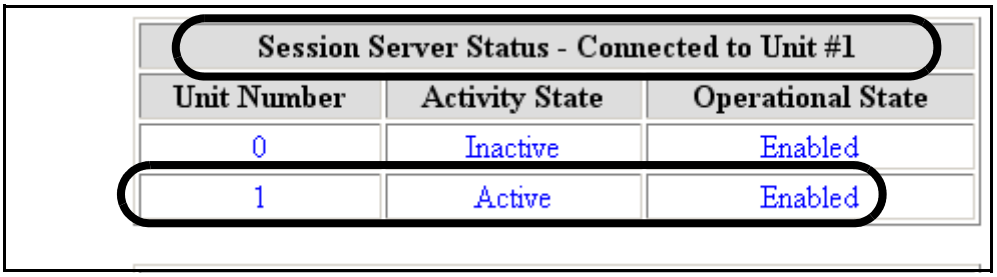
13 You have completed this procedure.

Accessing the inactive Session Server unit user interfaces

Use this procedure to access the CS 2000 NCGL Platform Manager GUI or Command Line Interface on the inactive unit only. Use this procedure for performing upgrade activities and other activities that require access to the inactive unit NCGL manager.

ATTENTION

You can not access the CS 2000 Session Server Manager GUI from the inactive unit. You can only access the CS 2000 Session Server Manager GUI from the active unit. Clicking on the CS 2000 Session Server Manager GUI link from the *inactive* unit launch point will automatically take you to the CS 2000 Session Server Manager on the *active* unit.

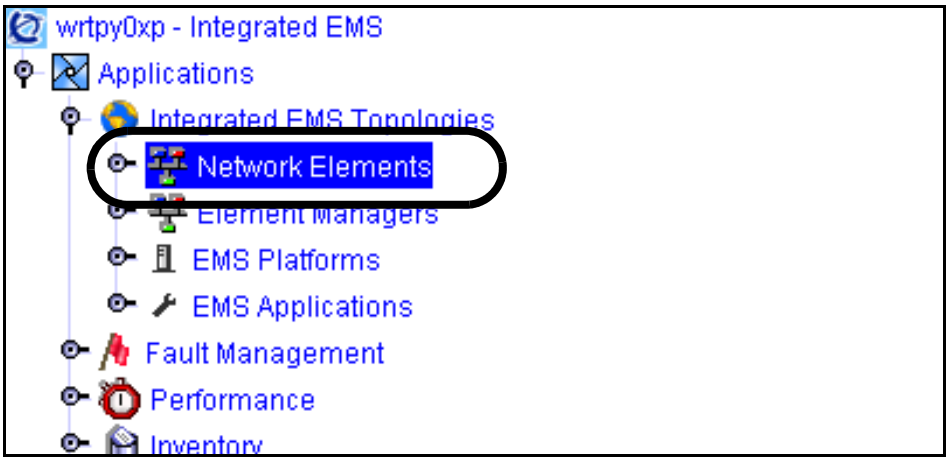


Accessing the inactive Session Server unit user interfaces

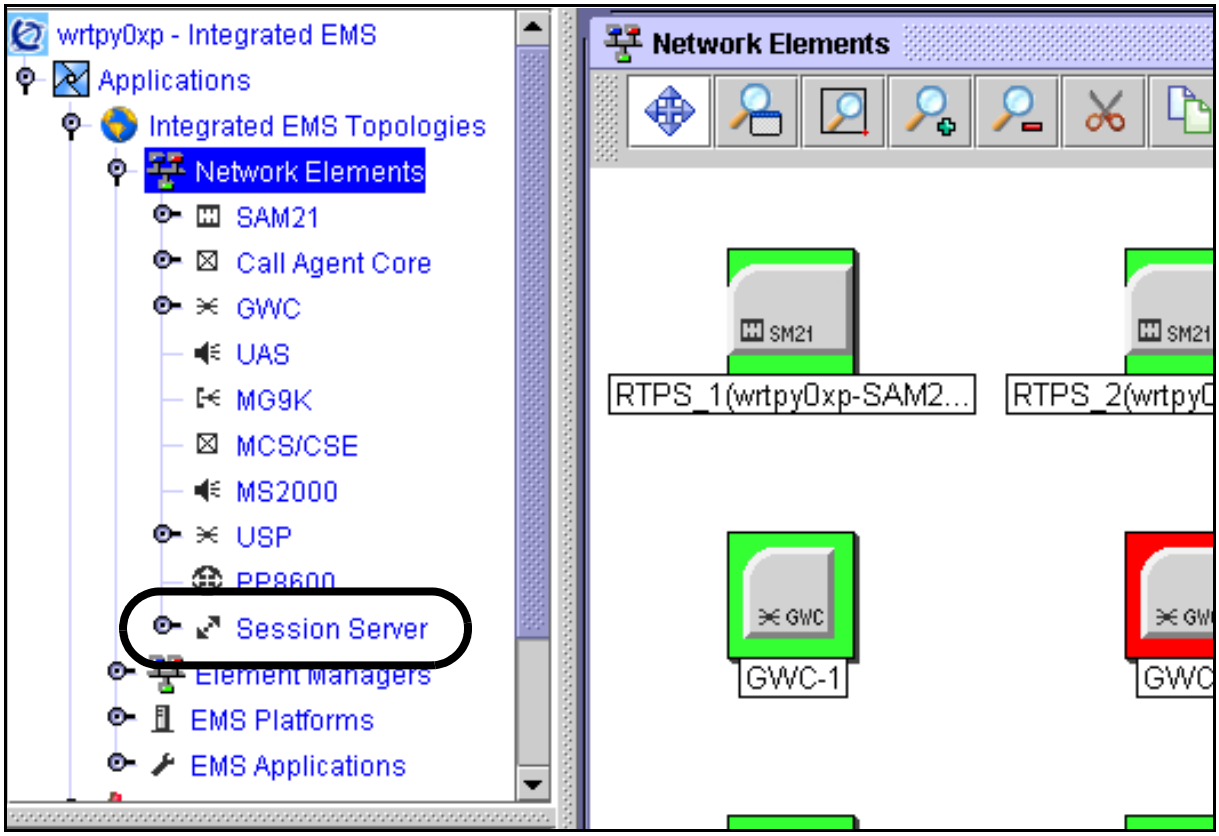
At a workstation or console running the IEMS client

1 If necessary, log into the IEMS Java Webstart Client.

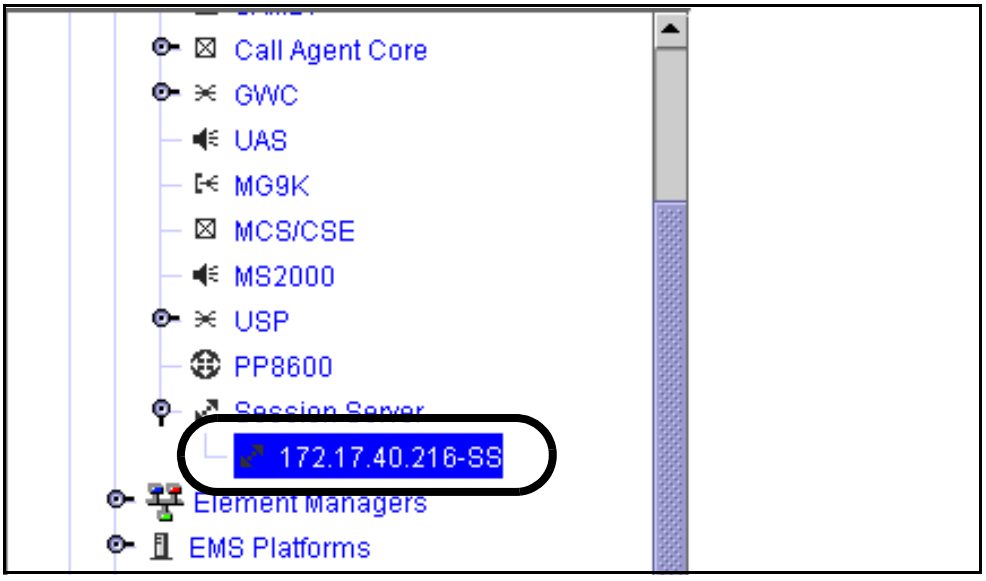
2 Select the **Network Elements** view.



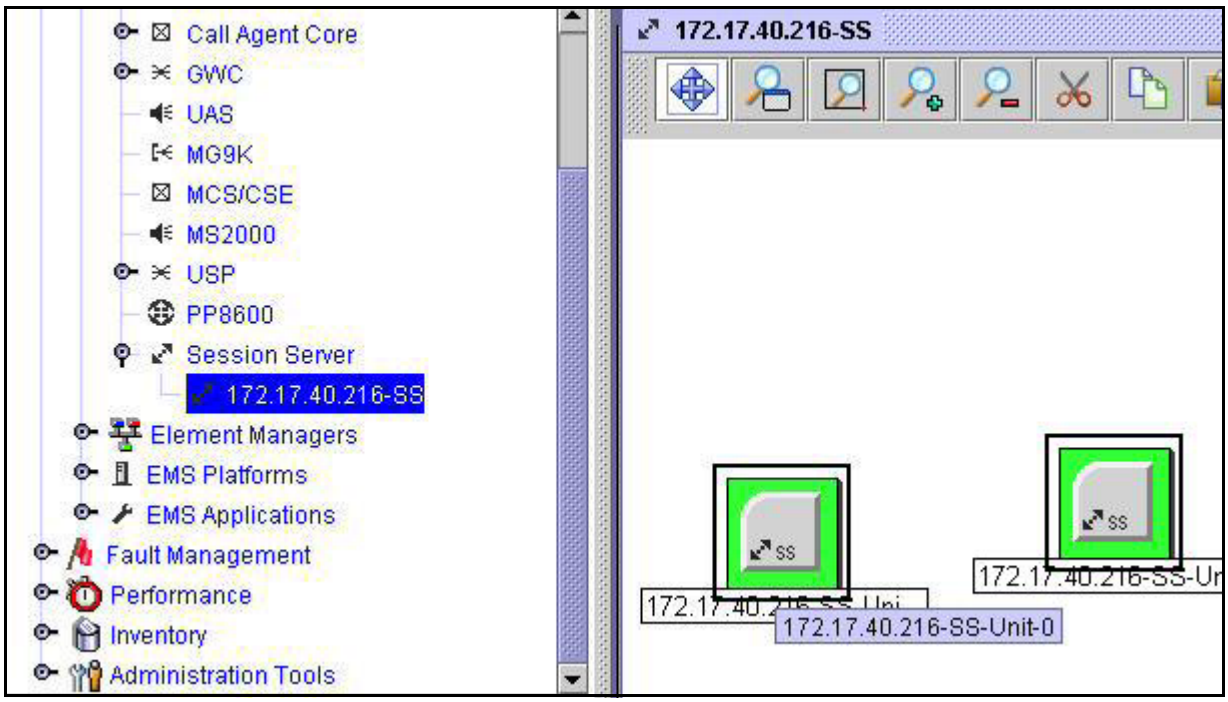
3 In the Network Elements view locate and click the Session Server element.



4 Double-click on the Session Server IP address.



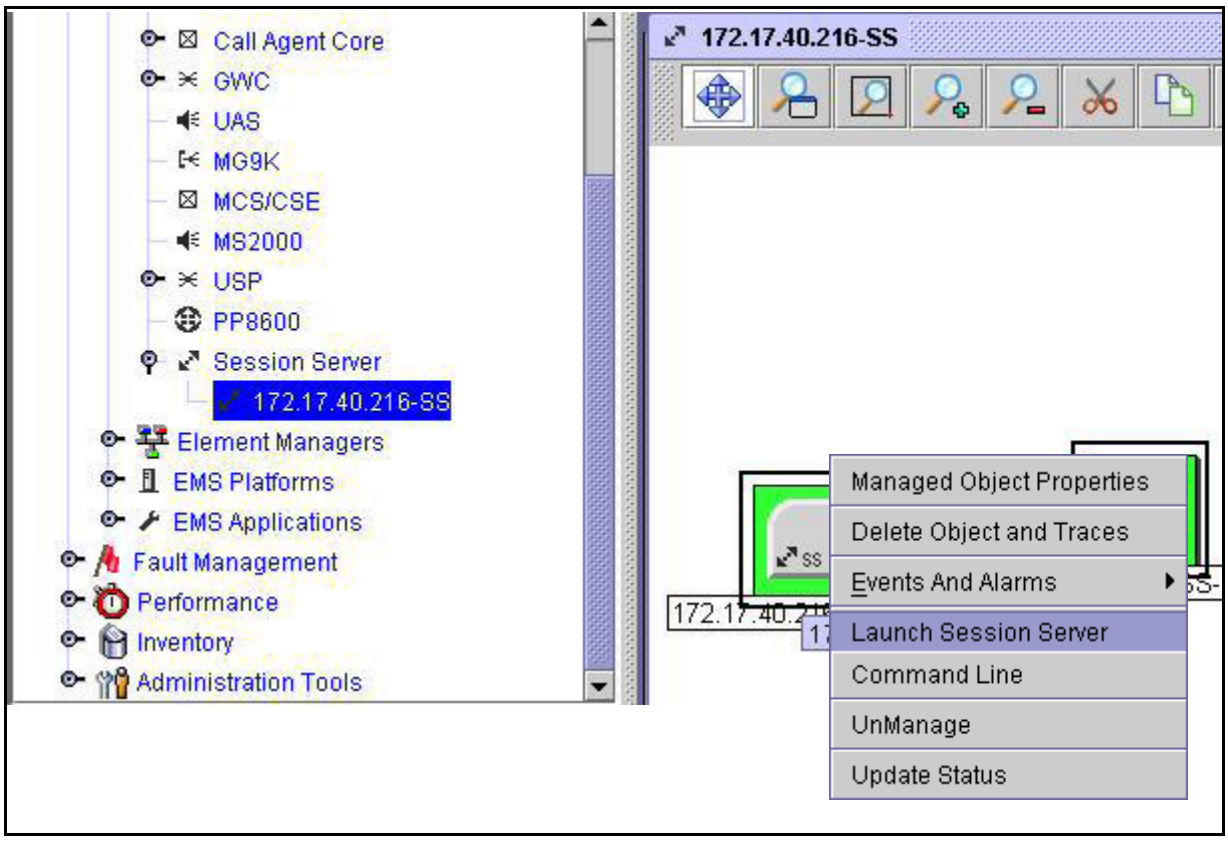
5 Hover the mouse over the first Session Server unit icon and note its unit number. Do the same for the second unit icon.



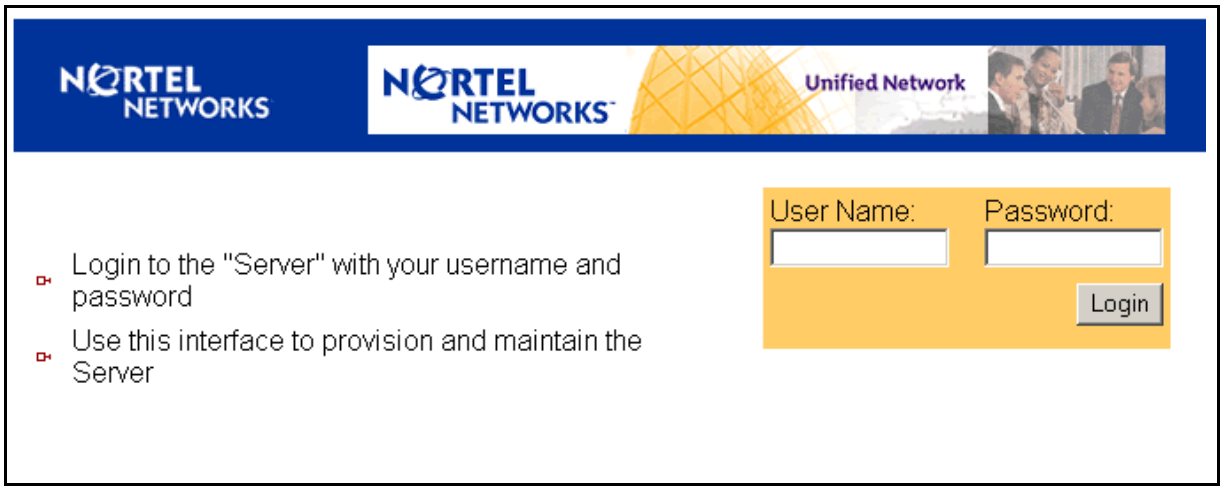
6 Use the following table to determine your next step.

If	Do
you want to launch a Command Line (CLI) session on the inactive unit	step 13
you want to launch the NCGL Platform Manager GUI on the inactive unit	step 7

7 Right-click on the either of Session Server unit icons and select **Launch Session Server**.



8 At the login screen enter your user id and password, then click the **Login** button.



9 Select the **Succession Communication Server 2000 NCGL Platform Manger** link.

ATTENTION

You can not access the CS 2000 Session Server Manager GUI from the inactive unit. You can only access the CS 2000 Session Server Manager GUI from the active unit. Clicking on the CS 2000 Session Server Manager GUI link from the *inactive* unit launch point will automatically take you to the CS 2000 Session Server Manager on the *active* unit.

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.

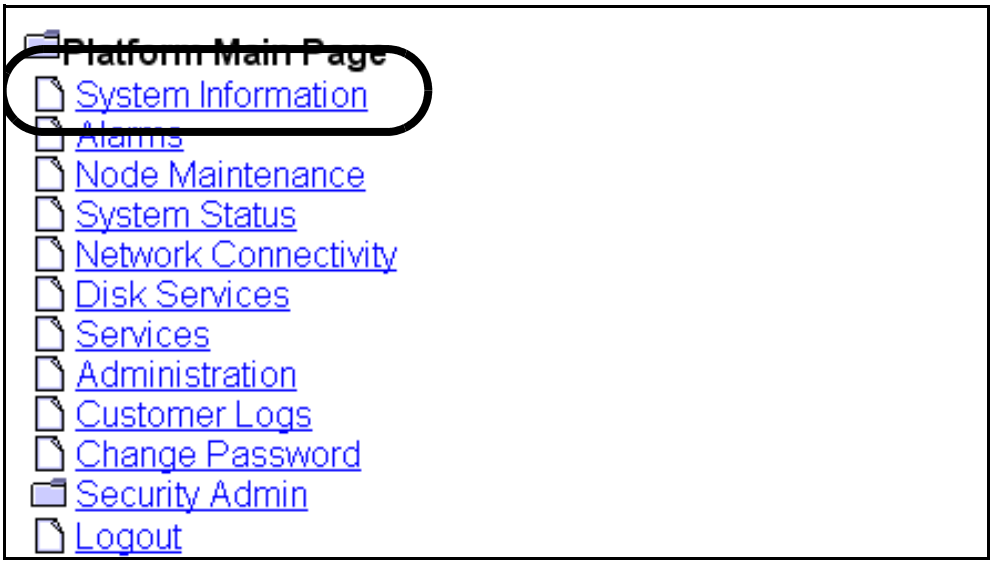
Please select one of the following management interfaces:

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

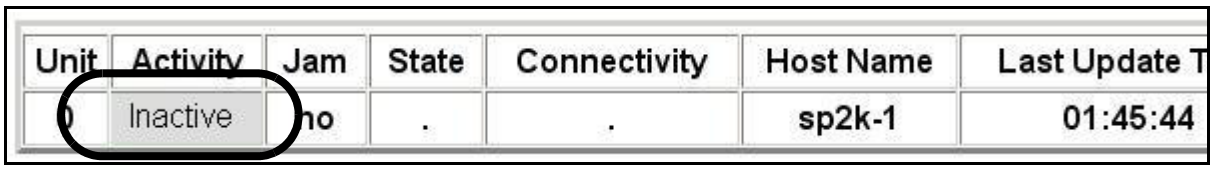
or

Logout

10 At the Platform Main Page menu, click the **System Information** link.

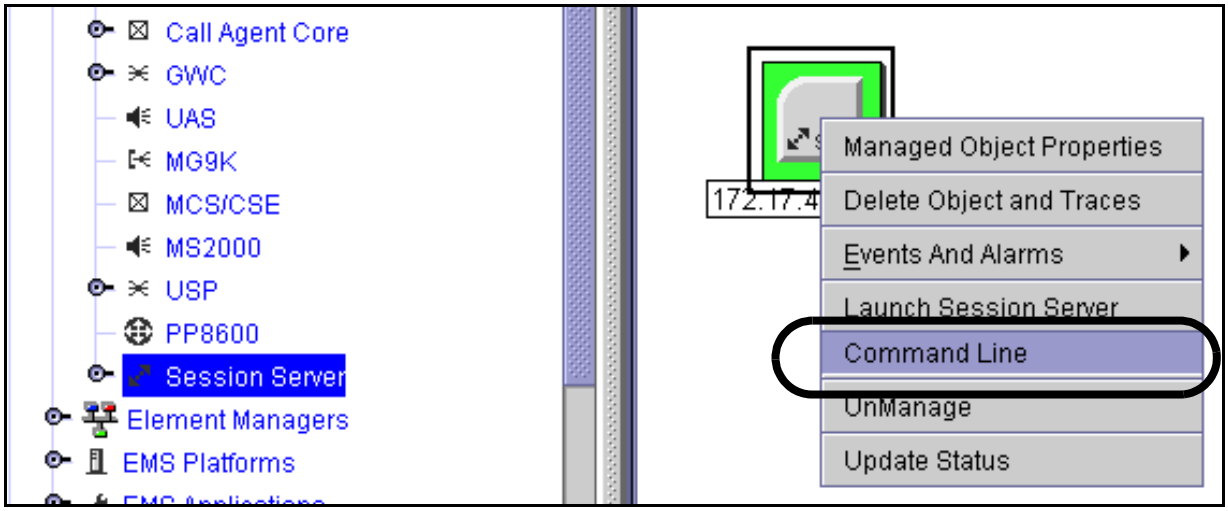


11 At the System Information page, determine if the unit you have logged onto is the inactive unit by viewing the Activity field.



12 Skip to step step 18.

13 To launch a Session Server Command Line session, right-click on the Session Server Node icon and select **Command Line** from the menu.



A secure shell (SSH) command line login window is presented.

14 If prompted to log onto the CS 2000 Management Tools server, enter the user id and password for the maintenance user.

15 At the login prompt enter the Session Server mtc user id and password.

16 Change to root user.

17 Determine if the unit you have logged onto is inactive by typing

```
mtccli status
```

and press the Enter key.

The system responds

```
Unit 0 Status:

                Jam: Link0:  Link1:  PTPLink:  OperationState:

Unit0 Inact   no     . Inact . Act     .          Enabled
Unit1 Act     no     . Inact . Act     .          Enabled
```

18 Use the following table to determine your next step.

If	Do
the unit you have logged onto is the inactive unit	you have successfully logged onto the inactive unit. Go to step 19.
the unit you have logged onto is not the inactive unit	log off from this (active) unit, return to step 4, and select the other Session Server unit icon.

19 You have completed this procedure.

Access Session Server/NCGL GUIs using a proxied client

Purpose of this procedure

This procedure describes how to access the Session Server web-based GUIs (CS 2000 NCGL Platform Manager and CS 2000 Session Server Manager) using a client workstation.

Limitations and Restrictions

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.

Ensure that the Session Server node has been configured to support GUI access through a web proxy. If you receive messages in your web browser that the access to the CS 2000 NCGL Platform Manager has been denied, your Session Server has not been properly configured for access through a web proxy. Refer to procedure “Manage SSPFS server web proxy setup for Session Server” found in the *Session Server Configuration Management*, NN10338-511, for instructions on configuring a web proxy to support access to the Session Server.

To perform provisioning of the SIP Application Gateway you must access the active Session Server unit.

When attempting to access the Session Server GUI, access to the active unit is only supported for non-upgrade activities. Accessing the active Session Server unit GUIs is supported in the methods provided in this document.

You will be required to enter your login information two or more times to access the Session Server GUI through the IEMS as the IEMS and the Session Server each validate login information individually.

Prerequisites

Ensure that you are using the correct version of a web browser for accessing the GUIs. Refer to the Overview section of *Session Server Configuration Management* , NN10338-511 for this information.

Action

At a client workstation

1 Open a supported web browser.

2 In the URL address bar of the browser access the active or inactive Session Server unit by typing

```
> https://<proxy_IP_address>/<SS_IP_address>/
```

and pressing the Enter key.

where

proxy_IP_address
is the IP address of the proxy server in your network

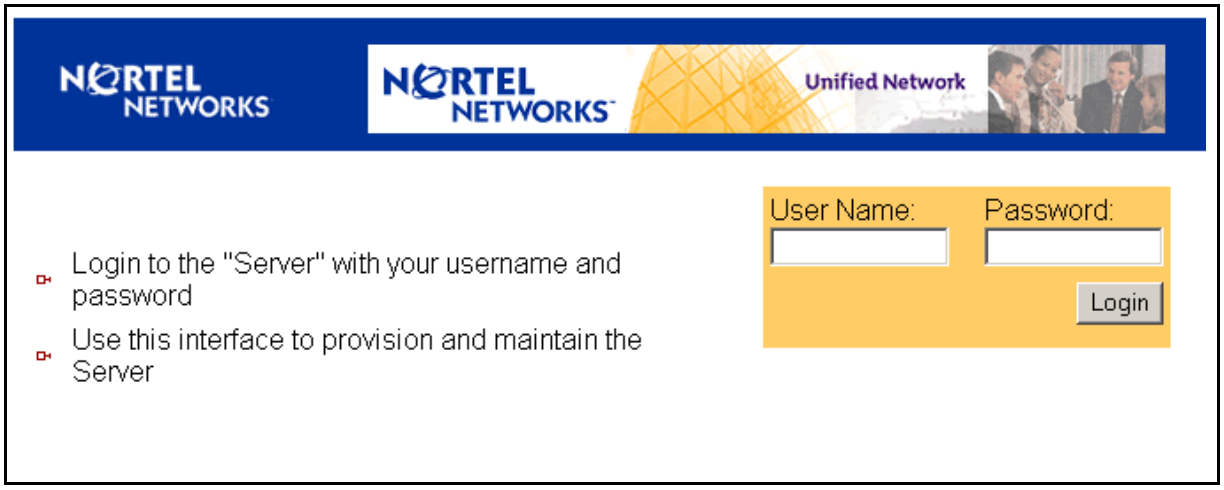
SS_IP_address
is the IP address of the Session Server active or inactive unit

Example
https://47.135.42.226/10.67.99.72/

3 If necessary, confirm any security alerts related to security certificates by clicking **Yes** to proceed.

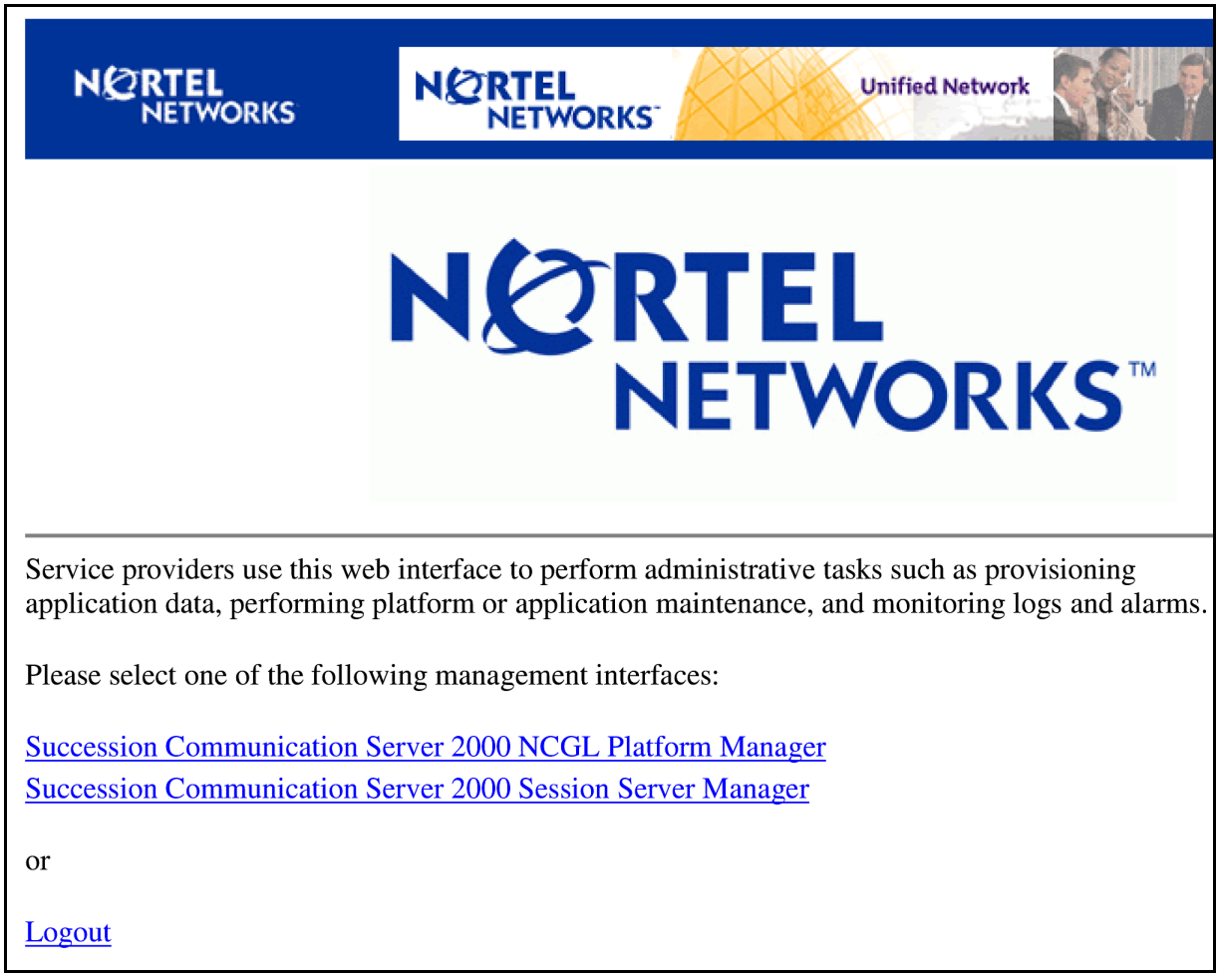
4 At the login screen enter your user id and password, then click the **Login** button.

Note: You cannot login to the Session Server GUIs as the root user.



5 Select the GUI you want to launch from the launch point menu.

- Select the CS 2000 NCGL Platform Manager if you want to perform maintenance or provisioning on the NCGL operating system of the Session Server platform
- Select the CS 2000 Session Server Manager if you want to perform maintenance or provisioning on the SIP Gateway Application.
- Select Logout if you want to exit back to the login screen.



6 You have completed this procedure.

Manage users on the Session Server platform

Purpose of this procedure

Use this procedure to add new users on a Session Server and assign them to user groups, or assign existing users to user groups. For more information about user groups refer to User and authorization categories on page 6.

Use this procedure also to delete existing users from the user database.

Limits and Restrictions

ATTENTION

Privileges for new users are only enforced on the CS 2000 Session Server Manager GUI, used for making provisioning changes to the SIP Gateway application. However, privileges are not enforced for new users on the CS 2000 NCGL Platform Manager.

ATTENTION

User accounts and passwords are not propagated to the standby Session Server. Perform account management activities such as setting up users, removing users, and changing passwords, on both servers.

To perform this procedure, you need to have the root user ID and password to log in to the server.

Users of the Nortel Networks OAM&P client applications must belong to the primary user group “succssn” for login access. Users must also belong to a secondary group, that specifies the operations a user is authorized to perform. Refer to the overview section for more information about primary and secondary user groups and user group domains.

Prerequisites

There are no prerequisites for using this procedure.

Action

At a Session Server console interface or command line interface

1 Log onto the Session Server unit and change to root user.

2 Use the following table to determine your next step.

If you are	Do
adding a new user	step 3
deleting a user	skip to step 8
are done with this procedure	skip to step 9

3 Add the user to the primary user group “succssn” by typing

```
# useradd -g succssn -G <groupA> <userid>
```

and pressing the Enter key.

where

groupA
is a secondary user group. Refer to the overview section for more information about primary and secondary user groups and user group domains.

userid
is a variable for the user name

4 Create a password for the user you just added by typing

```
# passwd <userid>
```

and pressing the Enter key.

where

userid
is the user name you added in the previous step.

ATTENTION
For security reasons, do not set a password with an empty value. Use a minimum of six characters for a password. Do not set the password to be the same as the user id.

5 When prompted, enter the password again for verification.

6 Note any primary and secondary user groups the user currently belongs to.

7 Return to step 2.

8 Delete the user from the server by typing

```
# userdel <userid>
```

and pressing the Enter key.

where

userid
is a variable for the user name

9 Repeat this procedure on the second (mate) Session Server unit.

ATTENTION

User accounts and passwords are not automatically propagated to the standby Session Server. Perform account management activities such as setting up users, removing users, and changing passwords, on both units.

10 Exit from root user by typing

```
# exit
```

and pressing the Enter key.

11 If necessary, exit the SSH session by typing

```
$ exit
```

and pressing the Enter key.

12 You have completed this procedure.

Manage user passwords using a Session Server console CLI

Purpose of this procedure

This procedure is used to enable, change or disable passwords for all user ids, including the root user id, on the Session Server using the Session Server platform console command line interface (CLI).

Limitations and Restrictions

ATTENTION

User accounts and passwords are not automatically propagated to the standby Session Server. Perform account management activities such as setting up users, removing users, and changing passwords, on both units.

Prerequisites

There are no prerequisites for this procedure.

Action

At a Session Server console interface or command line interface

1 Open a secure shell to the Session Server by typing

> **ssh -l <userid> <SS_IP_address>**

and pressing the Enter key.

where

userid
is a valid userid (like mtc) on the Session Server

SS_IP_address
is the IP address or host name of the Session Server on which you want to install the HTTPS certificate

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change the password for a specific user by typing

$ **passwd <userid>**

and pressing the Enter key.

where

userid
is a variable or code for the user's login identification

4 When prompted, enter a password of at least six characters.

ATTENTION

For security reasons, do not set a password with an empty value. Use a minimum of six characters. Do not set the password to be the same as the user id.

5 When prompted, enter the password again for verification.

6 Repeat this procedure on the mate unit.

ATTENTION

User accounts and passwords are not automatically propagated to the standby Session Server. Perform account management activities such as setting up users, removing users, and changing passwords, on both units.

7 You have completed this procedure.

Manage user passwords with the Session Server GUI

Purpose of this procedure

Use this procedure to change the mtc user password using the CS 2000 NCGL Platform Manager or the CS 2000 Session Server Manager GUIs.

Limits and Restrictions

When performing this procedure, you can only change the password for the user ID that you logged in with. To change passwords for other user-created IDs, log into the Session Server using that user ID.

ATTENTION

User accounts and passwords are not automatically propagated to the standby Session Server. Performing account management activities such as setting up users, removing users, and changing passwords, on both units.

Prerequisites

There are no prerequisites for this procedure.

Action

At the CS 2000 Session Server Launch Point

1 Select either the **CS 2000 Server NCGL Platform Manager** or the **CS 2000 Session Server Manager** from the launch point menu.

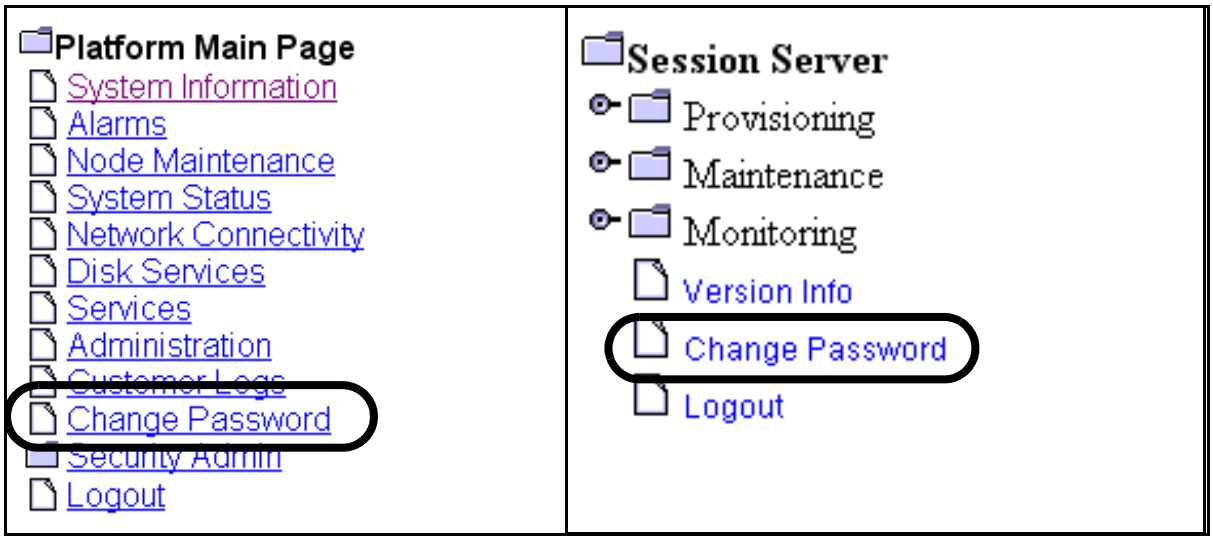
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

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

2 Click the **Change Password** link.

The Change Password page is displayed.



3 Refer to the following sub-steps:

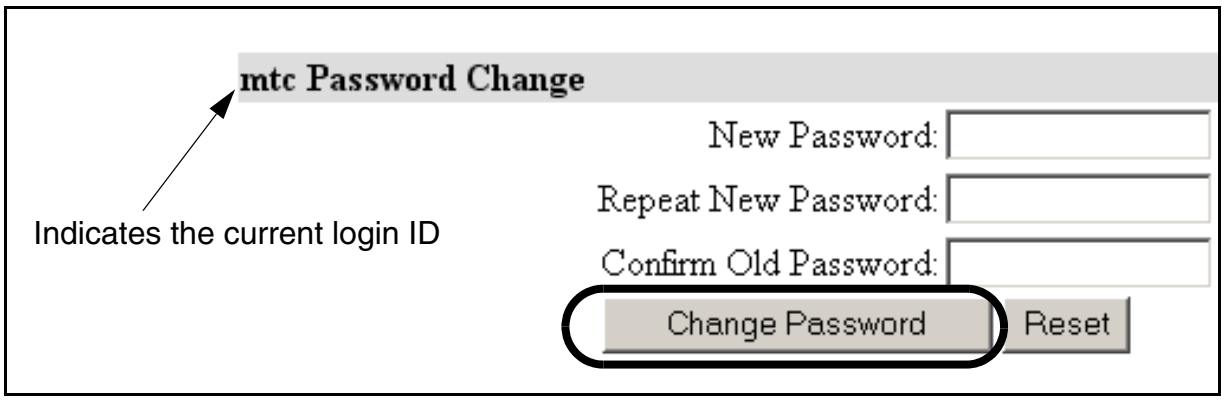
a Type the new password.

Note: For security reasons, do not set a password with an empty value. Use a minimum of six characters. Do not set the password to be the same as the user id.

b Retype the new password for verification.

c Type the old password.

d Click the **Change Password** button.



4 Repeat this procedure on the mate Session Server unit.

ATTENTION

User accounts and passwords are not automatically propagated to the standby Session Server. Perform account management activities such as setting up users, removing users, and changing passwords, on both units.

5 You have completed this procedure.

Invoke a maintenance SWACT of the Session Server - Trunks platform

Purpose of this procedure

This procedure manually performs a maintenance SWACT (switch of activity). A SWACT gracefully transitions call processing activity from the active unit to the standby unit without first reloading and reinitializing the SIP Gateway application on the standby unit.

Use this procedure as a standalone task or as part of a maintenance or fault clearing activity like replacing a faulty standby unit or a high-level activity such as upgrading a standby unit.

Note: An automatic failover SWACT can be initiated by the platform NCGL in cases of critical faults on the active unit. For more information about conditions required for a SWACT, refer to "Understanding conditions for a SWACT" in the *Session Server - Trunks Security and Administration*, NN10346-611.

Limits and Restrictions

ATTENTION
Perform a maintenance SWACT only when both the active and standby units are operationally enabled and their databases are synchronized.

You cannot perform a SWACT if the inactive unit is jammed. If the unit Jam state is jammed, refer to procedure Enable a system SwAct (Unjam) on page 70 to unjam the unit.

ATTENTION
Logins to the Session Server - Trunks do not survive a platform SWACT.

During an unforced maintenance SWACT, new calls are set up on the standby unit, while existing calls continue to be processed on the active unit until they are terminated. SIP-T calls in the process of setup during a SWACT can be lost. Over SIP-T trunks, the far end continues to receive the setup alert (ringing) until one of the following events occur:

- The end user answers and terminates the call.
- A GWC system audit runs and clears the trunks (once every 10 minutes).

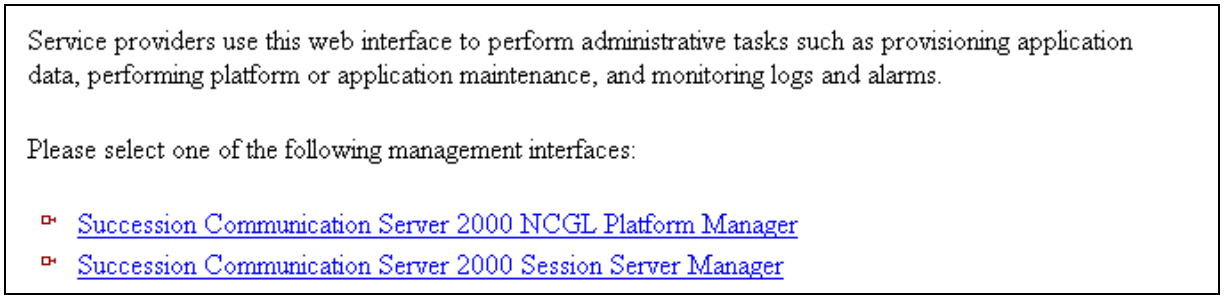
Prerequisites

If you are executing a Forced SWACT, confirm that there are no alarm conditions.

Action

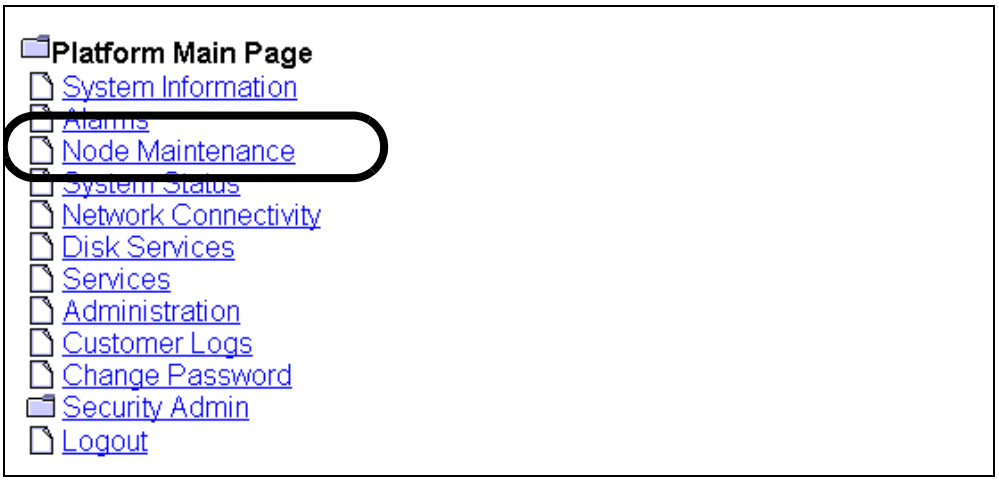
At the Session Server Manager or IEMS client of the active unit

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

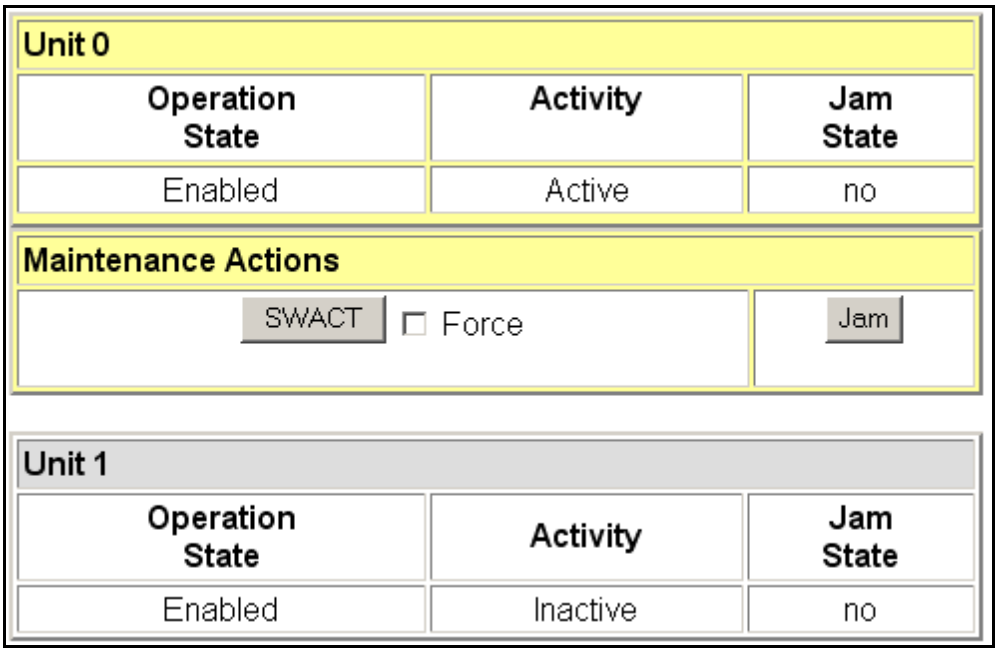


2 Click the Node Maintenance link.

The Node Maintenance page is displayed.



3 Refer to the table in section Additional status information on page 55 to review the description of the various fields of the Node Maintenance page.



Unit 0		
Operation State	**Activity**	**Jam State**
Enabled	Active	no

Maintenance Actions	
SWACT ☐ Force	Jam

Unit 1		
Operation State	**Activity**	**Jam State**
Enabled	Inactive	no

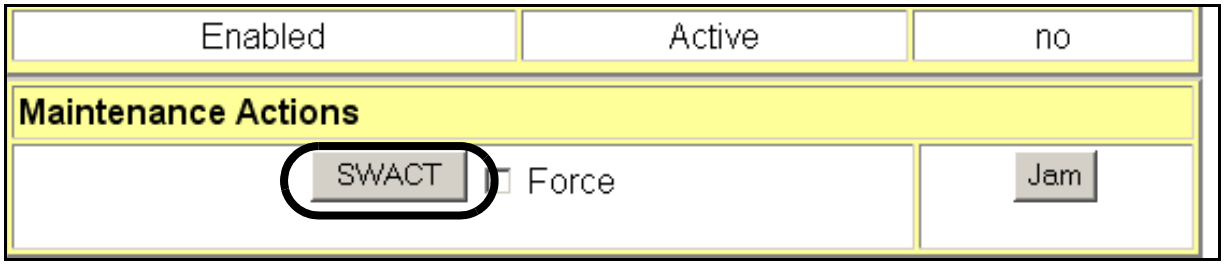
4 To SWACT the units, click the SWACT button.

or

To override any pre-SWACT queries, first click the Force checkbox, then click the SWACT button.

CAUTION
Possible service interruption
Due to the risk for loss of data and service outage, it is recommended that the Forced SWACT option not be used except when instructed by your Nortel customer support representative.

A forced SWACT overrides any SWACT pre-checks and is not recommended. SWACT prechecks monitor the inactive unit for critical faults on the platform, which will prevent a SWACT. In addition, the precheck ensures that the SIP Gateway application is in-sync. A SWACT force can result in a full service outage on the node if the inactive unit is not in-sync. There is potential for loss of provisioned data if a SWACT to an unstable unit is completed.

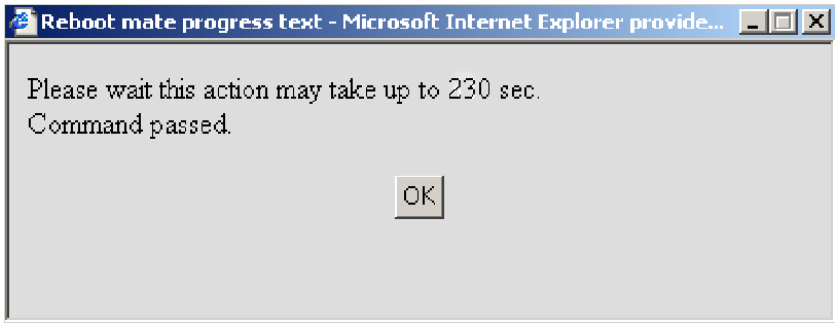


The system responds:

```
Are you sure you wish to swact? This may cause
a service interruption to applications running
on this server. Click OK to confirm server swact
or cancel to abort.
```

5 Click Yes to confirm either the SWACT or forced SWACT.

The system responds with the following message box:



6 Click OK to close the dialog box.

7 Observe the Activity field for each unit. Each unit's activity status (whether Active or Inactive) swaps.

8 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Additional status information

The following table describes the various fields of the Node Maintenance panel.

Field	Description
Operation State (unit 0 or 1)	operational state of the platform software, either enabled or disabled
Activity (unit 0 or 1)	activity state of the platform software, either active or inactive
Jam State (active unit only)	indicates whether or not the unit has been “jammed”, preventing the standby unit from being able to become active, regardless of any failures on the active unit. States are either jammed, where a SWACT is disabled, or unjammed, where a SWACT is enabled.
Maintenance Actions (active unit only)	maintenance panel for performing node SWACT activity and to jam or unjam node activity switches.

Invoke a manual cold SwAct of the SIP Gateway application

Purpose of this procedure

This procedure performs a manual switch of activity (SwAct) from the active to the standby Session Server unit. It also forces a reload and reinitialization of the SIP Gateway application on the standby unit before switching callP activity from the active unit to the standby unit.

This procedure is used for fault clearing activities, and when a problem has been detected with SIP Gateway call processing as determined by the alarm panel.

Limits and Restrictions

ATTENTION
Do not use this procedure to request a platform SwAct. Only proceed with this procedure if a platform SwAct has already occurred, and a problem has been detected with SIP Gateway call processing.

ATTENTION
You cannot cold SwAct the SIP Gateway application if the inactive (standby) Session Server unit is out of service. A SIP cold SwAct can only be performed when both the active and standby Session Server platform units are operationally enabled.

You cannot cold SwAct the SIP Gateway application if the active unit's communications mode is in a jammed state. If the active unit is jammed, refer to procedure Enable a system SwAct (Unjam) on page 70 to unjam the unit.

During a SIP application cold SwAct, all currently active SIP Gateway calls are taken down and all SIP calls in setup are lost. However, over SIP-T DPT trunks, the far end continues to receive the setup alert (ringing) until one of the following events occur:

- The end user answers and terminates the call.
- A GWC system audit runs and clears the trunks every 10 minutes.

Prerequisites

There are no prerequisites for performing this procedure.

Action

At the CS 2000 Session Server Launch Point

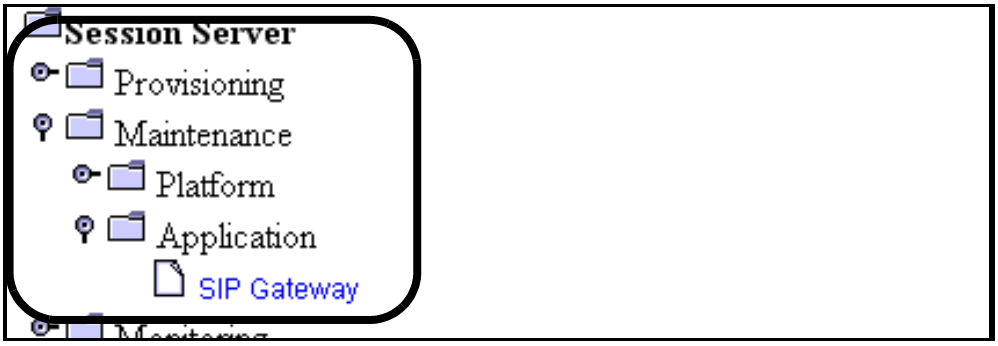
1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.

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:

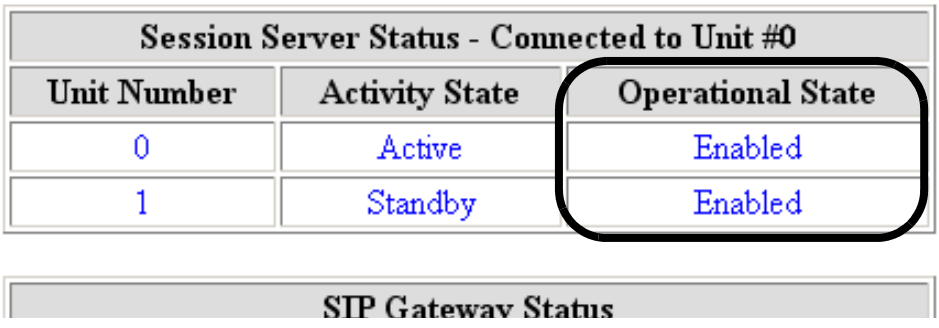
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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



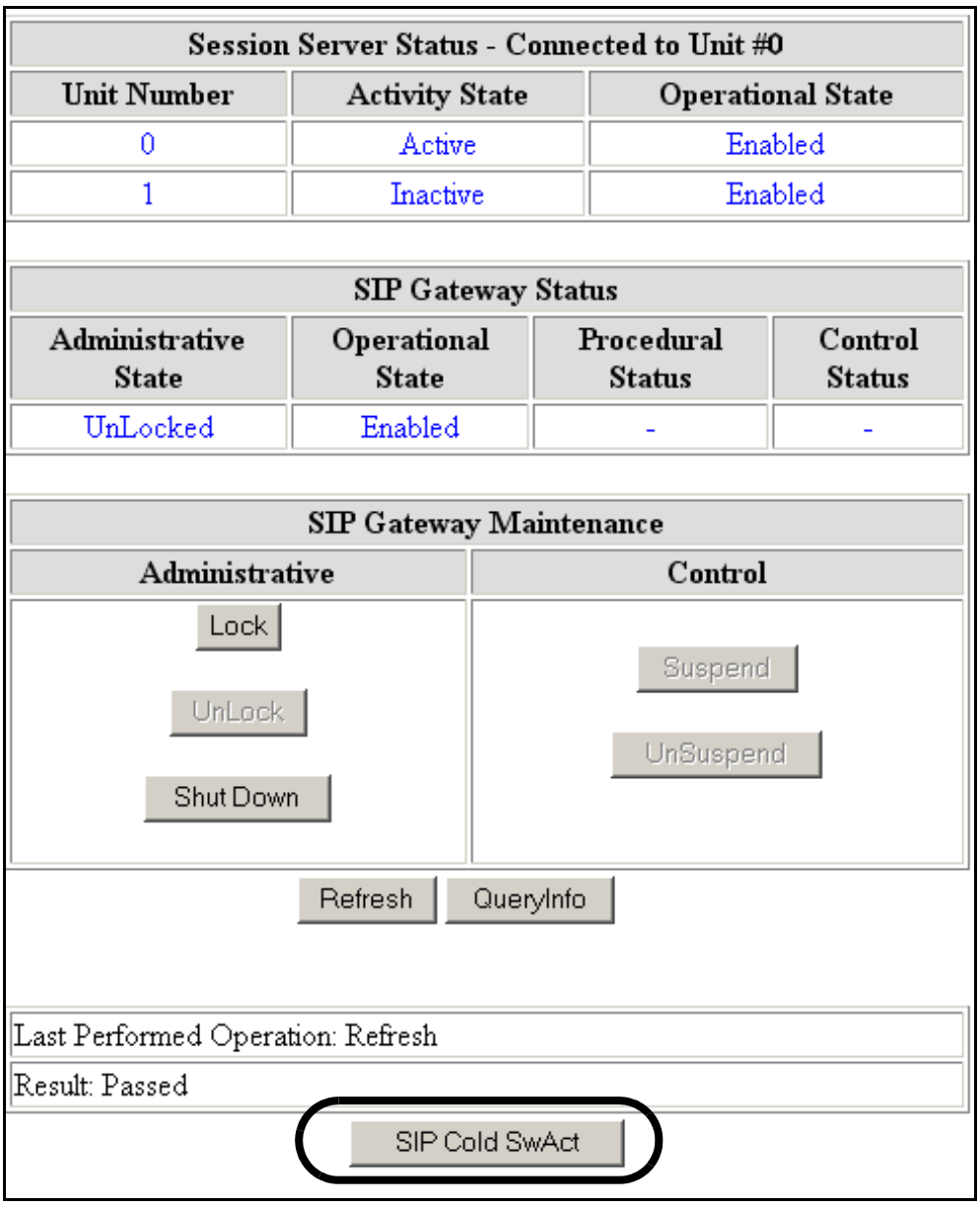
3 Click on the **SIP Gateway** folder to open it.

4 Determine whether both the active and standby units are operationally enabled and that the **SIP Cold SwAct** button is not disabled (shaded out).



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

5 To cold SwAct the SIP Gateway application, click the **SIP Cold SwAct** button.



A dialog box appears to verify if the user wants to proceed with a SIP Gateway cold SwAct

6 Confirm that you want to proceed with the SIP cold SwAct by clicking the **OK** button.

CAUTION

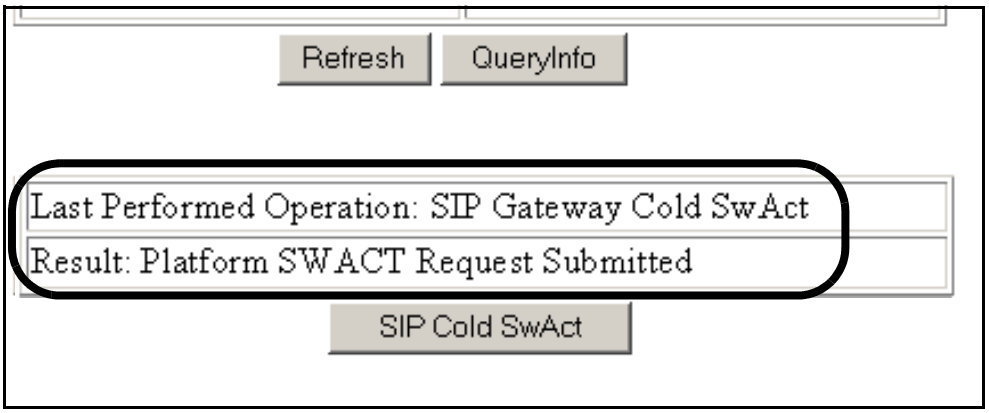
Continuing with this procedure will cause a temporary service outage on the Session Server.

The system responds:

```
RELEASE ALL <X> SIP Gateway CALLS AND PERFORM A
SESSION SERVER FORCED SWACT?
```

7 Confirm that you want to proceed with the SIP cold SwAct by clicking the **OK** button.

8 Observe the Message field for details about the SwAct transaction status.



If the result of the SIP cold SwAct request is anything but `Passed`, refer to the CS 2000 Session Server Fault Management NTP, NN10332-911, to troubleshoot the failure using logs and alarms and consult your next level of support.

For more information about determining the status of the SIP Gateway application, refer to procedure View the operational status of the SIP Gateway application on page 93.

9 The procedure is complete.

Invoke a manual switch of active links (Swlink)

Purpose of this procedure

This procedure provides a service-impacting recovery routine. It forces a switch of link activity on the Session Server units regardless of call activity on the active unit.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as in cases of a determining if a network ethernet link is faulty.

Links on either the active or standby Session Server units can be switched.

Prerequisites

There are no prerequisites to using this procedure.

Action

At the CS 2000 Session Server Launch Point

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

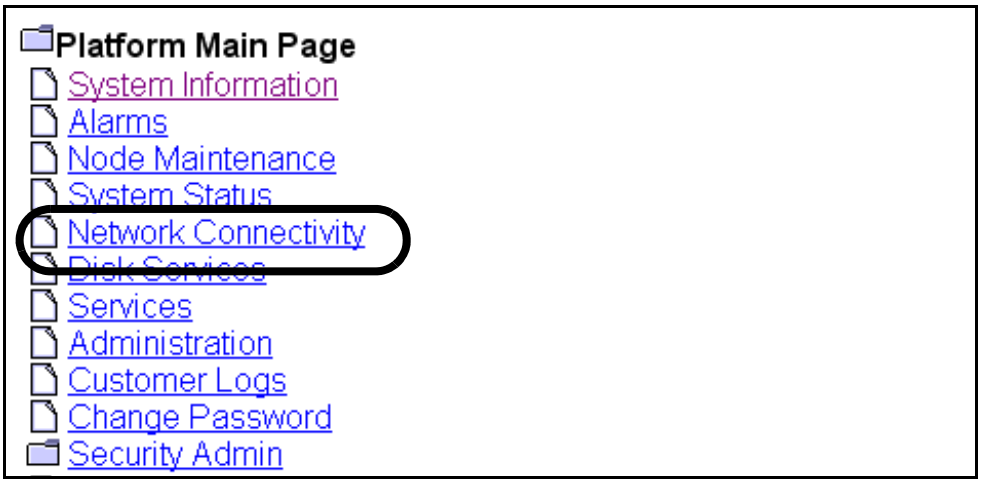
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

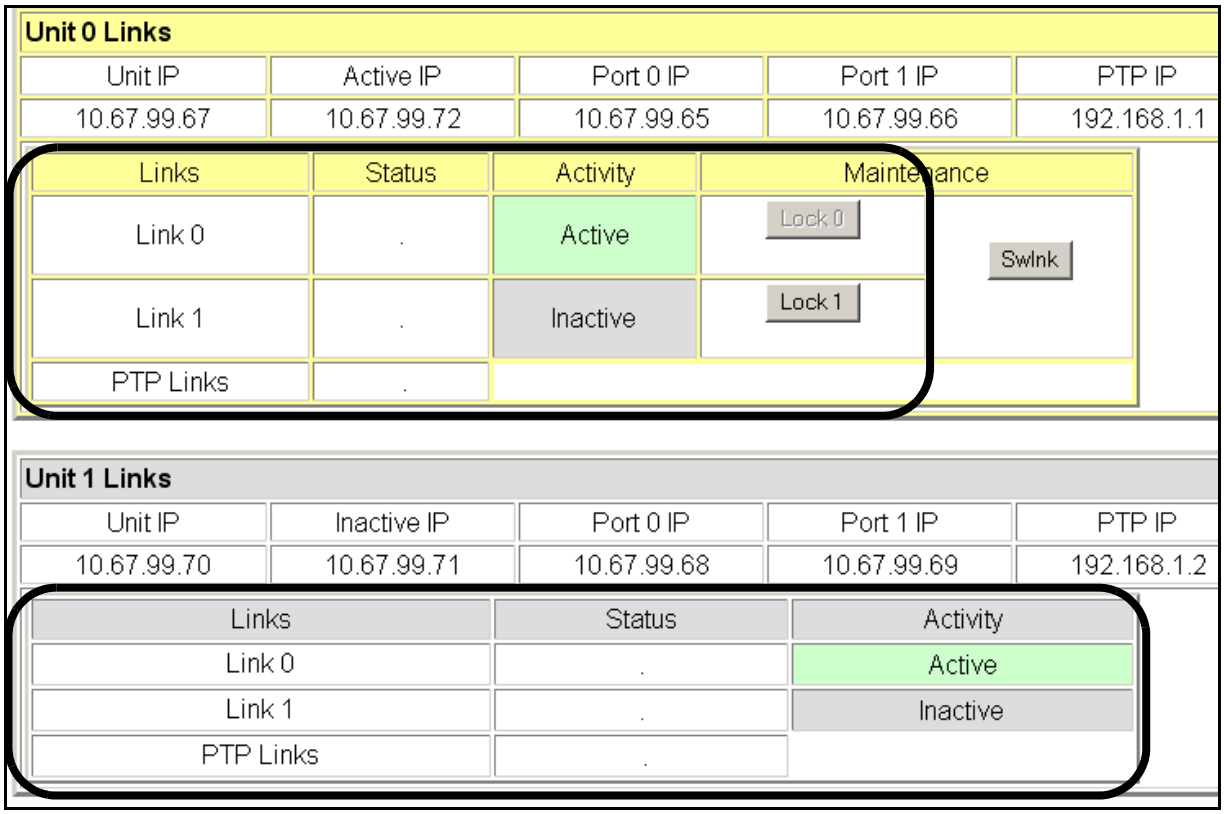
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Network Connectivity** link.

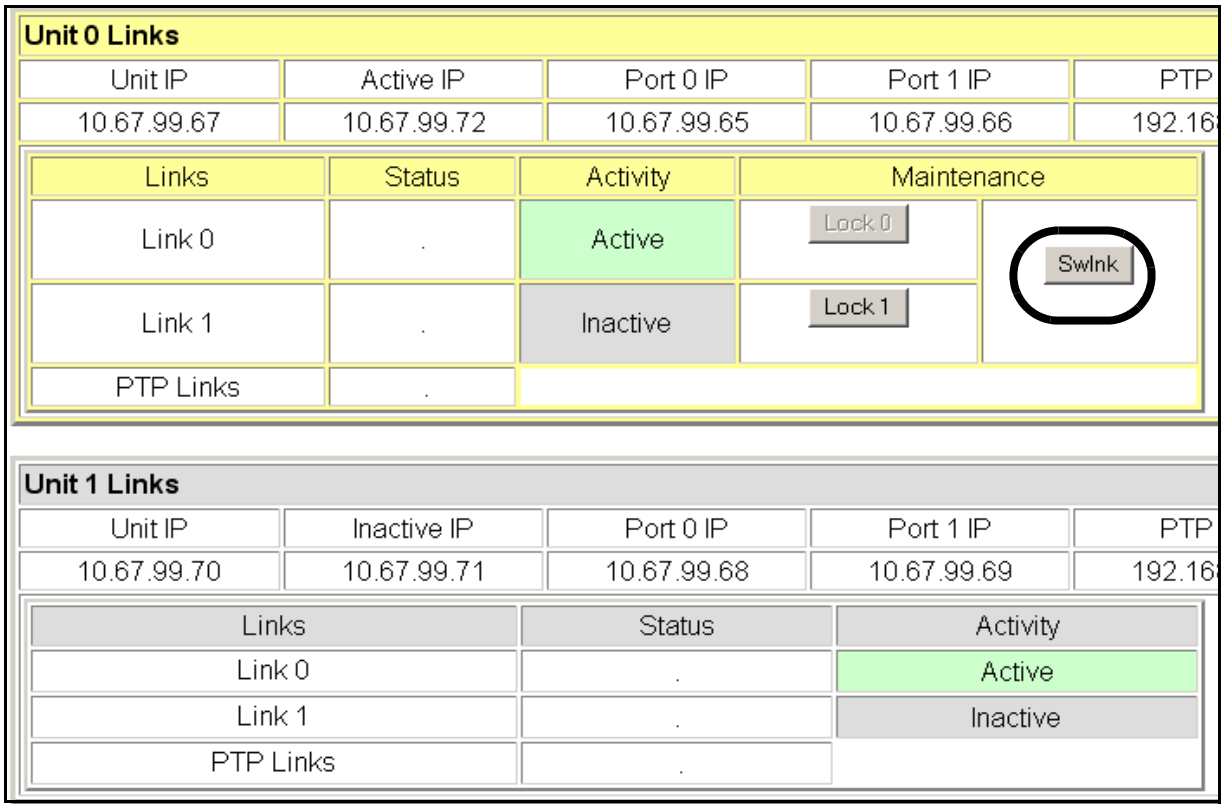
The Network Connectivity page is displayed.



3 Review the link state of both Session Server units.



4 Click the **Swlink** button for the active link on the active unit.

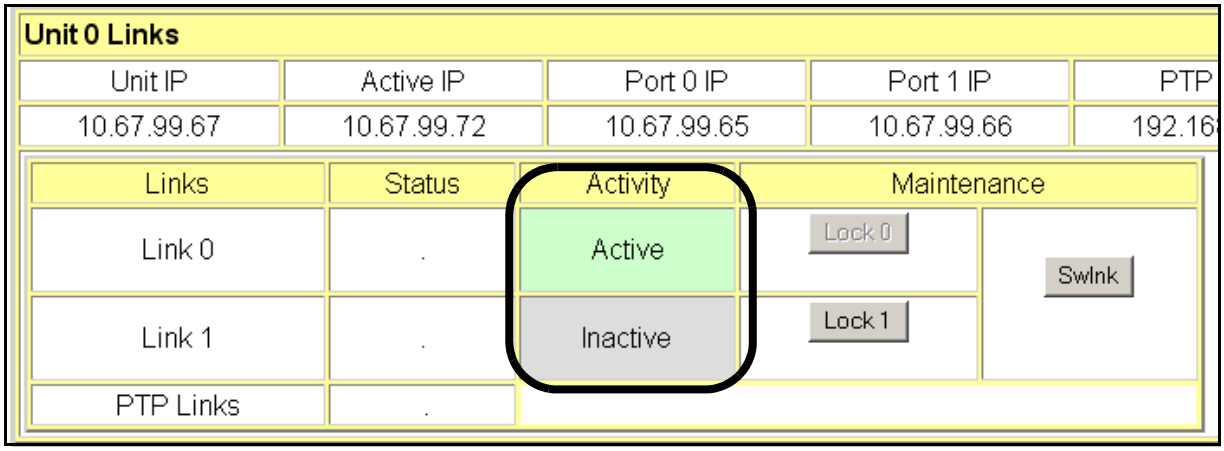


The system responds:

```
Are you sure you wish to switch link activity?
Click OK to confirm or cancel to abort.
```

5 Click **OK** to confirm the switch link activity.

6 Ensure that the state of the links swaps.



7 This procedure is complete.

Inhibit a system SwAct (Jam)

Purpose of this procedure

The jam command is used to manually prevent a SwAct (switch of activity) of the active and stand-by units by inhibiting the toggling of operational states of both units, thereby preventing the stand-by unit from going active.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as in cases of a replacing a faulty standby unit or upgrading the software for a standby unit.

ATTENTION

This procedure can be performed only from the active unit. You cannot Jam the active unit if the inactive unit is out of service.

CAUTION
Loss of redundancy

This procedure prevents the node from operating in a duplex, fault-tolerant mode and prevents the SIP Gateway application from being able to SwAct as needed. Keep a jam in effect only as long as is necessary.

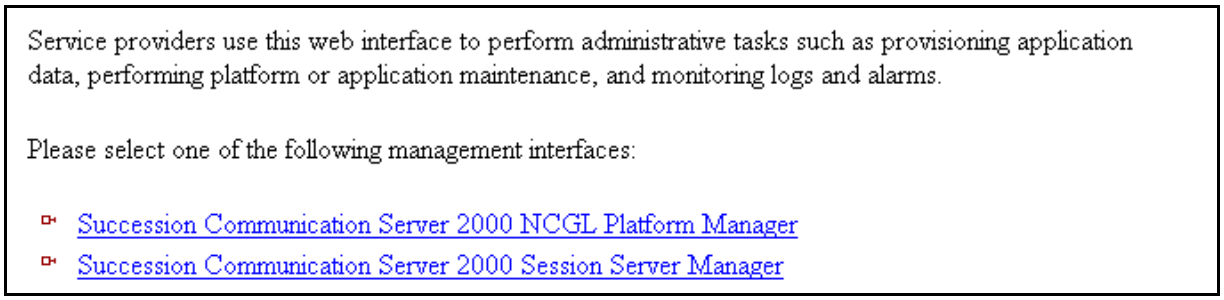
Prerequisites

There are no prerequisites for performing this procedure.

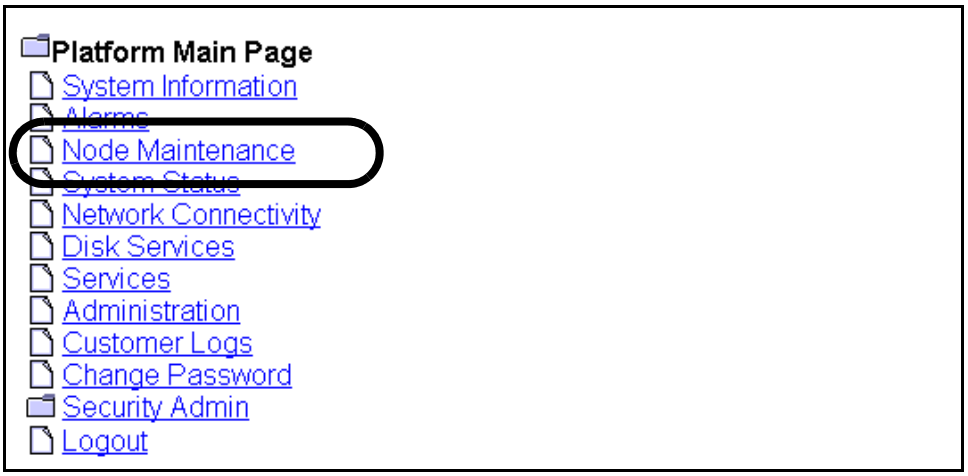
Action

At the CS 2000 Session Server Manager or IEMS workstation

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

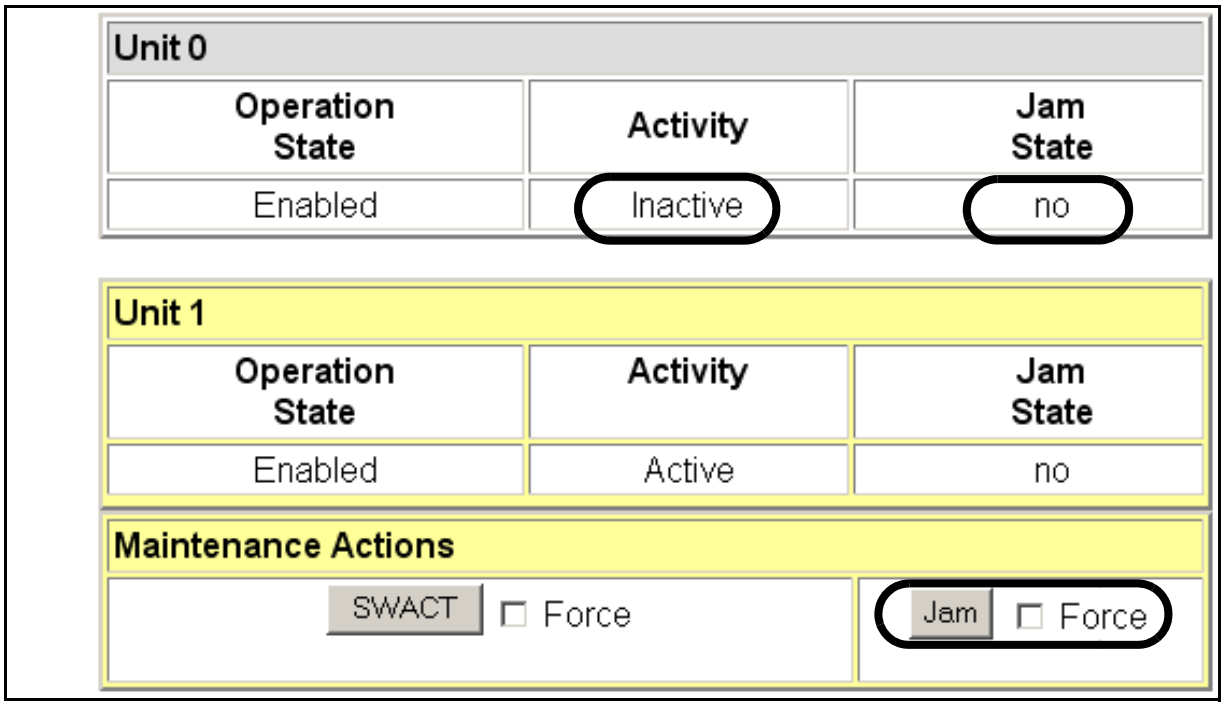


2 Click the Node Maintenance link.



The Node Maintenance page opens in the right side frame.

3 Determine if the Jam State of the standby unit is Yes or No. If it is Yes, then the unit is already jammed and you are done with this procedure. If it is No, then continue with the next step.

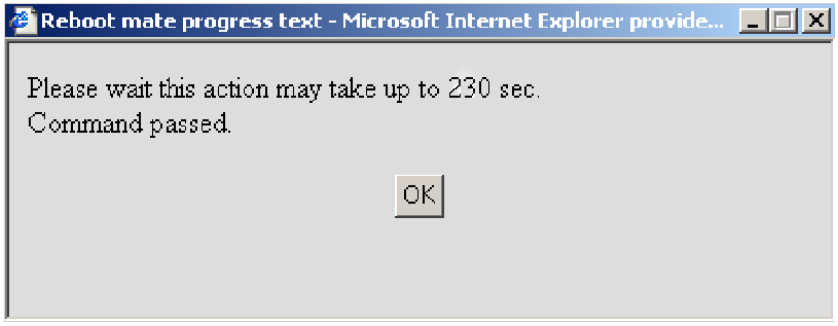


4 Click the Jam button. If the button is disabled, then this is the inactive unit; reconnect to the active unit.

A confirmation dialog window opens.

5 Click OK to proceed with the jam activity.

The system responds with the following message box:



6 Click OK to close the dialog box.

A dialog window indicates that the Jam passed. The Node Maintenance window refreshes and the Jam State for the inactive unit becomes yes.

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

Force Jam information

The Jam action does not work if critical faults exist on the active unit. Using the Jam command with the Force option overrides any pre-checks. A Forced Jam forces a Jam of the inactive unit even if critical faults exist on the active unit, in which case, a full service outage on the Session Server - Trunks node could occur on the if the active unit fails.

Enable a system SwAct (Unjam)

Purpose of this procedure

The Unjam command is used to manually enable a SwAct (switch of activity) of the active and stand-by units by allowing the two units to toggle their operational states.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities, such as replacing a faulty standby unit or upgrading a standby unit.

ATTENTION
This procedure can only be performed from the active unit.

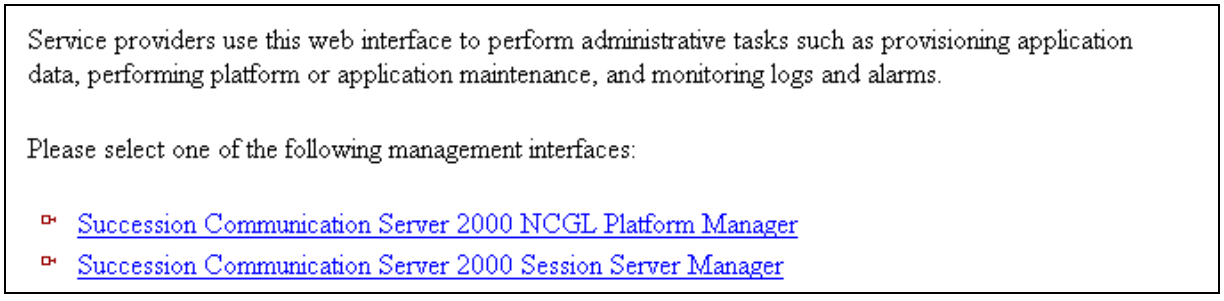
Prerequisites

There are no prerequisites for performing this procedure.

Action

At the CS 2000 NCGL Platform Manager or IEMS client

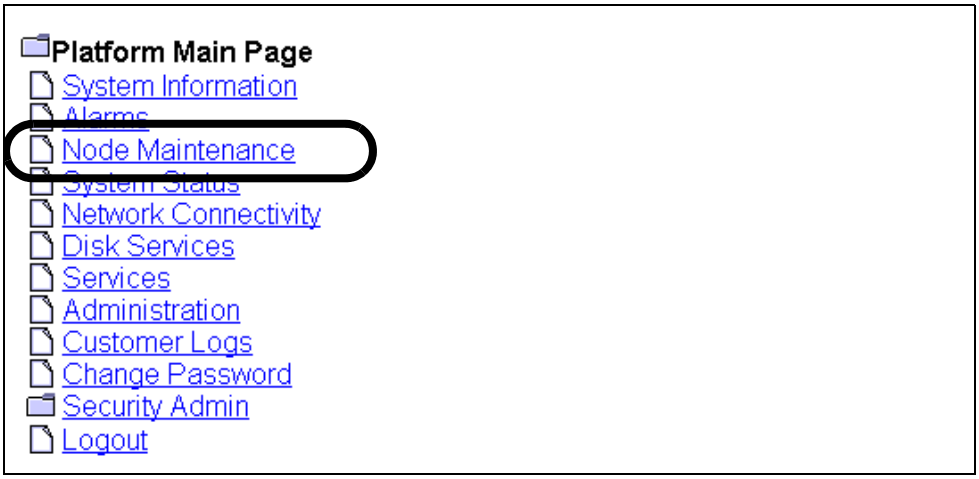
1 Select Succession Communication Server NCGL Platform Manager from the launch point menu.


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:

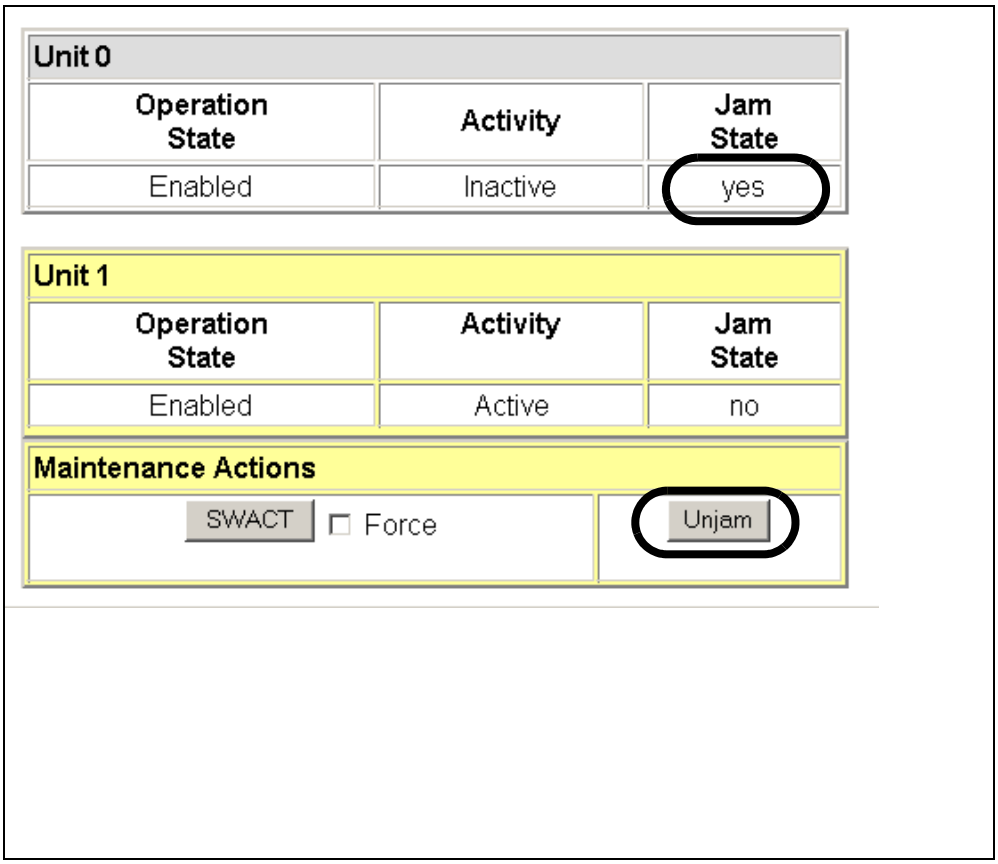
- Succession Communication Server 2000 NCGL Platform Manager
- Succession Communication Server 2000 Session Server Manager

2 Click the Node Maintenance link.



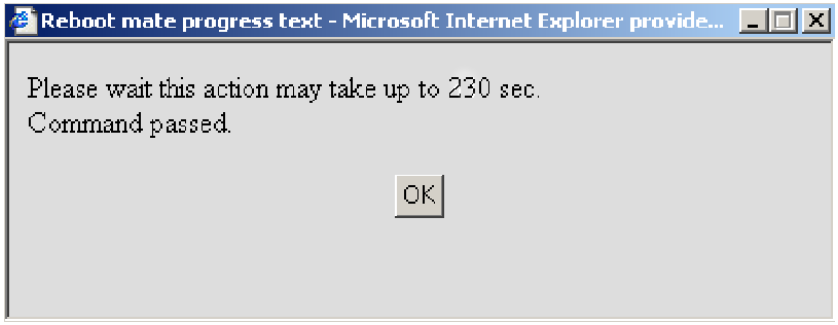
The Node Maintenance page opens in the right side frame.

3 Determine if the Jam State of the standby unit is Yes or No. If it is No, then the unit is already unjammed and you are done with this procedure. If it is Yes, then continue with step 4.



4 Click the Unjam button.

The system responds with the following message box:



5 Click OK to close the dialog box.

The system responds with a dialog window:

```
Info: Unjam - Command passed.
```

Then the Jam State becomes no and the JInact alarm clears.

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

Lock network ethernet link

Purpose of this procedure

This procedure is used to lock (shut down) the inactive ethernet link on a Session Server unit, preventing a switch of link activity (Swlnk) to the inactive link. These links allow the Session Server to communicate with other components in the network.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities.

CAUTION

This procedure prevents the Session Server node from operating in a fully fault-tolerant mode.

Prerequisites

There are no prerequisites to using this procedure.

Action

At the CS 2000 Session Server Launch Point

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

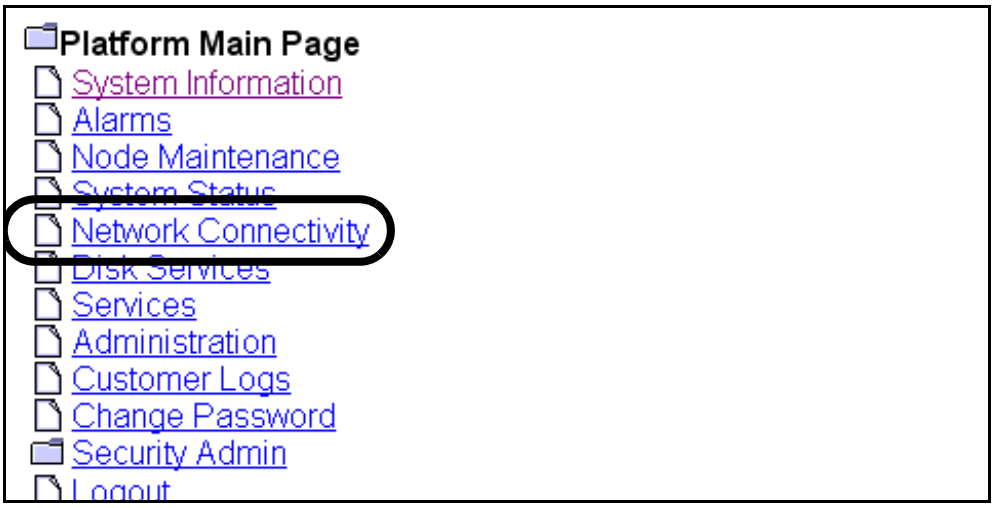
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

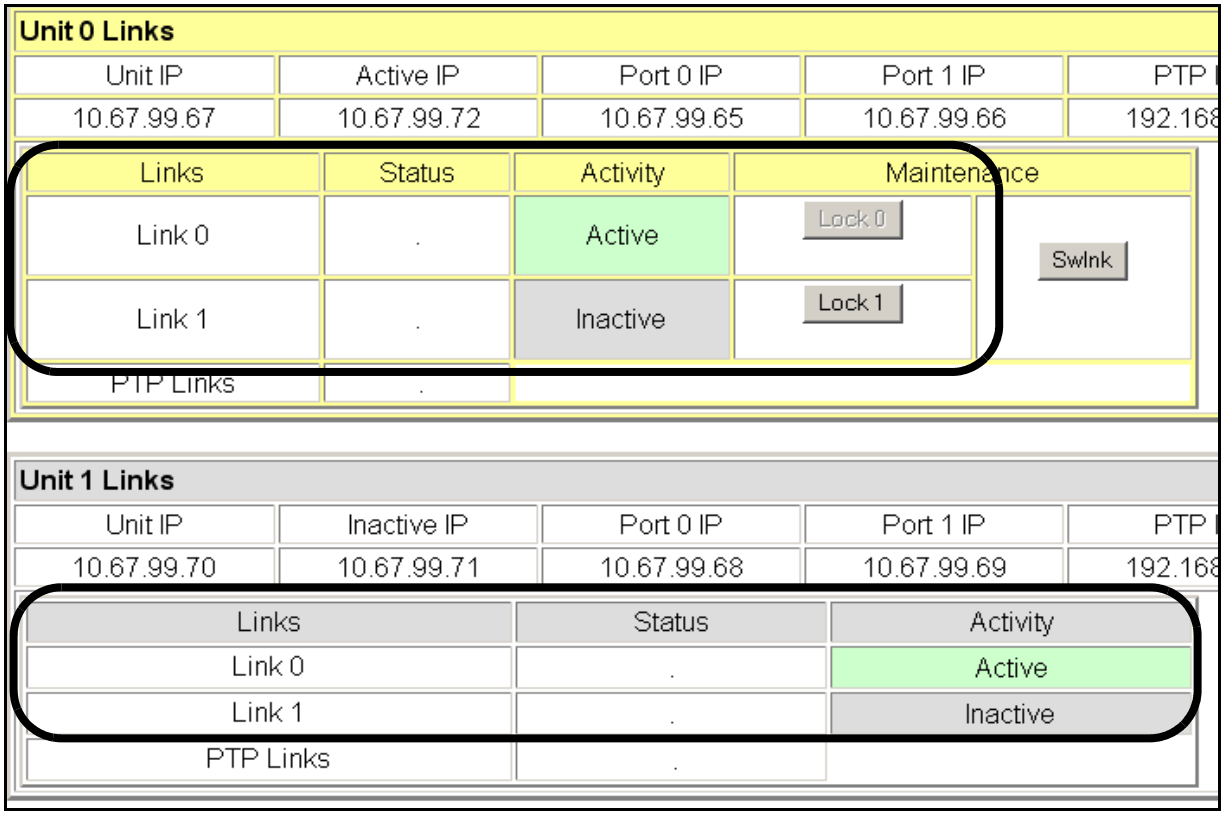
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Network Connectivity** link.

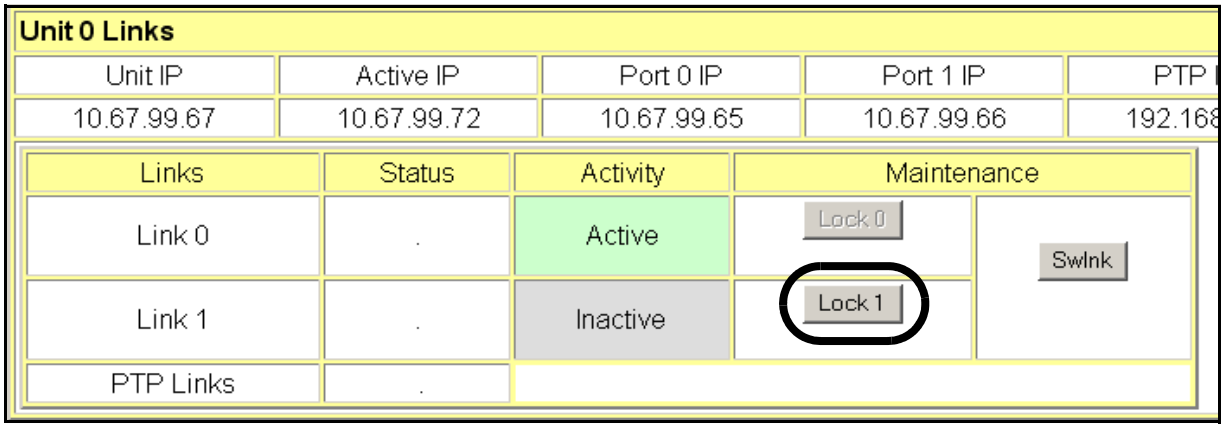
The Network Connectivity page is displayed.



3 Review the link state of the Session Server units.



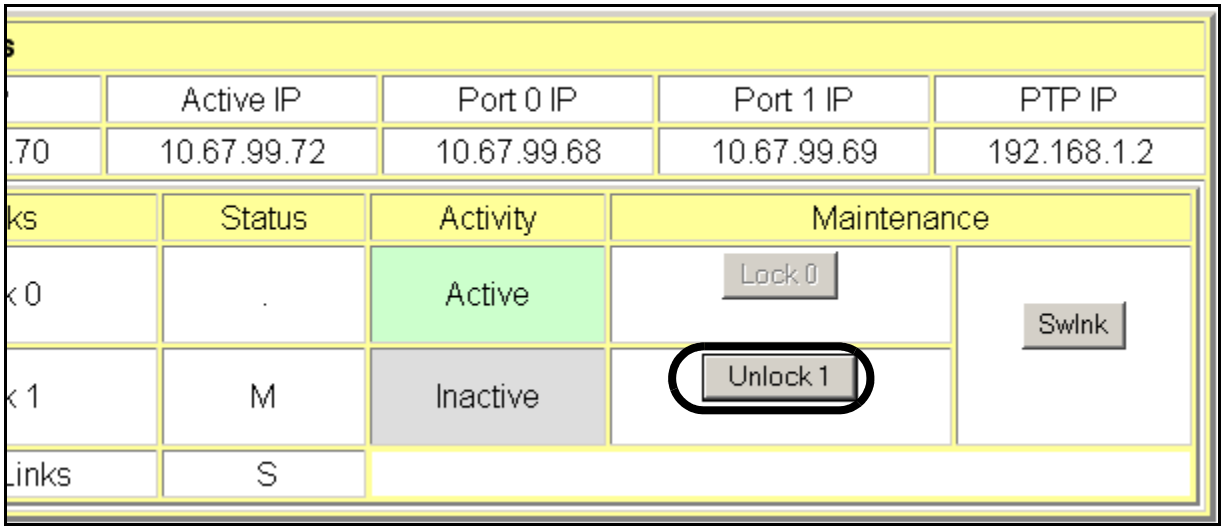
4 Click the **Lock** button for the inactive link on the active unit.



The system responds:

```
Info: Lock Link X - Command passed.
```

5 Ensure that the **Lock** button for the inactive link transitions to **Unlock**.



6 This procedure is complete.

Unlock network ethernet link

Purpose of this procedure

This procedure is used to unlock (start) a Session Server unit's inactive (locked) ethernet link.

Limits and Restrictions

Use this procedure as part of maintenance or fault clearing activities.

Prerequisites

The unit's inactive ethernet link must already be in a locked state.

Action

At the CS 2000 Session Server Launch Point

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

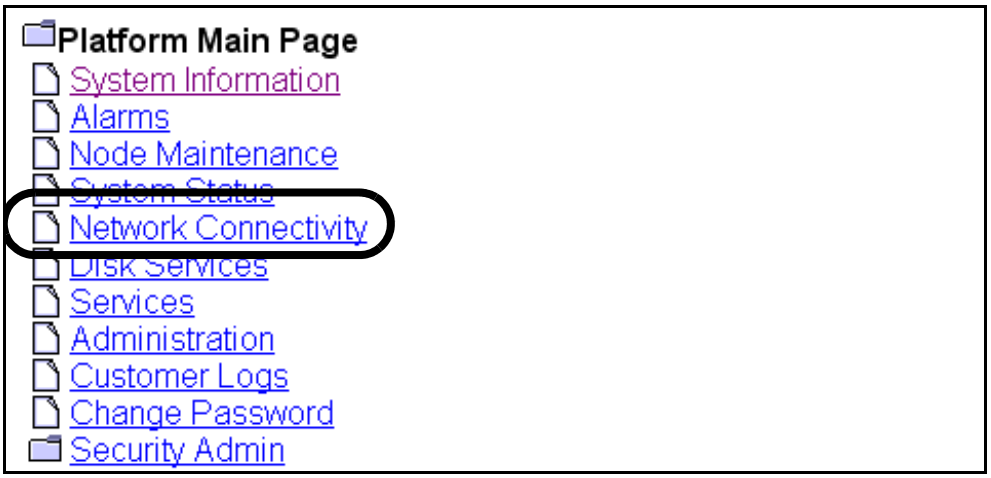
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

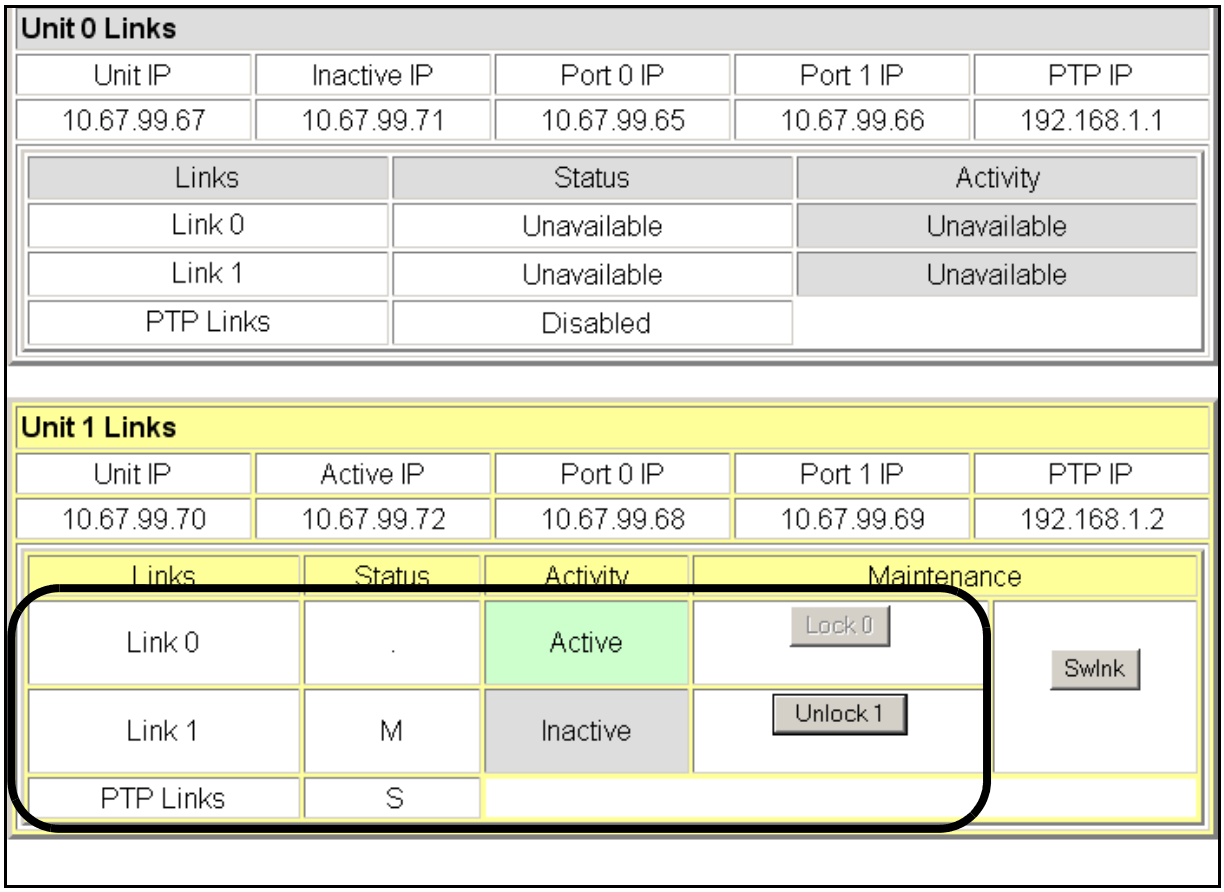
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Network Connectivity** link.

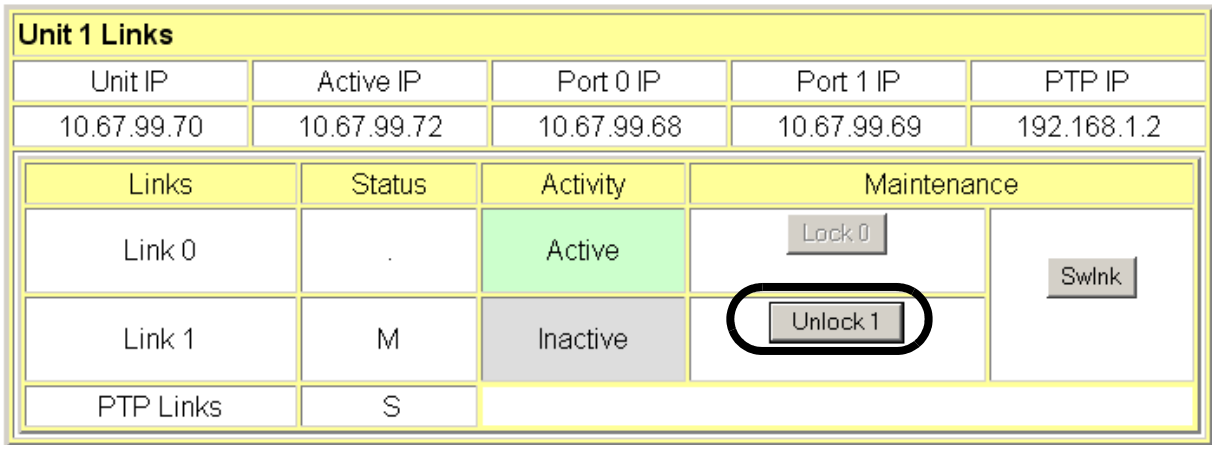
The Network Connectivity page is displayed.



3 Review the link state of the active Session Server unit.



4 Click the **Unlock** button for the inactive link on the active unit.



The system responds:

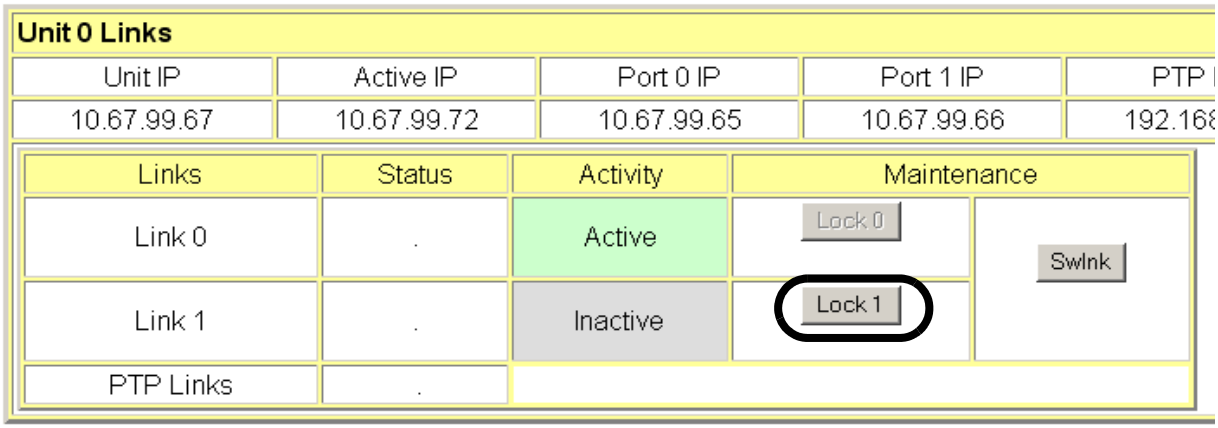
```
Are you sure you wish to Lock link X?
Click OK to confirm Lock or cancel to abort.
```

5 Click **OK** to confirm the unlock.

The system responds:

```
Info: Unlock Link X - Command passed.
```

6 Ensure that the **UnLock** button for the inactive link transitions to **Lock**



7 This procedure is complete.

Halt (shutdown) a Session Server unit

Purpose of this procedure

This procedure is used to perform a graceful shutdown a Session Server platform NCGL operating system. Use this procedure only as part of a high-level activity such as part of a controlled shutdown activity or part of a software upgrade activity. Included at the end of this procedure is an alternate CLI method for halting a unit.

Limitations and Restrictions

This procedure can only be performed from the active Session Server unit.

This procedure does not cause the Session Server unit to power-off.

CAUTION

This procedure halts all call processing activity and billing record generation on the affected unit, and prevents the Session Server node from operating in a fault-tolerant mode. Ensure that the unit you are shutting down is not performing call processing activities.

Prerequisites

Use procedure View the operational status of the NCGL platform on page 99 to check for any disk array rebuilds in progress. Wait for the rebuild to complete before executing this procedure.

Action

At the Session Server GUI or Integrated EMS client

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

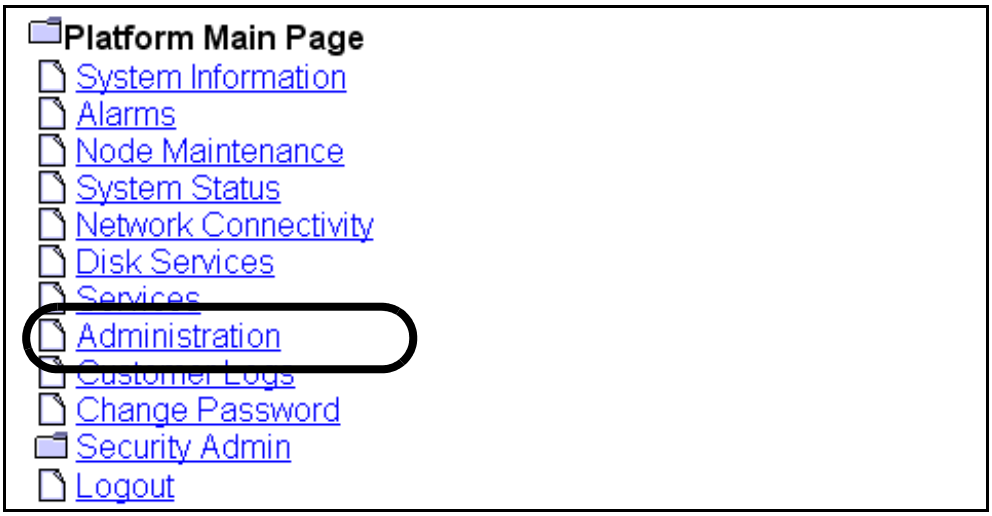
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

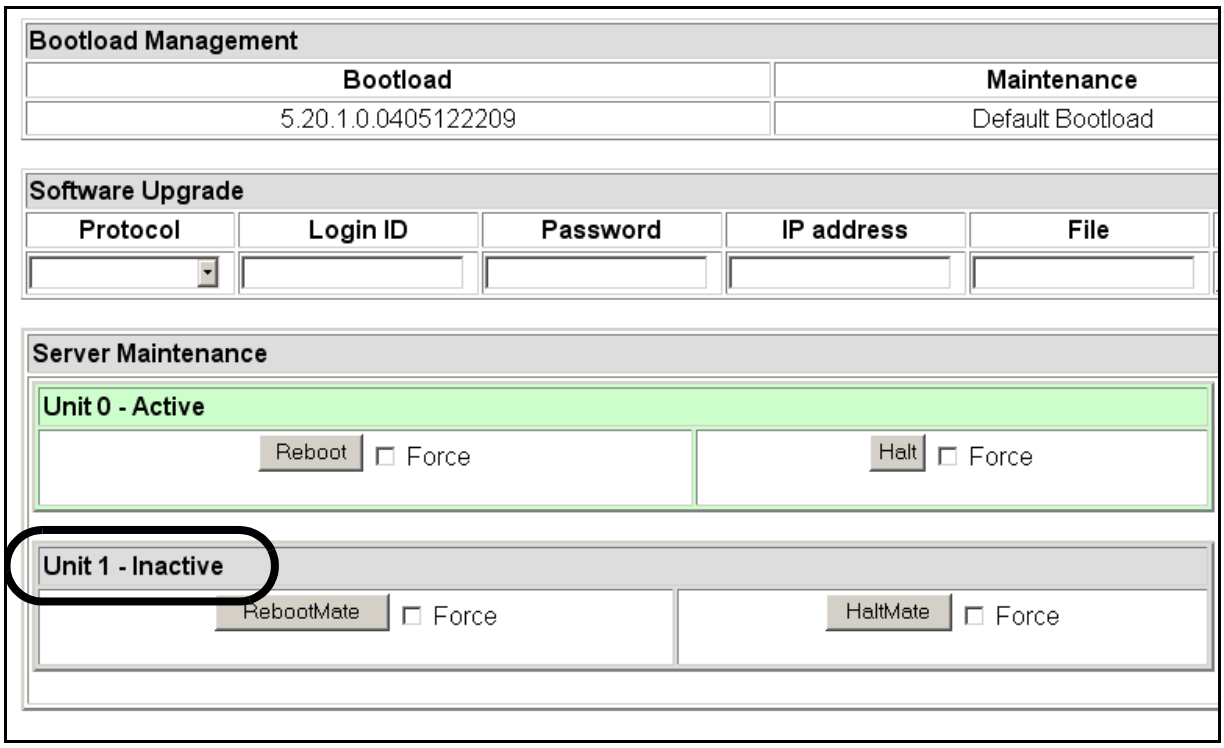
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Administration** link.

The Administration page is displayed.



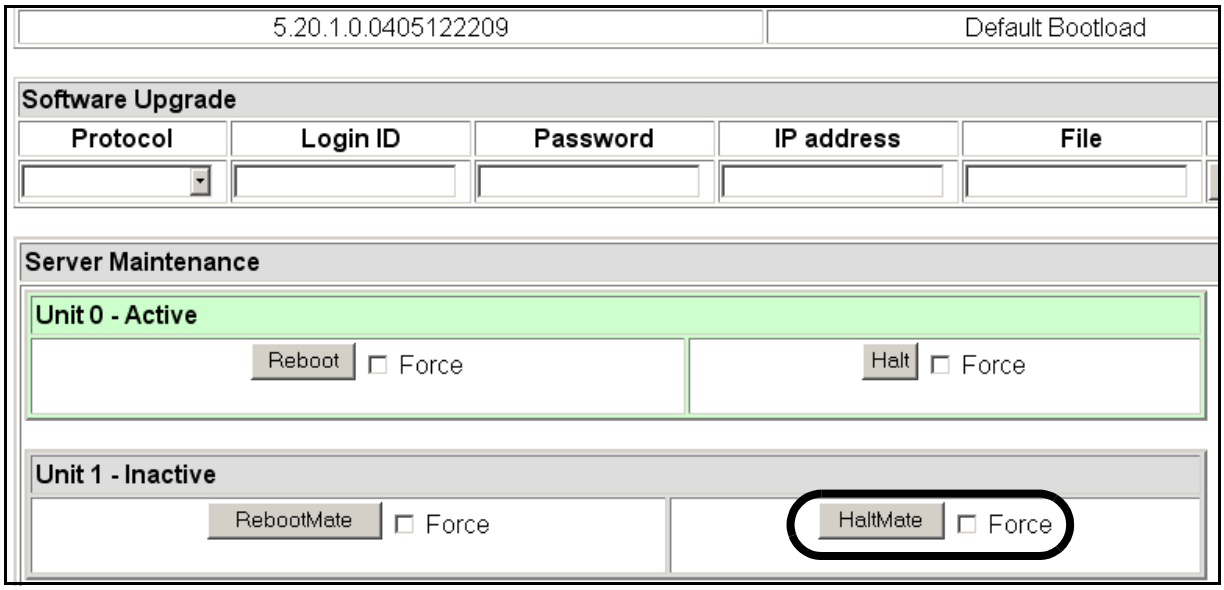
3 Review the status of the unit you want to halt. If it is unavailable, the **Halt** or **HaltMate** buttons are not accessible.



4 Click the **Halt** or **HaltMate** button for the Session Server unit you want to halt the NCGL operating system for.

Note 1: To override any pre-halt (shutdown) queries, click the **Force** check box before clicking the **Halt** or **HaltMate** button.

Note 2: In a system operating in fault-tolerant (duplex) mode, only the inactive unit can be shut down using HaltMate or a Forced HaltMate. A Halt or Forced Halt can only be performed if the system is operating in simplex mode.



The system responds:

```
Are you sure you wish to halt?
This may cause an extended service outage to any
clients currently using this server. Click OK to
confirm server halt or cancel to abort.
```

5 Click **OK** to confirm the halt operation.

The NGCL and all call activity on the affected Session Server begin the process of halting. This can take several minutes.

6 If you receive the following message, you must halt the unit using the Force option in step 4.

```
Error: Command failed. Reason: Mate not
available.
```

7 If applicable, complete procedure Power-Off a Session Server unit on page 137 to disconnect power from the unit.

8 This procedure is complete.

To Haltmate or Force Haltmate?

The Haltmate action does not work if the SIP Gateway application database on the active unit is out of sync with the database on the inactive unit. Using the Haltmate command with the Force option overrides any pre-checks for this condition and forces a Halt of the inactive unit regardless of the sync state of the active unit database.

Alternate command line interface (CLI) method

ATTENTION

All prerequisites and restrictions shown on page 80 apply to using this procedure.

At Session Server CLI or Integrated EMS client

1. Log onto the active Session Server unit CLI and change to the root user.
2. Shutdown the selected Session Server unit by typing

   `# mtccli haltmate` (to shutdown the inactive unit)

   or

   `# mtccli halt` (to shutdown the active unit operating in simplex mode)

   and pressing the **Enter** key.
3. If applicable, complete procedure Power-Off a Session Server unit on page 137 to disconnect power from the unit.
4. You have completed this procedure.

Reboot a unit

Purpose of this procedure

Use this procedure to perform a graceful shutdown and reboot of a unit. Use this procedure only as part of a high-level activity such as maintenance or fault clearing activities or as part of a software upgrade activity.

ATTENTION
This procedure causes a three to four minute service interruption of the affected unit. Use this procedure only when recommended by Nortel support personnel.

Limitations and Restrictions

ATTENTION
Nortel recommends performing this procedure only on the standby unit; however, this procedure can be performed only from the active unit.

CAUTION
Loss of redundancy
This procedure halts all call processing activity and billing record generation on the affected unit and prevents the node from operating in a fault-tolerant mode.

Prerequisites

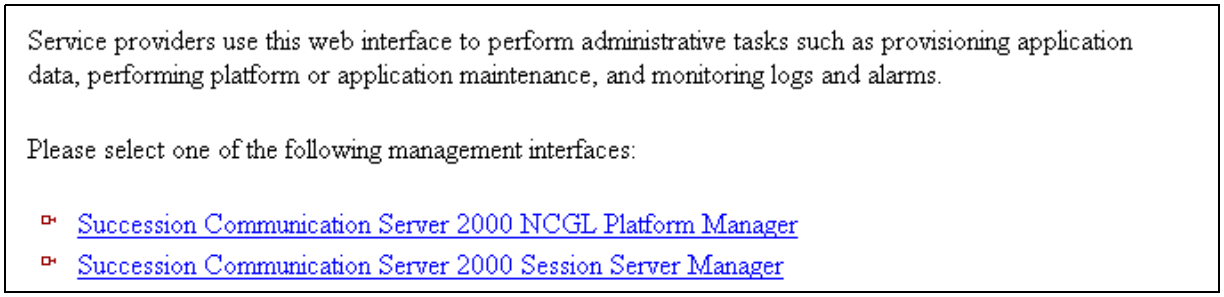
Use procedure View the operational status of the NCGL platform on page 99 to check for any disk array rebuilds in progress. Wait for the rebuild to complete before executing this procedure.

Ensure that you have your bootable software installation CD/DVD disk available, in case you have trouble rebooting the unit.

Action

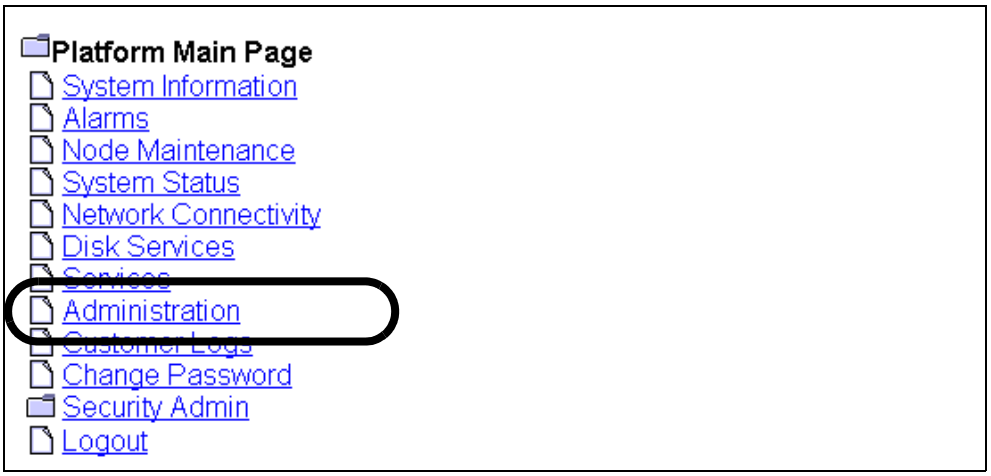
At the CS 2000 NCGL Platform Manager or IEMS client for the active unit

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



2 Click the Administration link.

The Administration page is displayed.

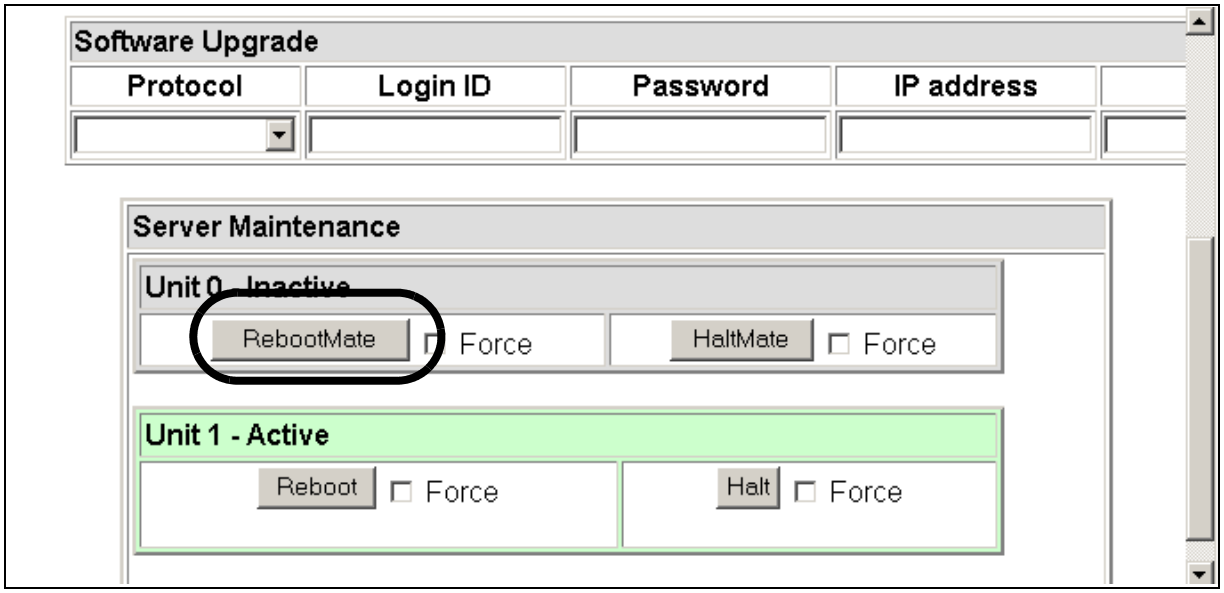


3 Review the status of the unit you want to reboot.

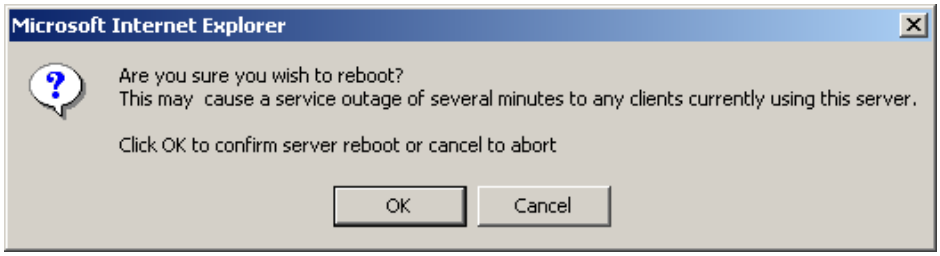
4 Click RebootMate to reboot the inactive unit, or Reboot to reboot the active unit.

Note 1: If you want to override any pre-reboot queries including a pre-check by applications running on the unit, click the Force check box.

Note 2: If the buttons are disabled, then this is the inactive unit. Reconnect to the active unit.

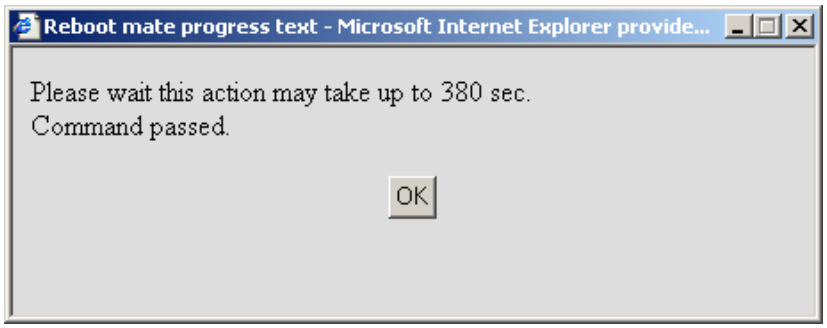


The system responds with the following message box. If pop up windows are disabled in the web browser, the message box does not appear.



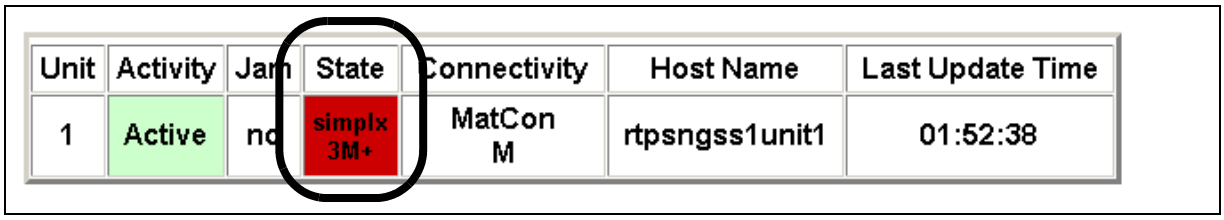
5 Click OK to confirm the reboot operation.

The NGCL and all call activity on the affected unit is shutdown and the unit begins to reboot. The system responds with the following message box:



6 Click OK to close the dialog box.

7 Monitor the recovery of the rebooting unit using procedure View the operational status of the NCGL platform on page 99 to confirm the recovery of the unit after reboot. Continue monitoring the active unit until you see the State field in the alarm panel change back to duplex.



8 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Alternate command line interface (CLI) method

CAUTION
Loss of redundancy
This procedure halts all call processing activity and billing record generation on the affected unit and prevents the node from operating in a fault-tolerant mode.

Halting the active unit will cause loss all call processing and billing generation for the entire node.

ATTENTION
All prerequisites and restrictions shown on page 84 apply when using this procedure.

At NCGL CLI or IEMS client

1 Log on to the active unit and change to the root user.

2 Reboot the selected unit by typing

```
# mtccli rebootmate  (to reboot the inactive unit)
```

or

```
# mtccli reboot  (to reboot the active unit operating in simplex mode)
```

3 Use procedure View the operational status of the NCGL platform on page 99 to confirm the recovery of the unit after reboot.

4 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Troubleshooting reboots

The following possible error messages received during a reboot attempt and their meaning are described:

Error: Command failed. Reason: Mate not available.
Reboot the unit using the Alternate command line interface (CLI) method on page 88.

Error: Reboot - Command rejected. Reason: Mate is available.
The user has attempted to reboot the active server when the inactive server is available.

Error: Halt - Command rejected. Reason: Mate is available.
The user has attempted to halt the active server when the inactive server is available.

Error: Command failed. Reason: PRECHECK FAILED: application rejected request.
The user has attempted a rebootmate or haltmate command and the application rejected the request. Check /var/log/designlog to determine the name of the application that rejected the maintenance command.

Actions:

- Using the Force option overcomes a pre-check failure by any application running on the unit.
- Try the operation again later. If the problem persists, then contact Nortel Networks support personnel for assistance.

Verify synchronization status

Purpose of this procedure

Use this procedure to determine the synchronization status of the two units.

Limitations and restrictions

There are no restrictions for performing this procedure.

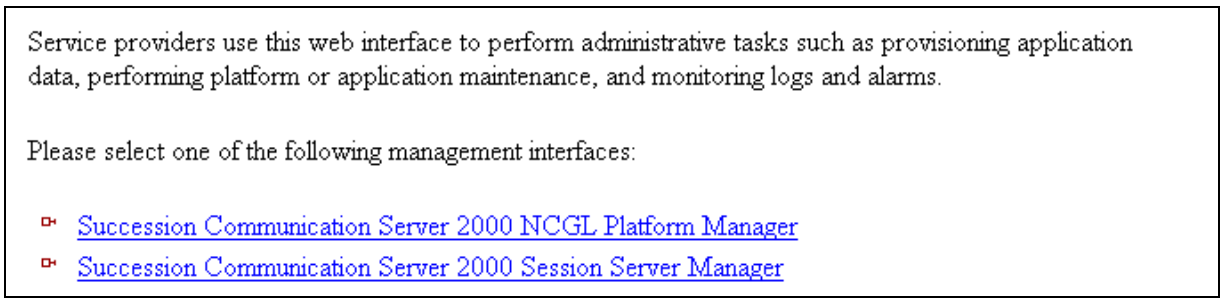
Prerequisites

There are no prerequisites for performing this procedure.

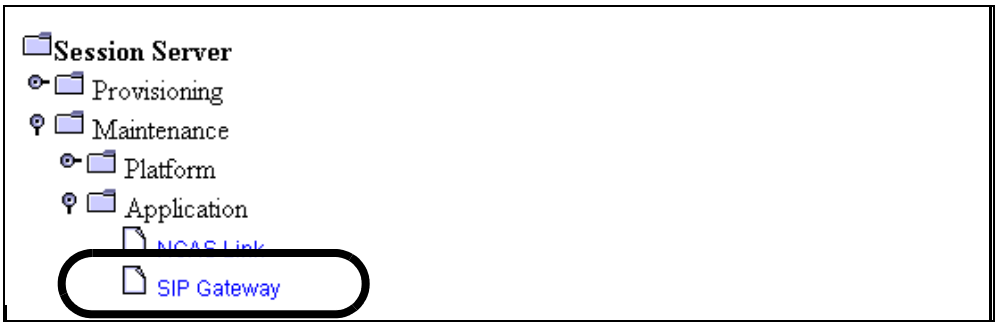
Action

At the CS 2000 Session Server Manager or IEMS client

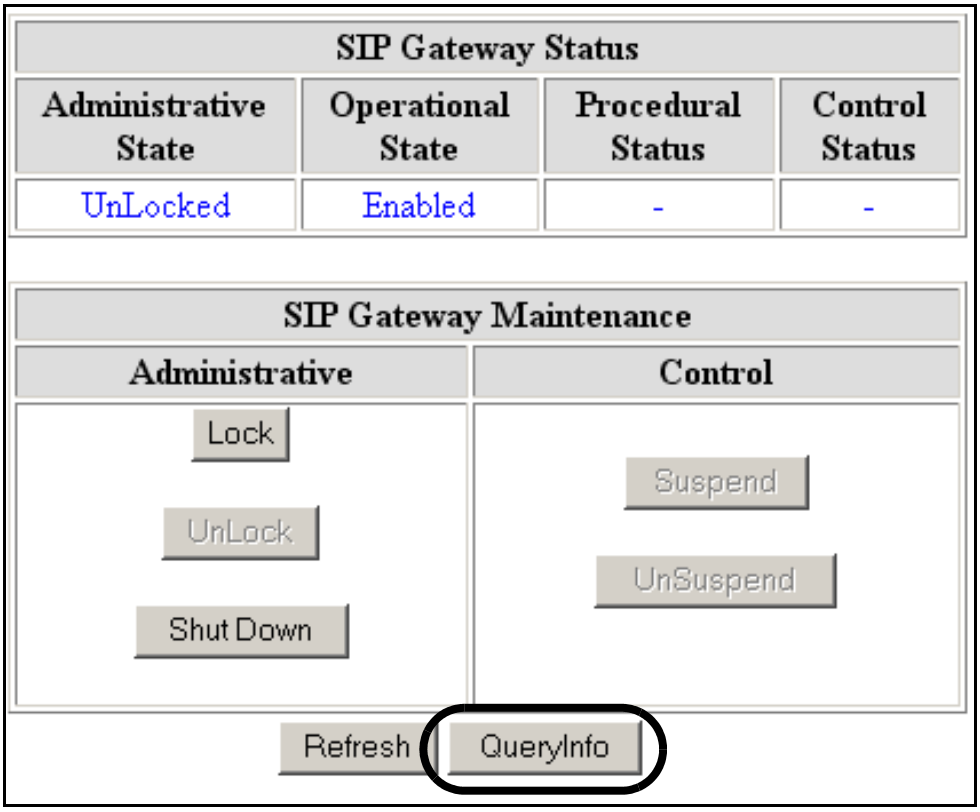
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.



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

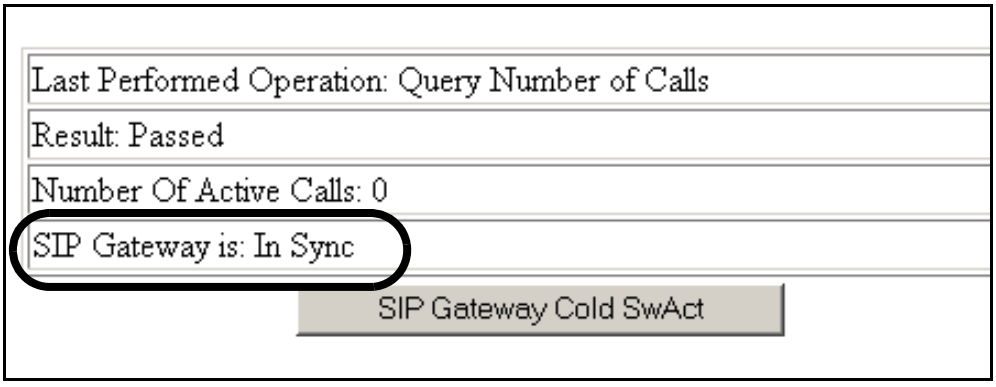


3 At the bottom of the SIP Gateway Maintenance panel, locate and click the QueryInfo button.



4 The synchronization status of the units is displayed at the bottom of the query results panel.

If the units are not in sync, check for alarm conditions.



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

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.

Limitations and restrictions

This procedure provides instructions for determining the service status of the SIP Gateway application software only. For instructions on determining the status of the platform and operating system, refer to procedure View the operational status of the NCGL platform on page 99.

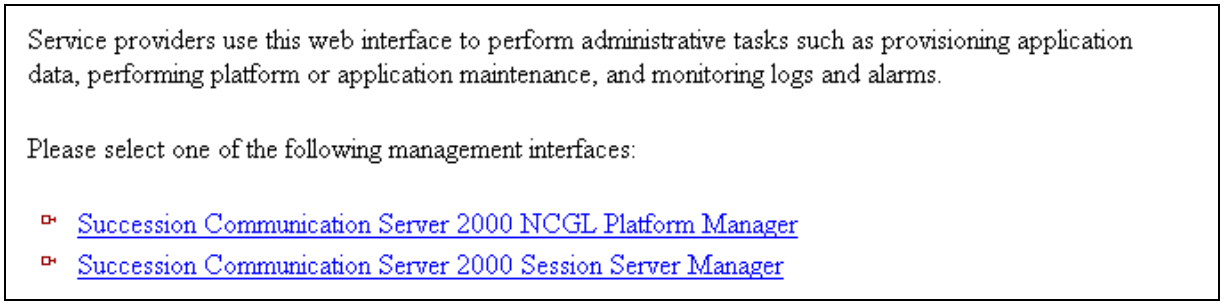
Prerequisites

There are no prerequisites for this procedure.

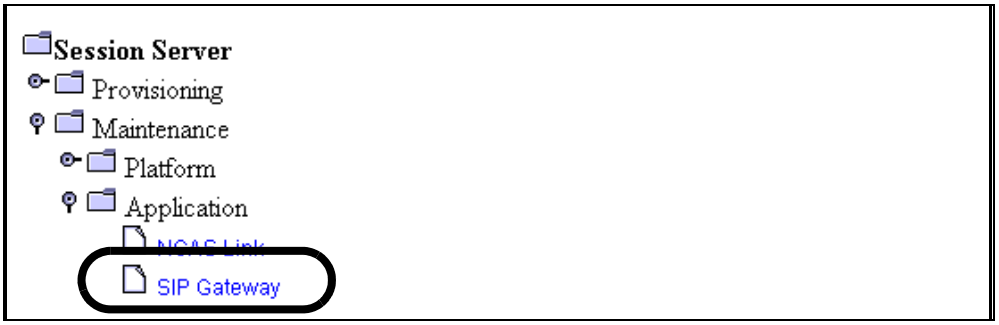
Action

At the CS 2000 Session Server Manager or IEMS client

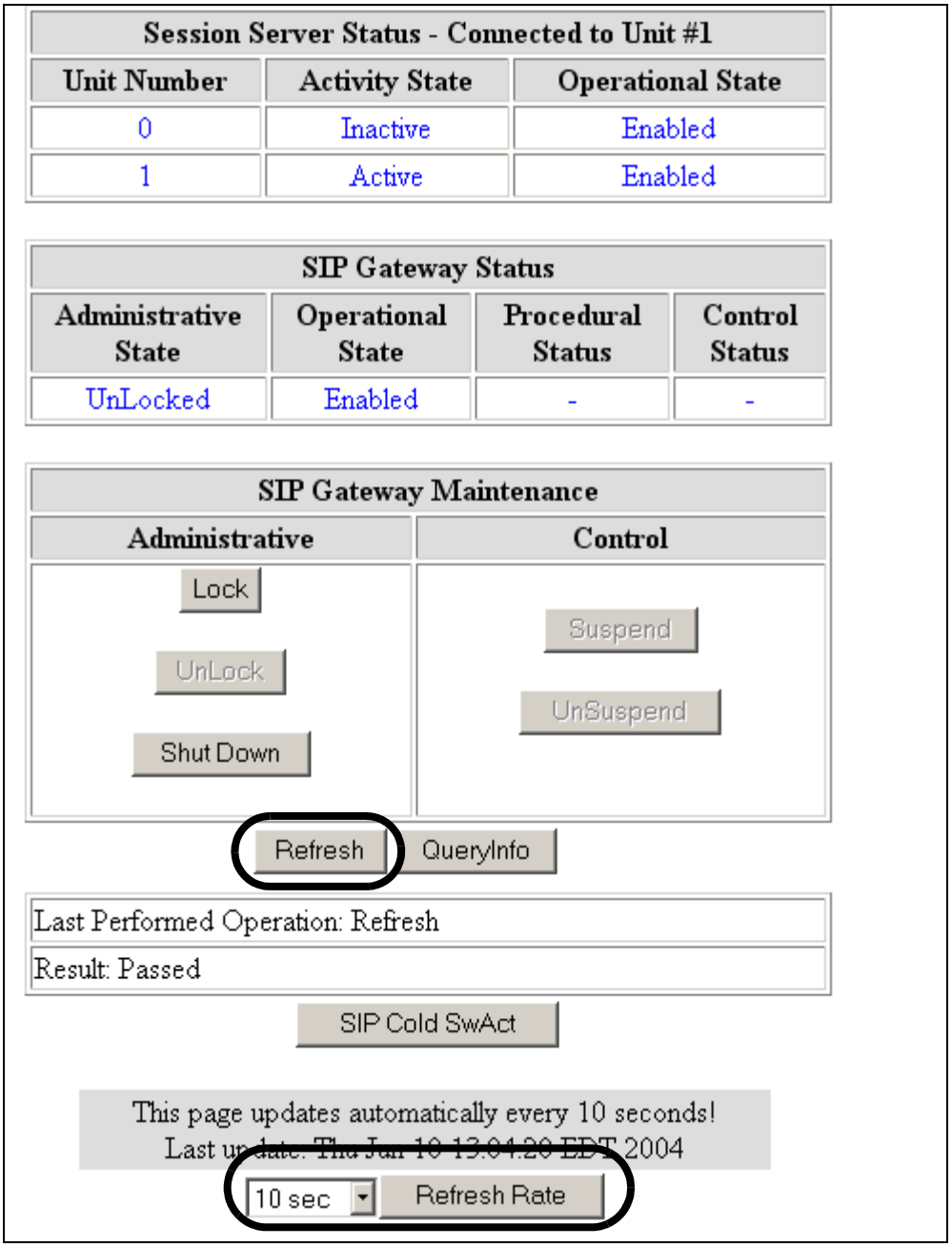
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.



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



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



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.

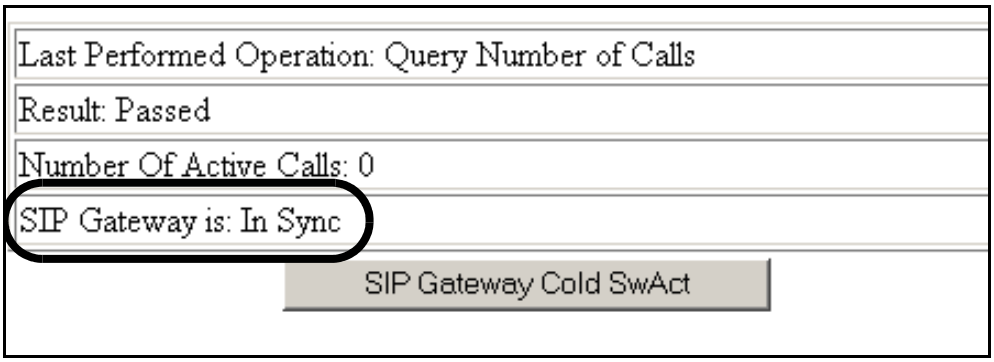
4 Refer to section Interpreting SIP Gateway application status and maintenance fields on page 96 to review the description of the various fields of this view.

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

5 The following service affecting actions are available:

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

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



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

Interpreting SIP Gateway application status and maintenance fields

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

Node status field descriptions

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

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

SIP Gateway application Status field descriptions

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

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

SIP Gateway Maintenance field descriptions and interpretation of service states

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

Purpose of this procedure

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

Limitations and restrictions

This procedure provides instructions for determining the service status of the 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 *Session Server - Trunks Configuration Management*, 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 view customer logs or alarms. For detailed instructions on viewing customer logs or alarms, refer to procedures in *Session Server - Trunks Fault Management*, NN10332-911.

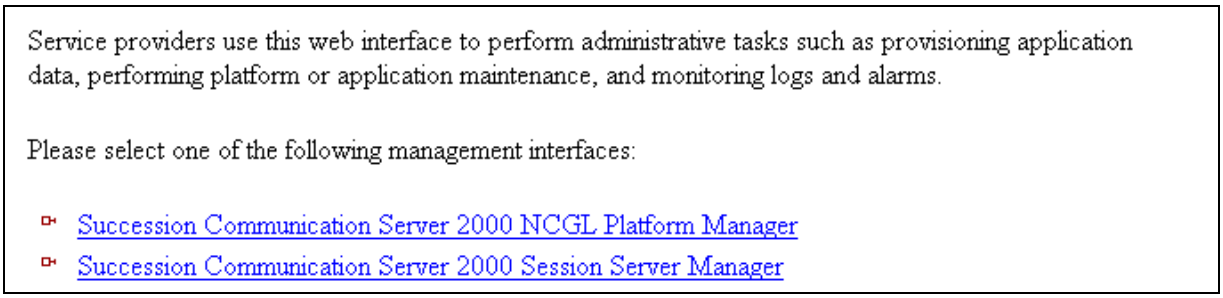
Prerequisites

There are no prerequisites for using this procedure.

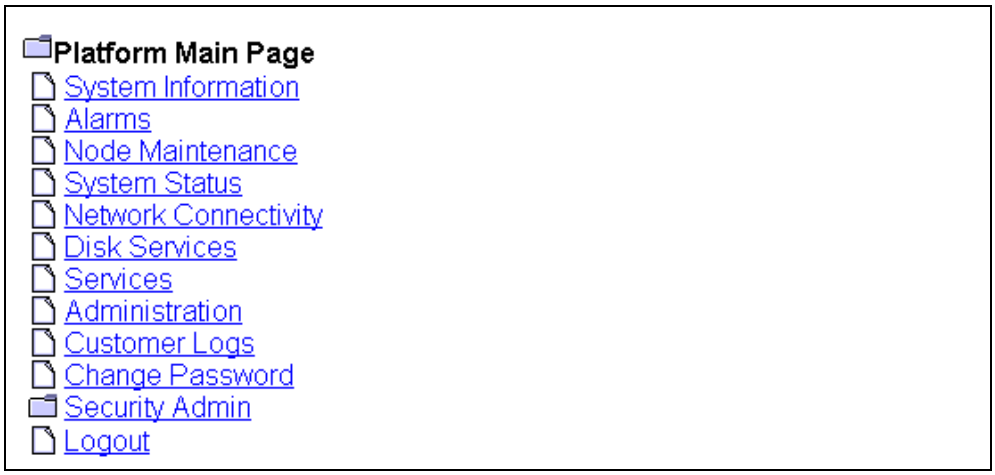
Action

At the CS 2000 NCGL Platform Manager or IEMS client

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



The Platform Main Page menu is displayed.



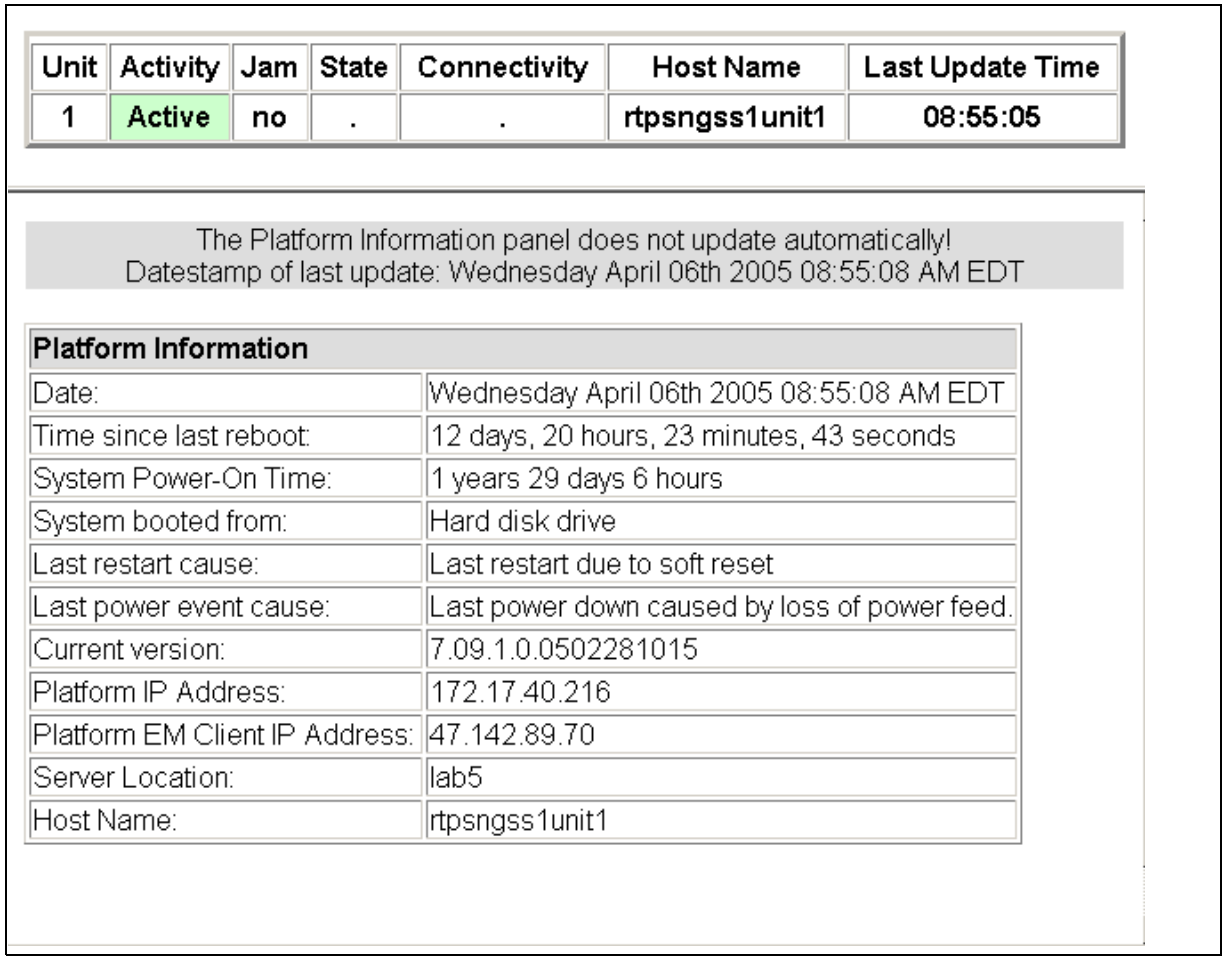
2 Use the following table to determine your next step:

If	Do
you want to review the version of the platform software load, boot statistics and platform IP address	Click the System Information link and go to step 3.
you want to review existing platform alarms	Go to step 17 and go to procedure "View Session Server alarms" in *Session Server Fault Management*, 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 *Session Server - Trunks Security and Administration*, NN10346-611.	Click the Network Connectivity link and go to step 9.
you want to review storage related information including array status, disk capacity and disk alarm thresholds	Click the Disk Services link and go to step 10.
you want to review details about platform services including the network time protocol servers	Click the Services link and go to step 12.
you want to review platform version information only	Click the Administration link and go to step 14.
you want to review customer logs	Go to step 17 and refer to *Session Server - Trunks Fault Management*, NN10332-911.
you want to change root passwords	Go to step 17 and refer to *Session Server - Trunks Security and Administration*, NN10346-611.
you want to view TLS security information or manage security certificates	Go to step 17 and refer to *Session Server - Trunks Configuration Management*, NN10338-511 to review TLS security settings.
you are finished reviewing information and want to log out from the GUI	step 16.

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

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
1	Active	no	.	.	rtpsngss1unit1	08:55:05

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

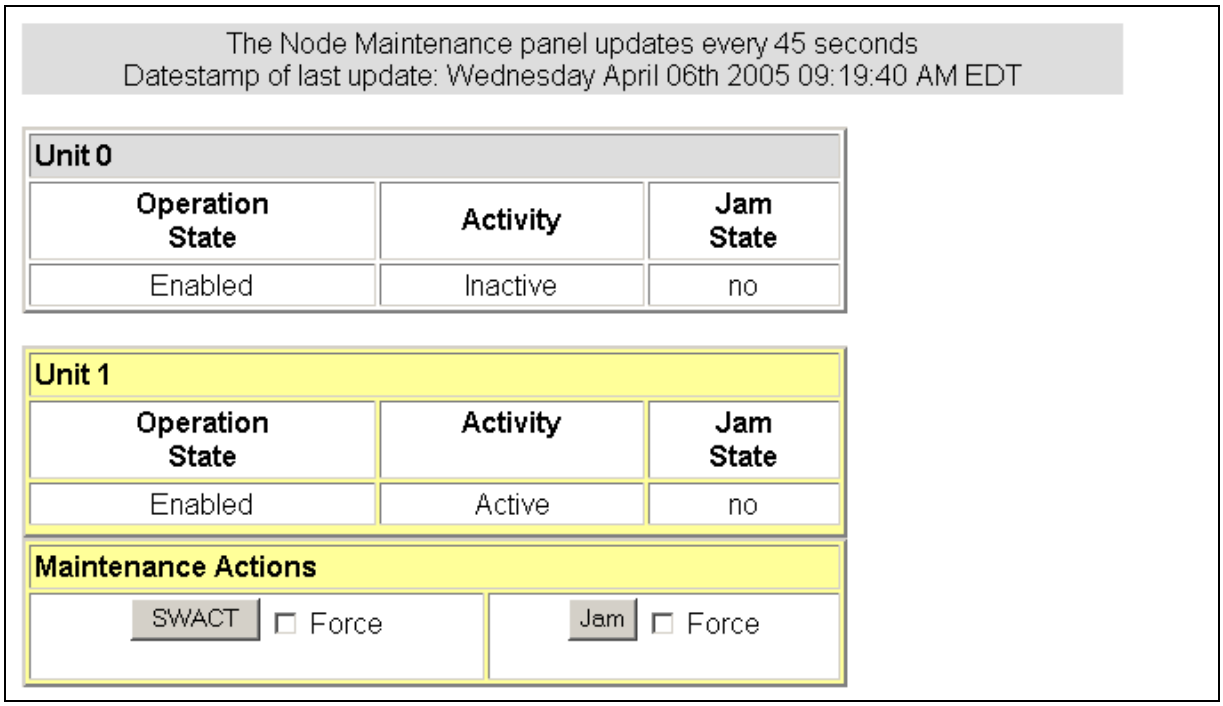
Platform Information	
Date:	Wednesday April 06th 2005 08:55:08 AM EDT
Time since last reboot:	12 days, 20 hours, 23 minutes, 43 seconds
System Power-On Time:	1 years 29 days 6 hours
System booted from:	Hard disk drive
Last restart cause:	Last restart due to soft reset
Last power event cause:	Last power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

Field	Description
Unit	unit number in the node that you are logged into
Activity	activity of the unit (either active or standby)
Jam	indicates if the inactive unit is Jammed. The value is YES only if logged in to the inactive unit. From the active unit, the status is NO, but a JInact alarm indicates the inactive is Jammed.

Field	Description
State	indicates if the node is operating in a duplex (fault-tolerant) mode or a simplex mode (the standby unit is off-line)
Connectivity	state of the network links on the node
Host Name	name of the unit (not node)
Date	system date as maintained by the network time protocol (NTP) server
Time since last reboot:	amount of time that has elapsed since the unit was last rebooted for any reason
System Power-On Time:	recorded system time that the unit has been powered up
System booted from:	indicates whether the unit is currently booted from the hard drive or DVD-ROM drive
Last restart cause:	indicates any event that forced a platform reboot (manual or system generated)
Last power event cause:	indicates any event that affected the power supply subsystem of the unit chassis
Current version:	installed version of the NCGL platform software
Platform IP Address:	unit IP address
Platform EM Client IP Address:	IP address of the client web browser. When a web proxy is used, the IP address of the machine performing the proxy is displayed
Server Location:	physical location of the unit
Host Name:	name of the unit

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

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



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

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

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

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

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

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

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

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

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

Note: The Chassis Information panel is not automatically refreshed.

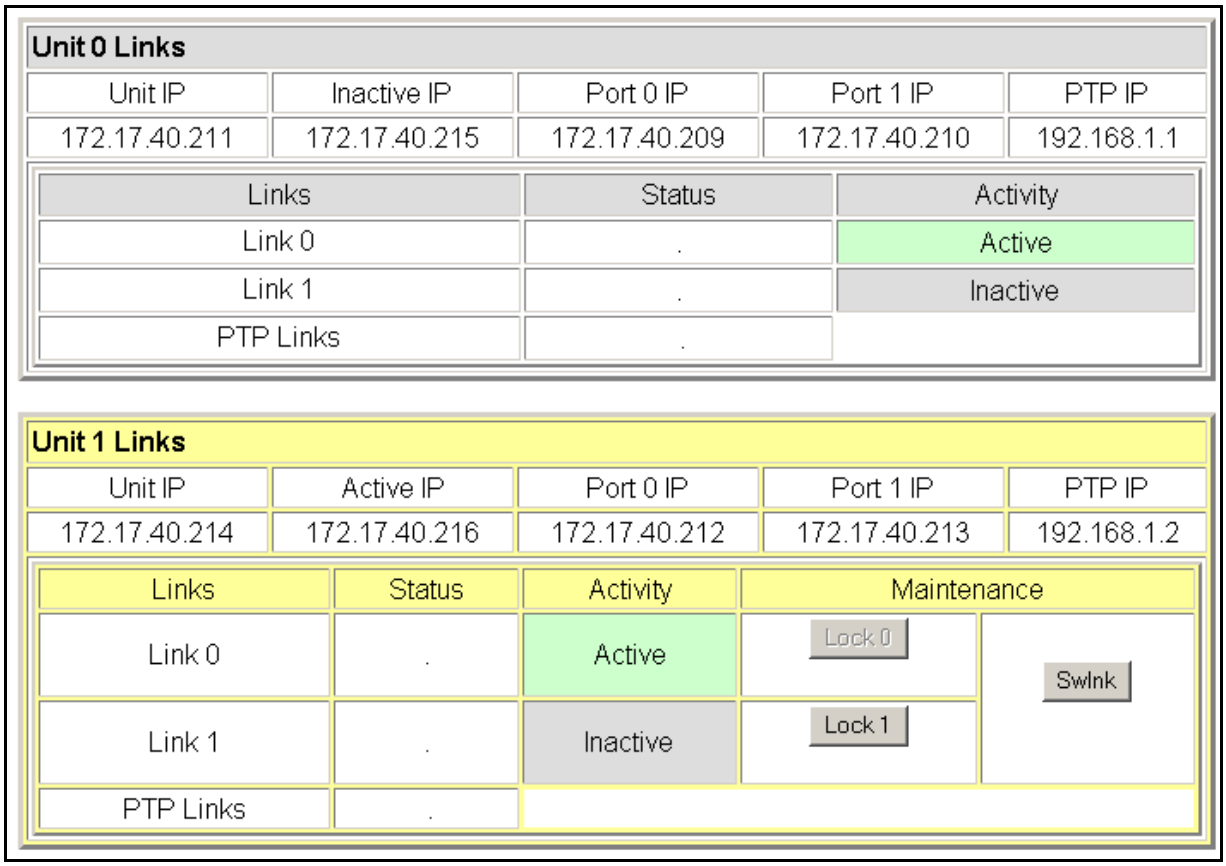
Field	Description
Chassis information: Self Test	status of the self test performed on the platform at boot up
Chassis information: Chassis Subsystems	status of the platform hardware subsystems including the memory, CPU, all drives, network connection, power supplies, cooling and other I/O connections
CPU 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	total number of processes (non-threaded) that are running on the Session Server Platform
Process Information: Number of zombie processes	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	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	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	maximum number of zombie processes allowed to be run by the CPU before a critical alarm is raised indicating that the set threshold has been exceeded
Memory Information: Total Memory (MB)	total amount of RAM installed on the motherboard of each Session Server unit. Both units must have the same amount.
Memory Information: Free Memory (MB)	amount of memory available unallocated for use
Memory Information: Available memory (MB)	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:

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



Unit 0 Links

Unit IP	Inactive IP	Port 0 IP	Port 1 IP	PTP IP
172.17.40.211	172.17.40.215	172.17.40.209	172.17.40.210	192.168.1.1

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

Unit 1 Links

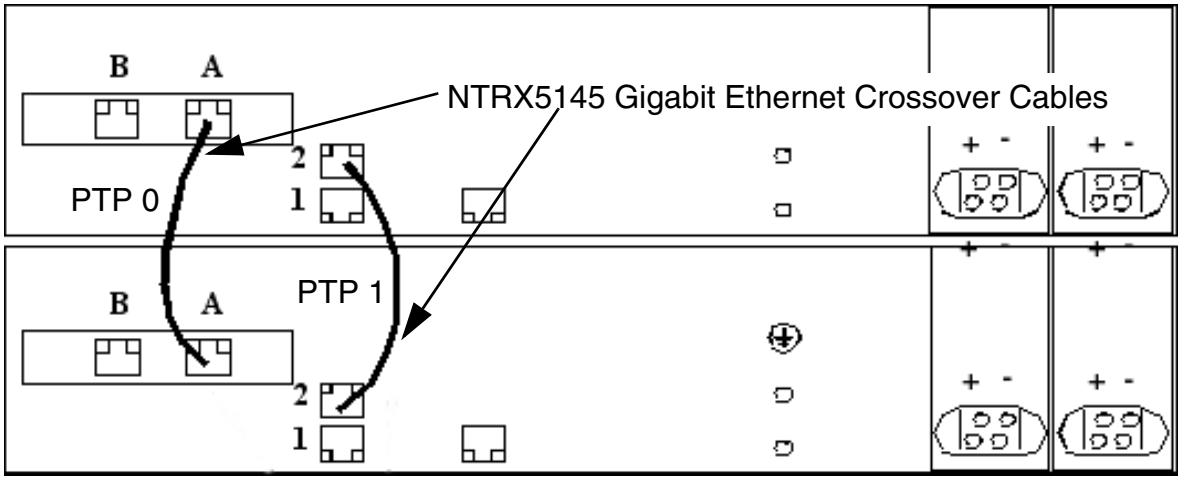
Unit IP	Active IP	Port 0 IP	Port 1 IP	PTP IP
172.17.40.214	172.17.40.216	172.17.40.212	172.17.40.213	192.168.1.2

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

Field	Description
Unit 0,1 Links	indicates which Ethernet IP links are installed on the units (each unit has two links)
Unit 0,1 Status	status of the Ethernet links
Unit 0,1 Activity	activity status of the Ethernet links, either active or inactive
Unit 0,1 Maintenance	indicates the maintenance actions that can be performed on the Ethernet links, either Lock, Unlock or Swlink
Unit 0,1 PTP Links status	status of the PTP links between both units in the node

Field	Description
Unit IP	network IP address of the Session Server unit
Active IP	IP address of the local (active) Session Server unit
Inactive IP	IP address of the mate (inactive) Session Server unit
Port 0 IP	IP address of the active or inactive Ethernet port 0
Port 1 IP	IP address of the active or inactive Ethernet port 1
PTP IP	IP address of the active or inactive PTP link

Crossover and LAN Ethernet cable connections for 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 *Session Server - Trunks Configuration Management*, 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

Create New Filesystem | Remove Filesystem

Volume Group Information

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

Field	Description
RAID Array Status: Name	indicates the name of each RAID-1 array in the system
RAID Array Status: Size (GB)	indicates the size of the partition in gigabytes

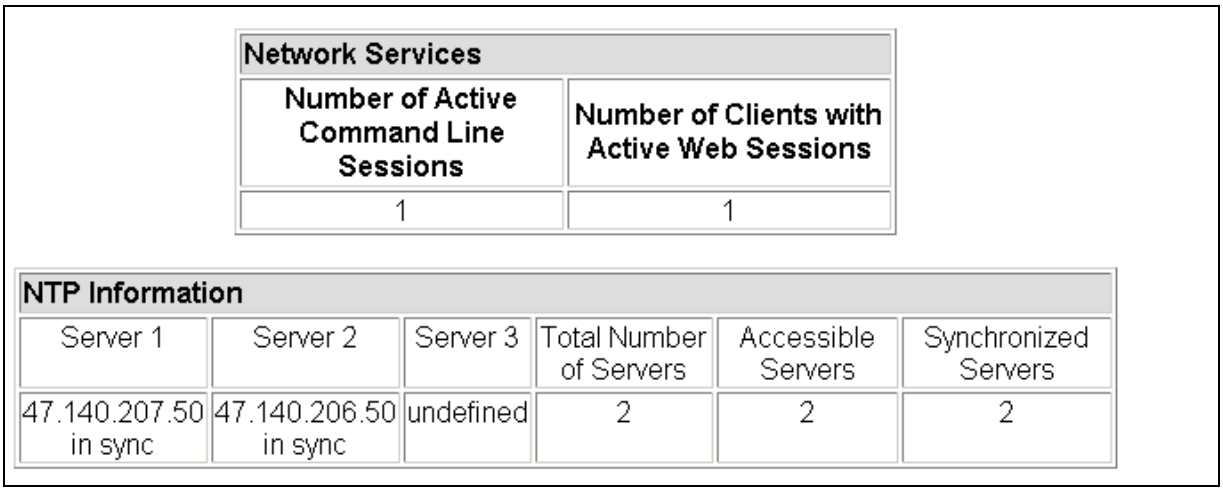
Field	Description
RAID Array Status: State	Indicates a high level state for the array: - ".": indicates the array is functioning normally. - Missing: a disk was removed from the array. - Failed: a disk in the array has failed and needs to be replaced. - Rebuilding: the array is in the process of rebuilding to a fault-tolerant mode.
RAID Array Status: Disk 0	service status of disk 0
RAID Array Status: Disk 1	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)	total capacity of the disk drive in gigabytes
Disk Maintenance: Disk State	installation state of the disk
Disk Maintenance: Disk Action	indicates whether a hard disk can be inserted into the RAID array
Filesystem Information: Monitor	indicates the status of individual filesystems on the disk array
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)	total amount of disk space (in MB) allocated for this filesystem
Filesystem Information: Total Space Used (MB)	total amount of disk space (in MB) in use on this file system
Filesystem Information: Total Space Used (%)	total amount of disk space (in %) in use on this file system

Field	Description
Filesystem Information: Total Space Available (MB)	percentage of total disk space (in MB) free for use on this filesystem
Filesystem Information: Total Space Available (%)	amount of disk space (in %) available for use by platform processes and applications
Filesystem Information: Minor Alarm Threshold (%)	maximum amount of disk space (in %) that can be used before a minor alarm is raised indicating that the set threshold has been exceeded
Filesystem Information: Major Alarm Threshold (%)	maximum amount of disk space (in %) that can be used before a major alarm is raised indicating that the set threshold has been exceeded
Filesystem Information: Critical Alarm Threshold (%)	maximum amount of disk space (in %) that can be used before a critical alarm is raised indicating that the set threshold has been exceeded
Volume Group Information: Volume Group Name	name of the volume group in the array
Volume Group Information: Volume Group Size (GB)	total size of the volume group in the array
Volume Group Information: Total Space Allocated (GB)	amount of volume group space, in gigabytes, currently allocated to filesystems
Volume Group Information: Total Space Allocated (%)	amount of volume group space (in %) currently allocated to filesystems
Volume Group Information: Total Space Available (GB)	amount of unallocated volume group space, in gigabytes, available for filesystems
Volume Group Information: Total Space Available (%)	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
1	1

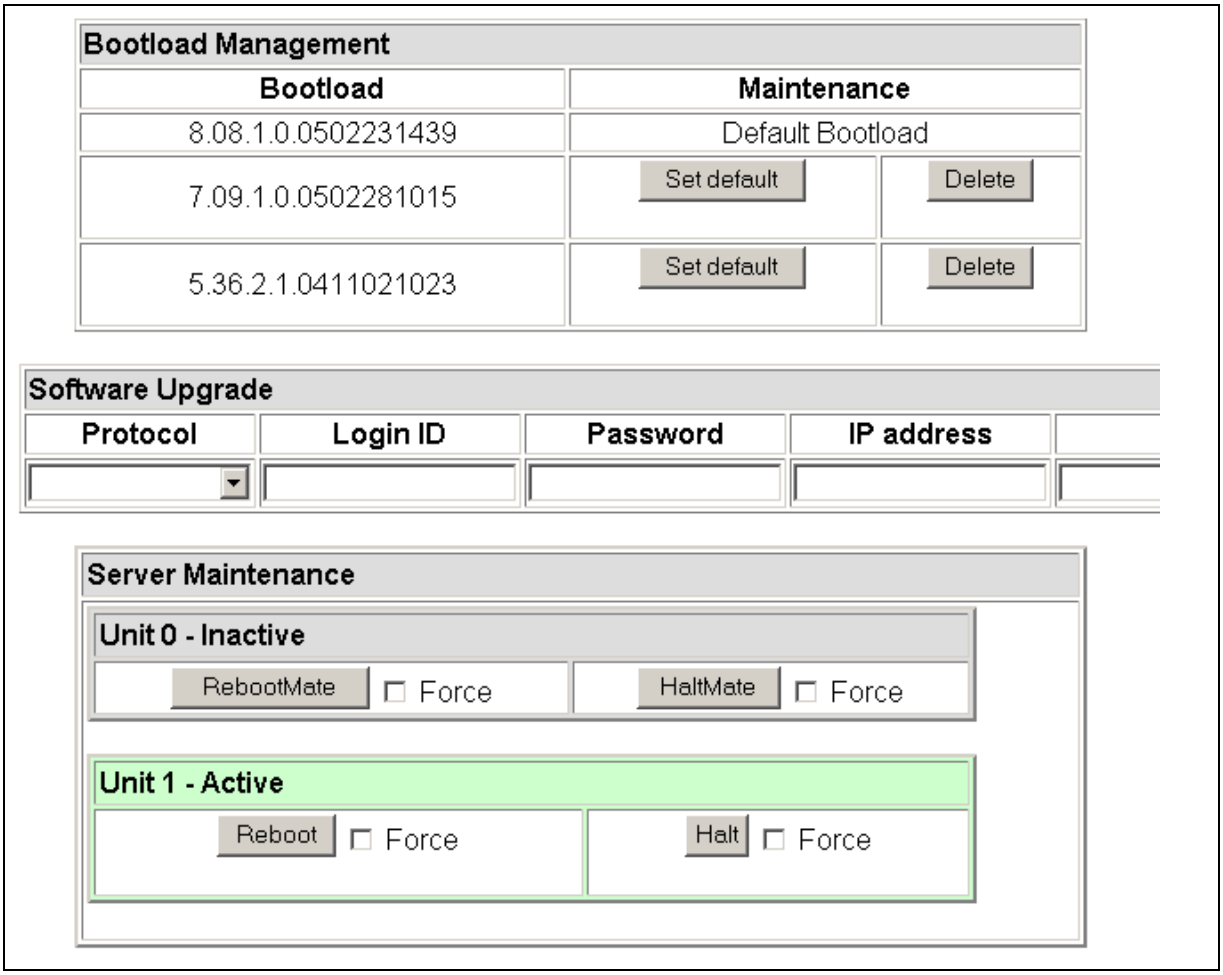
NTP Information					
Server 1	Server 2	Server 3	Total Number of Servers	Accessible Servers	Synchronized Servers
47.140.207.50 in sync	47.140.206.50 in sync	undefined	2	2	2

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

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

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

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



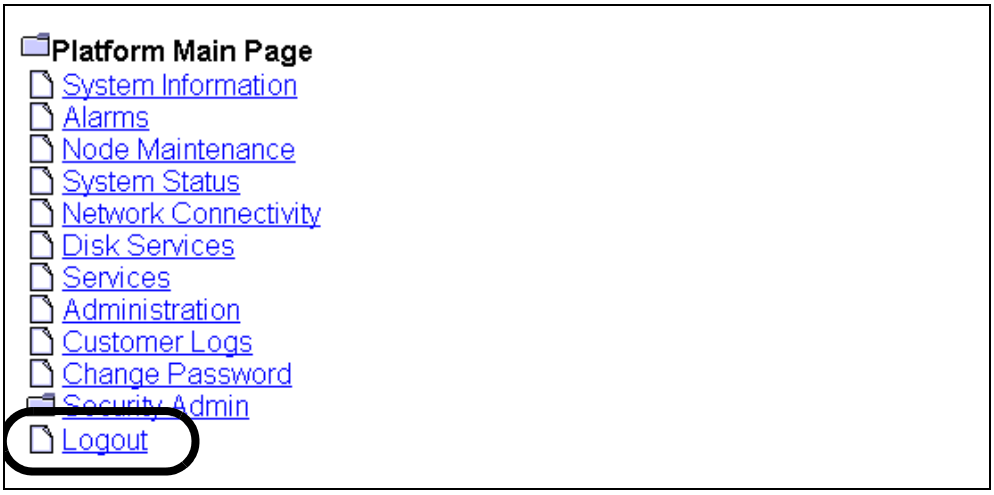
Field	Description
Bootload Management: Bootload	load ID for the NCGL platform software load
Bootload Management: Maintenance	indicates whether the Bootload is the default. Can also allow choosing a new default bootload if there is more than one load available. Additional loads can come from maintenance releases.
Software Upgrade: Protocol	file transfer protocol or source location for the platform software upgrade: FTP, Anonymous FTP, HTTP, HTTPS, Local File, Local 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.

Field	Description
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.
Server Maintenance (active and inactive units)	used to execute the Reboot, Halt, Rebootmate, and Haltmate functions. These are service affecting commands.

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

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

You are returned to the login page



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

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.

Limitations and restrictions

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

CAUTION
Service interruption
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.

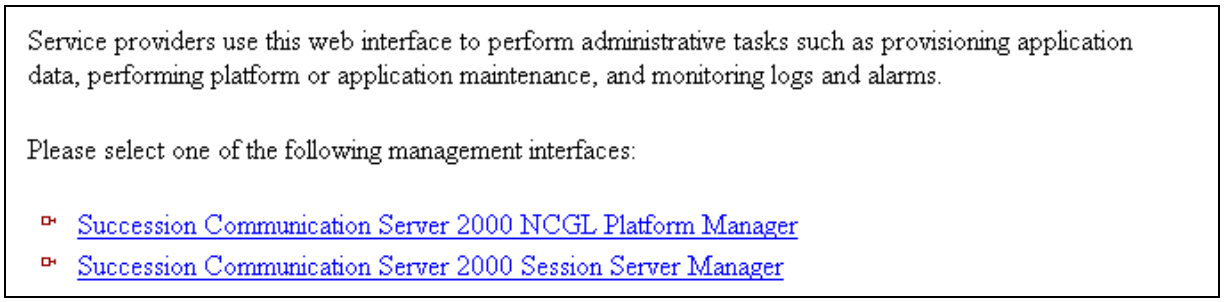
Prerequisites

There are no prerequisites for this procedure.

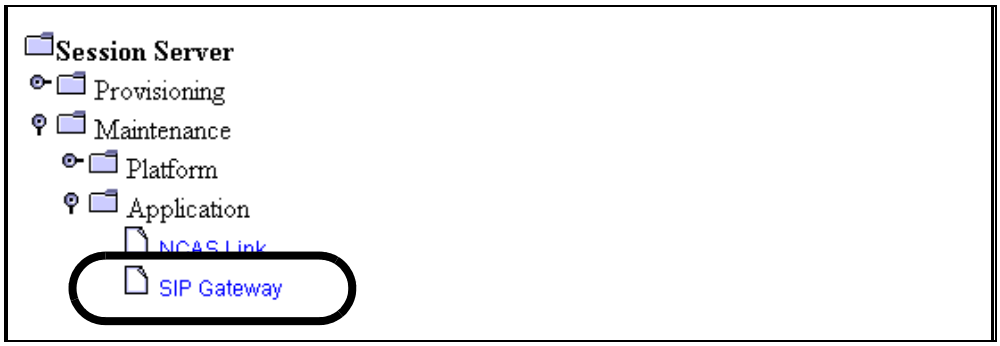
Action

At the CS 2000 Session Server Manager or IEMS client

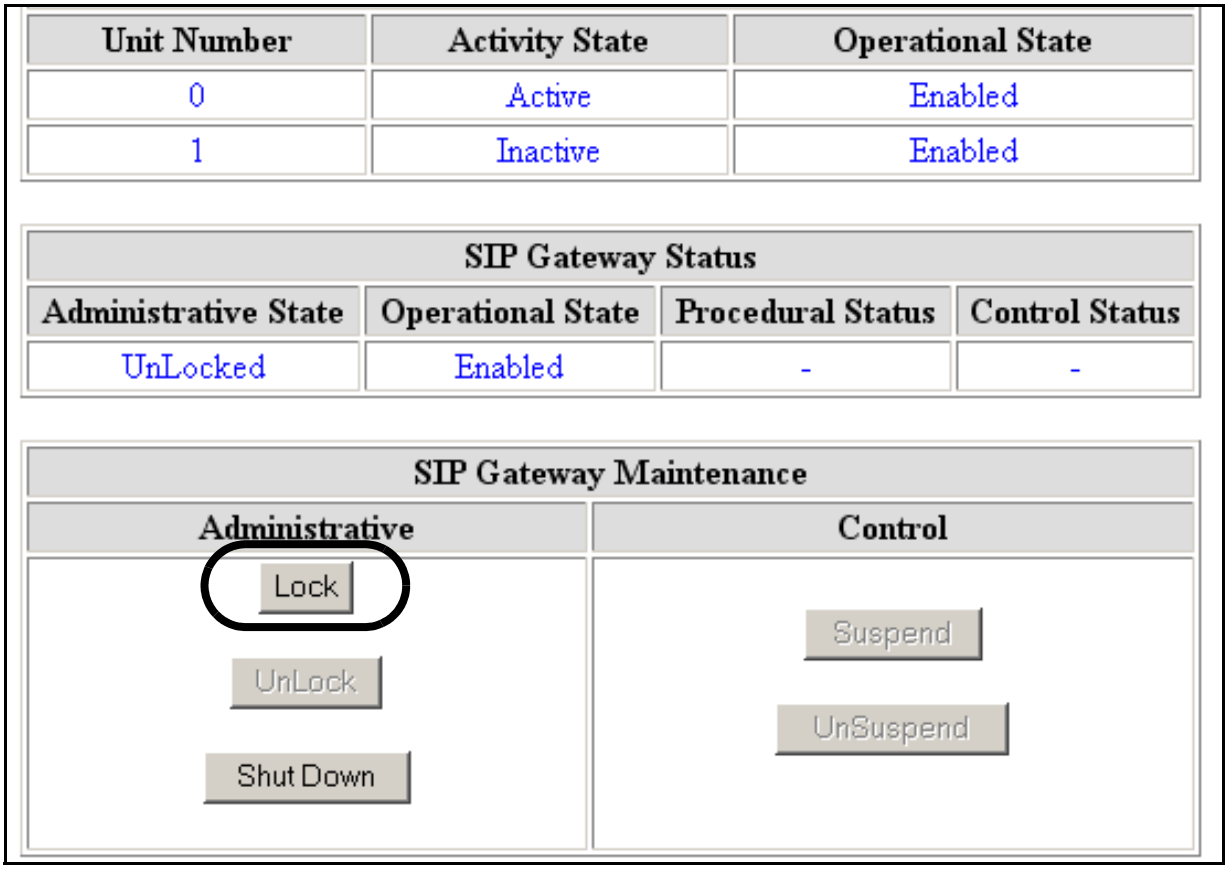
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.



2 Select Session Server > Maintenance > Application > SIP Gateway.



3 In the SIP Gateway panel click the Lock button.

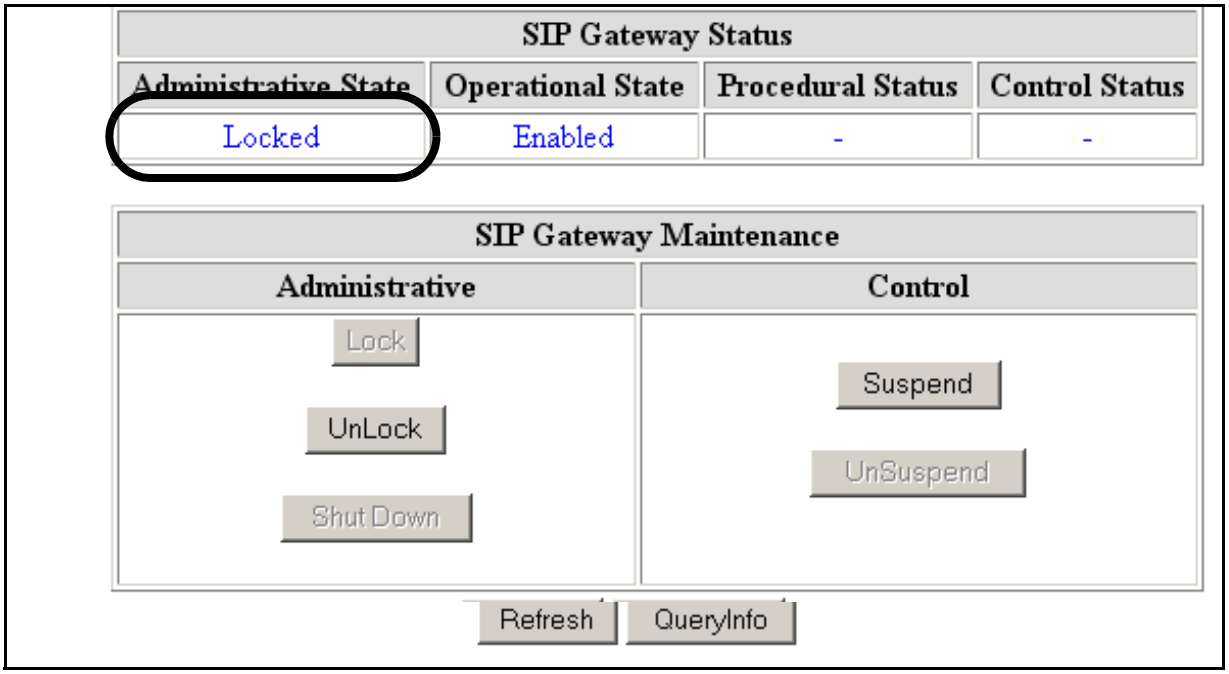


The system responds:

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

4 Click OK to confirm locking the SIP Gateway application.

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



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

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 call processing to begin.

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

Limitations and restrictions

This procedure provides instructions for changing the service status of the SIP Gateway application software only. For instructions on determining the status of the platform and operating system, refer to procedure View the operational status of the NCGL platform on page 99.

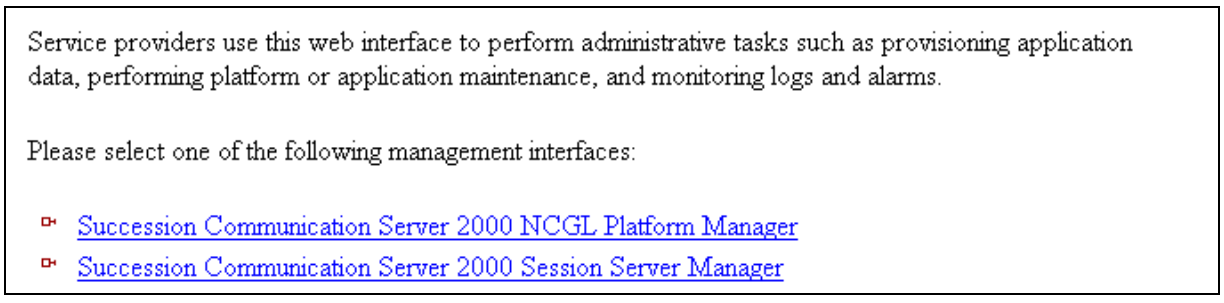
Prerequisites

The active unit must be in a locked Administrative state. If it is not locked or you are uncertain of the state of the application, refer to procedure Lock the SIP Gateway application on page 117.

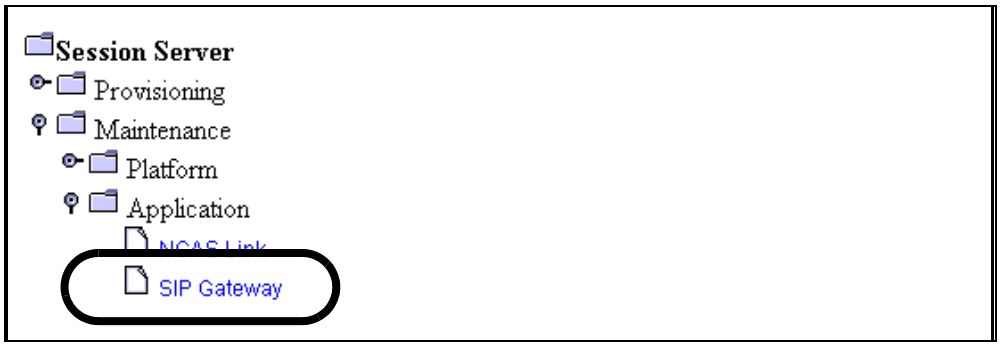
Action

At the CS 2000 Session Server Manager or IEMS client

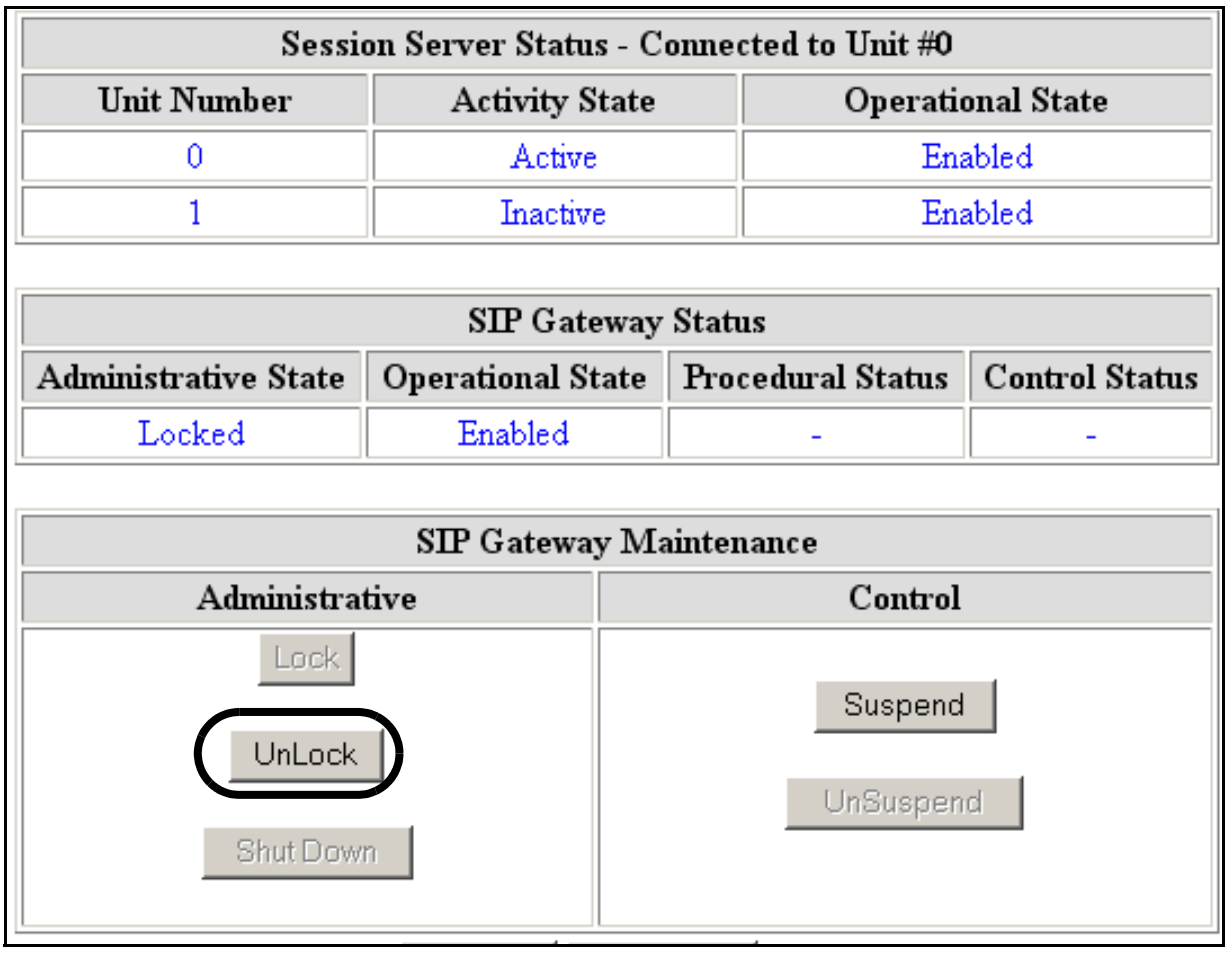
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.



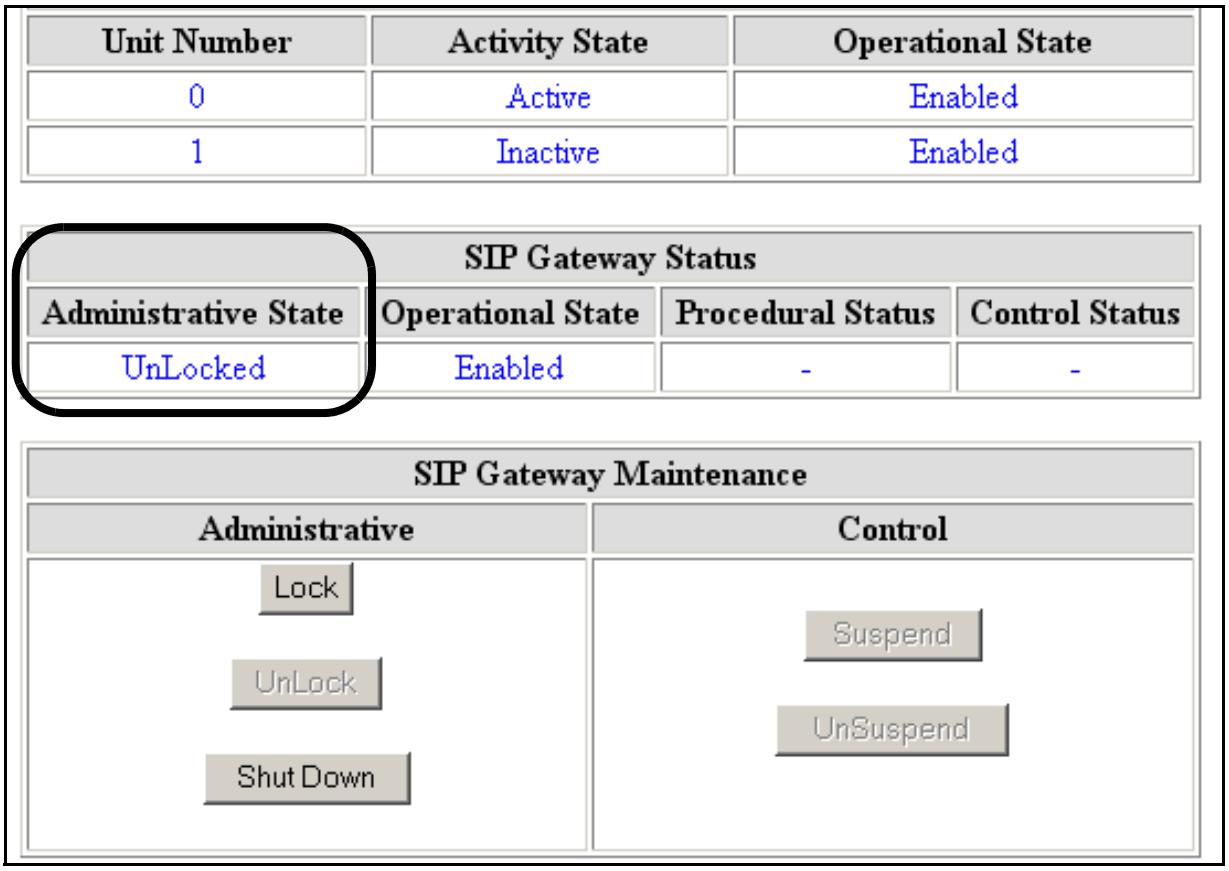
2 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu:



3 In the SIP Gateway panel click Unlock.



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



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

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

SIP Gateway Maintenance	
Administrative	Control
Lock UnLock Shut Down	Suspend UnSuspend

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.

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

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 “Interpreting SIP Gateway application states” in the *Session Server - Trunks Security and Administration*, NN10346-611.

Limitations and restrictions

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

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

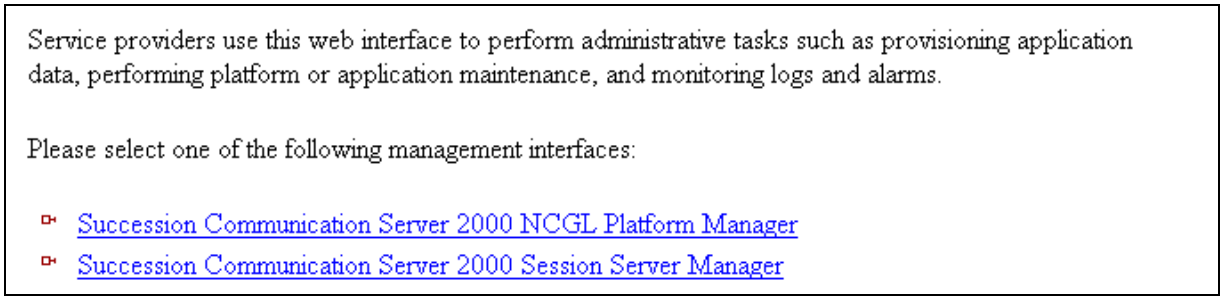
Prerequisites

The SIP Gateway application must previously have been locked. If it is not locked or you are uncertain of the state of the application, refer to procedure Lock the SIP Gateway application on page 117.

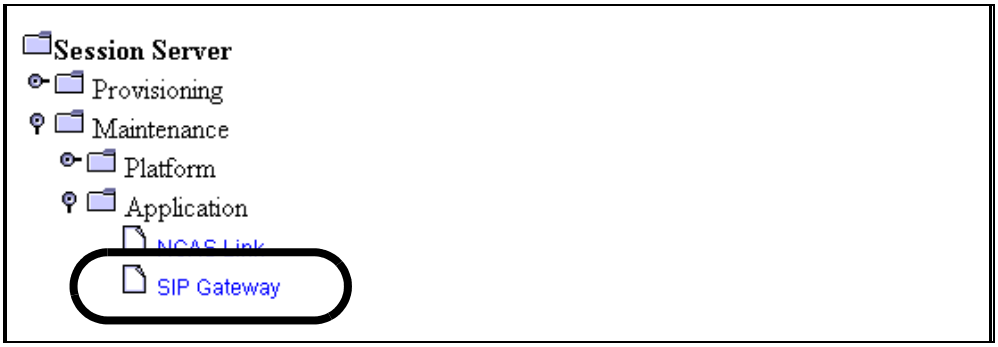
Action

At the CS 2000 Session Server Manager or IEMS client

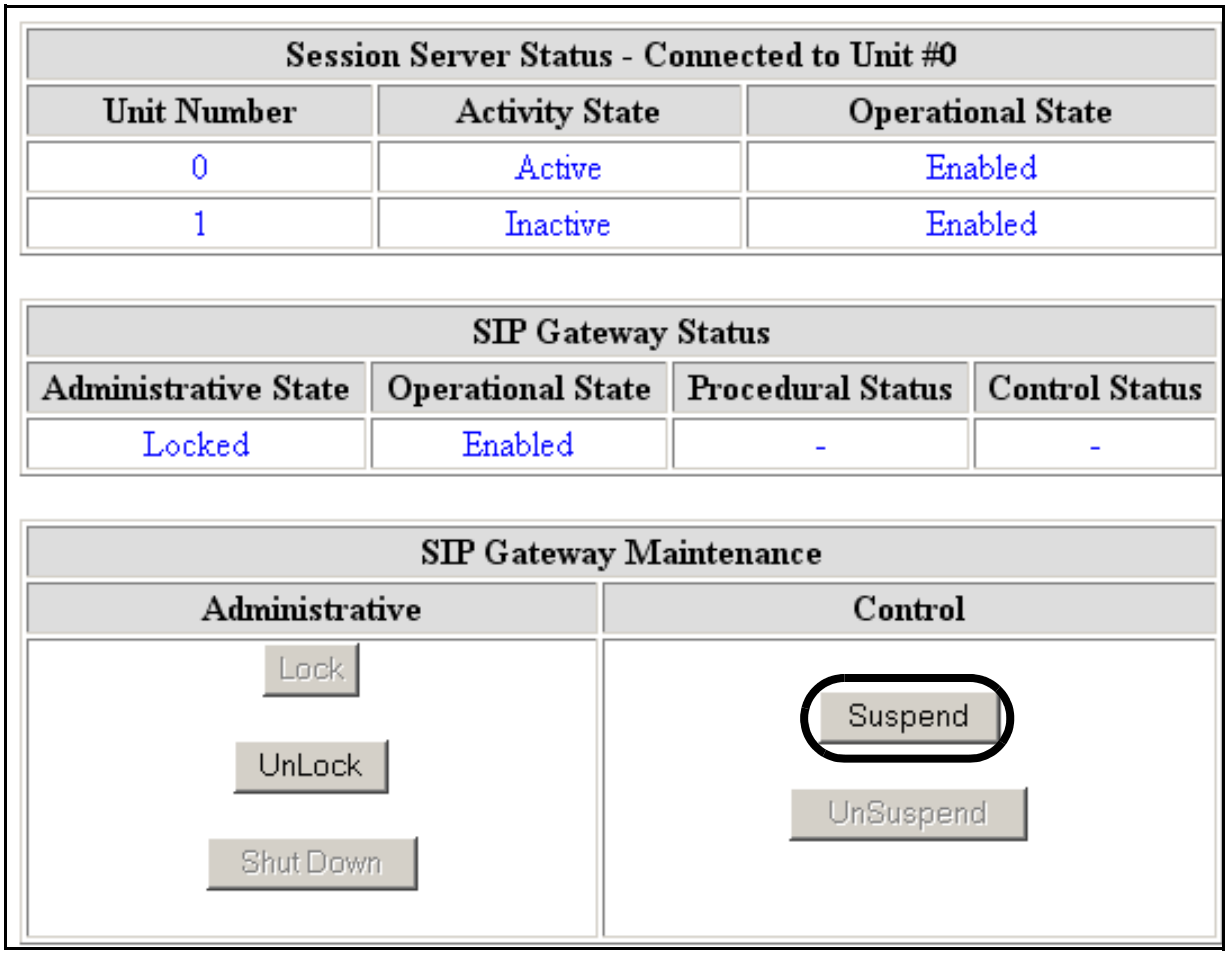
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.



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

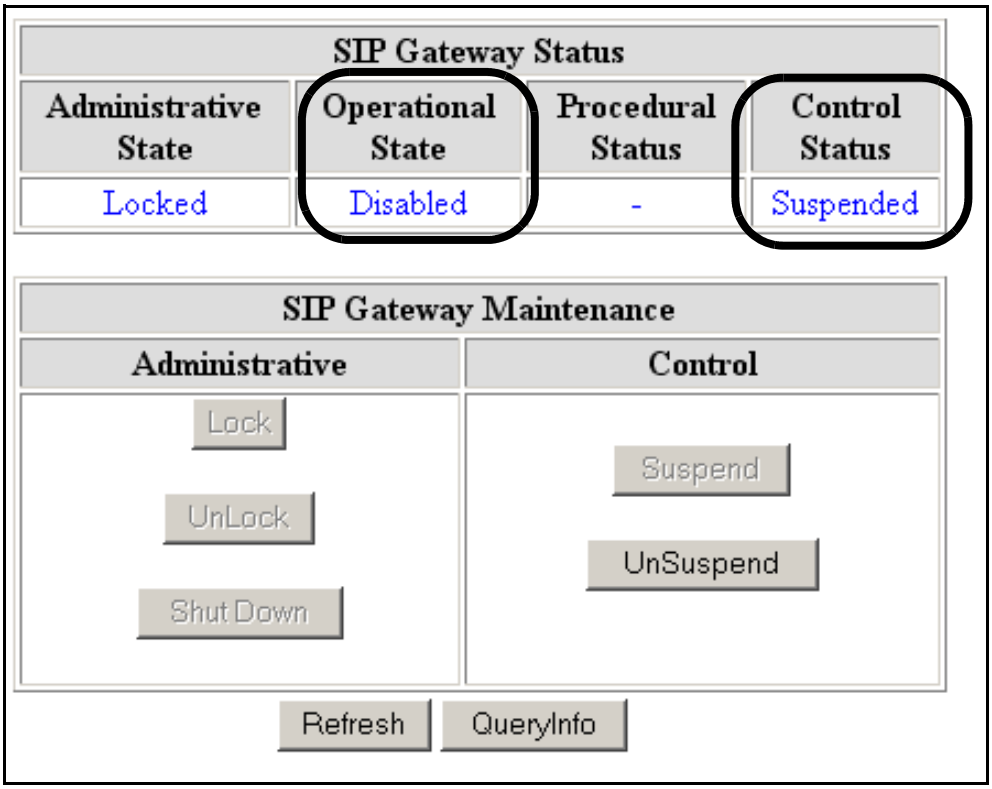


3 In the SIP Gateway panel click Suspend.



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

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



5 If applicable, restart the SIP Gateway application by executing procedures Unsuspend the SIP Gateway application on page 128 and Unlock the SIP Gateway application on page 121, in the order shown.

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

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 *Session Server - Trunks Security and Administration*, NN10346-611.

Limitations and restrictions

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

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

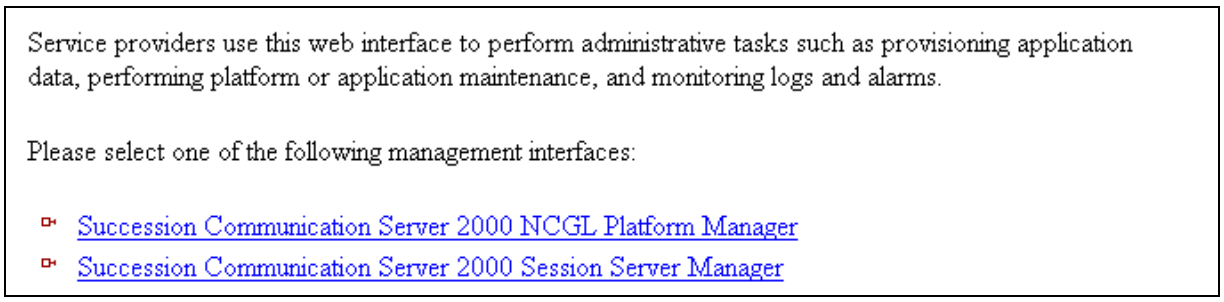
Prerequisites

The SIP Gateway application must previously have been suspended. If it is not suspended or you are uncertain of the state of the application, refer to procedure Suspend the SIP Gateway application on page 124.

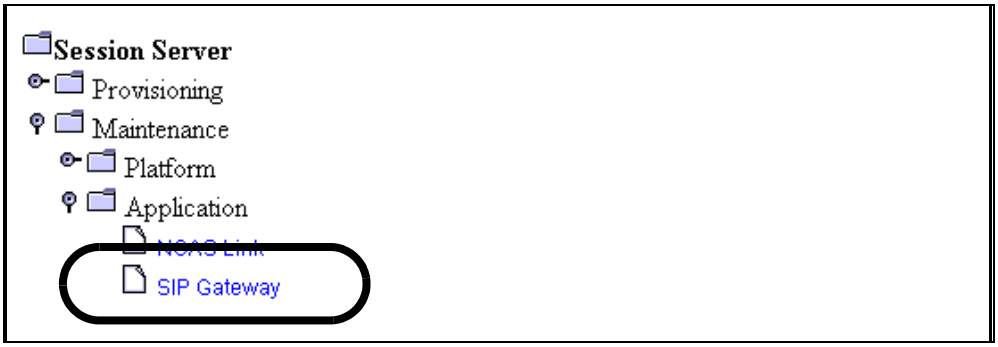
Action

At the CS 2000 Session Server Manager or IEMS client

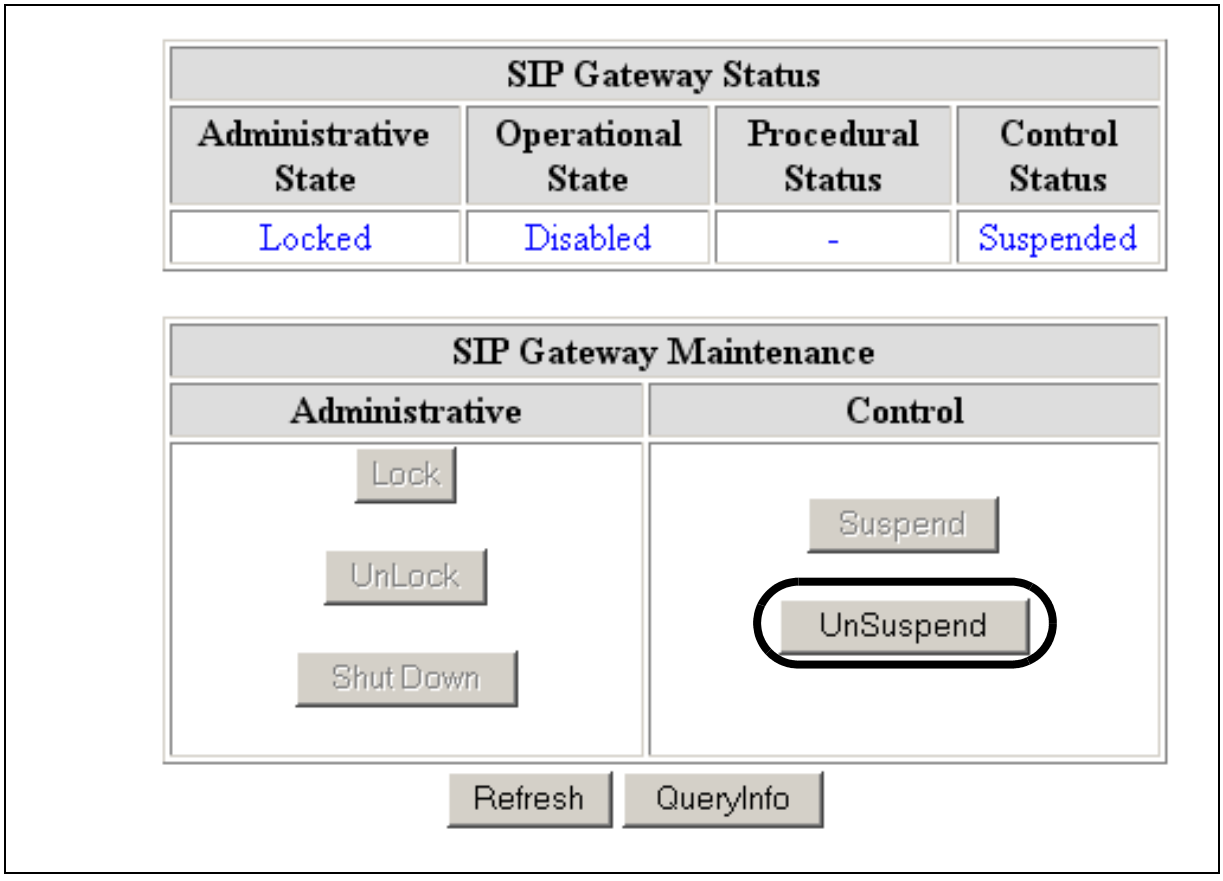
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.



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

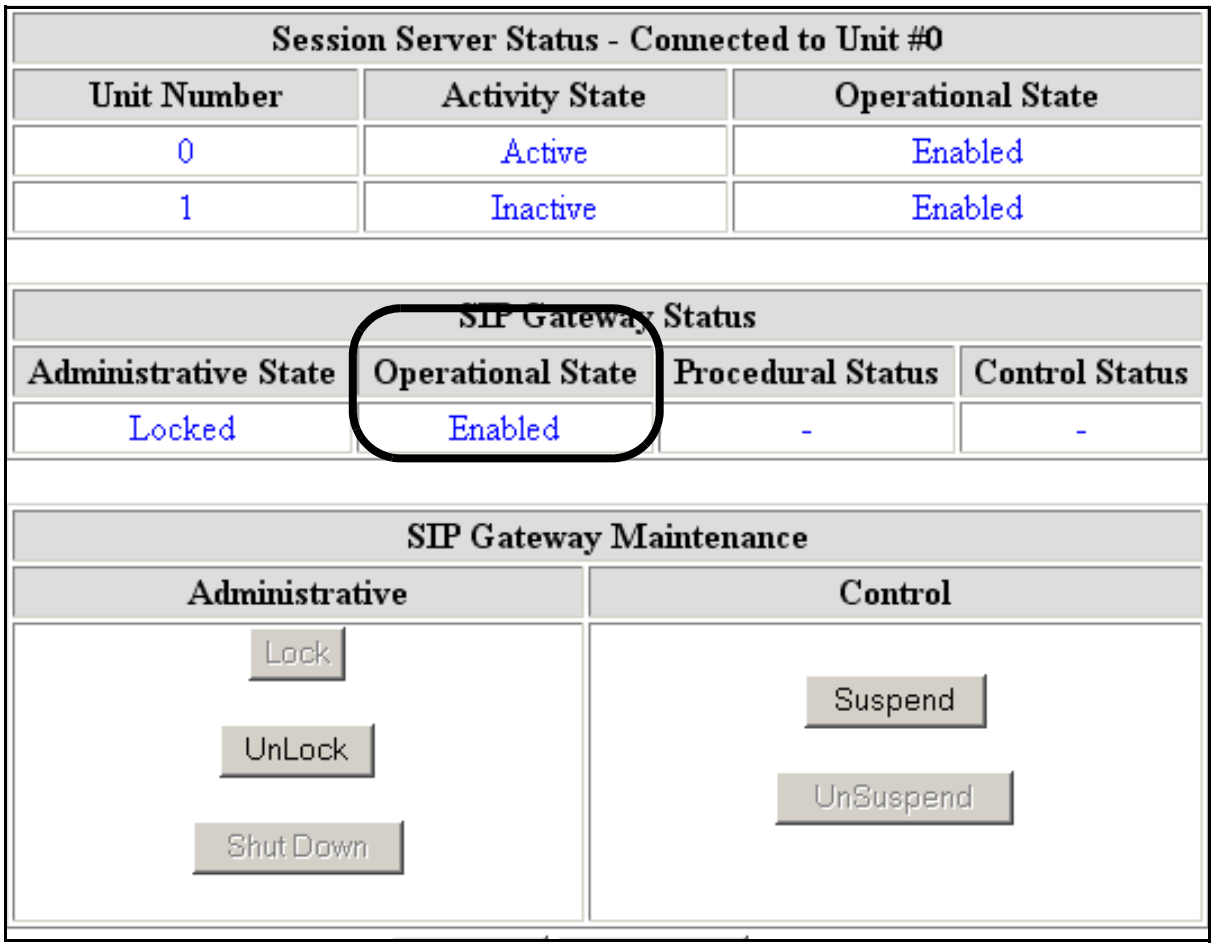


3 In the SIP Gateway panel click Unsuspend.



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

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



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 If necessary, bring the SIP Gateway application back into service by executing procedure Unlock the SIP Gateway application on page 121.

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

Session Server - Trunks backup

By default, the unit performs a backup of the database and critical files every day at 1:00 AM. Refer to Rescheduling backup time on page 133 to alter the schedule.

The contents of the backup are stored locally on each unit in the `/data/bkresmgr/backup` directory in tape archive (tar) format.

Security related files are not automatically backed up. Refer to Manual backup of security related files on page 135.

Purpose of this procedure

Use this procedure to make a manual backup or change the backup time.

Limitations and Restrictions

ATTENTION
SIP Gateway application provisioning activities must be suspended during the time of the database backup in order to ensure that an accurate and complete copy of the active unit database is created. However, call processing is not affected and there is no enforcement in the database to prevent provisioning.

Security related files must be backed up manually.

Prerequisites

ATTENTION
The SIP Gateway application database must be in sync with the CS 2000 to ensure an accurate copy of the active unit database is created. Verify this condition using procedure Verify synchronization status on page 90.

Making a backup

Follow this procedure to make an immediate backup.

At the NCGL CLI or Integrated EMS client

1 Log on to the **ACTIVE** unit and change to the root user.

2 Execute the command to make the backup by typing

`/opt/apps/db_install/sd/bkup_ngss.sh`

and pressing the Enter key.

The following output is printed to the screen and the backup is recorded to /data/bckresmgr/backup.

bkup_ngss.sh response

```
-------------------------------------------------------
- Move files
-------------------------------------------------------
-------------------------------------------------------
- Backup Solid database -
-------------------------------------------------------
-------------------------------------------------------
- Copy certificate files to backup directory -
-------------------------------------------------------
-------------------------------------------------------
- Copy commish files to backup directory -
-------------------------------------------------------
-------------------------------------------------
- Copy web files to backup directory -
-------------------------------------------------
-------------------------------------------------
- Creating Meta-Data File Listing -
-------------------------------------------------
-------------------------------------------------
- Waiting for Solid DB to complete backup -
-------------------------------------------------
-------------------------------------------------
- Waiting for Solid DB to complete backup -
-------------------------------------------------
-------------------------------------------------
- Solid DB backup complete -
-------------------------------------------------
tar: Removing leading `/' from absolute path names in the archive
data/bkresmgr/temp/
```

The backup pauses at this point while the database is backed up.

bkup_ngss.sh response

```
data/bkresmgr/temp/hosts
data/bkresmgr/temp/ntp.conf
data/bkresmgr/temp/ifcfg-eth0
data/bkresmgr/temp/netnodes
data/bkresmgr/temp/group
data/bkresmgr/temp/passwd
data/bkresmgr/temp/shadow
data/bkresmgr/temp/ssh_host_dsa_key.pub
data/bkresmgr/temp/ssh_host_key.pub
data/bkresmgr/temp/ssh_host_rsa_key.pub
data/bkresmgr/temp/server.xml
data/bkresmgr/temp/redirect.jsp
data/bkresmgr/temp/redirect_SSPFS.jsp
data/bkresmgr/temp/redirect_no-SSPFS.jsp
data/bkresmgr/temp/redirect_apps.php
data/bkresmgr/temp/META-DATA.txt
data/bkresmgr/temp/hostname.txt
data/bkresmgr/temp/solid.db
data/bkresmgr/temp/solid.ini
data/bkresmgr/temp/solmsg.out
$
```

The backup filename is located in /data/bkresmgr/backup and is identifed by hostname, date, and time as indicated in the following example:

Example
unit0.backupfile.2005-04-12_17-10.tgz

3 For security purposes, ensure that a copy of the backup file is transferred to a secure location.

Use the **scp** command to make a secure copy of the backup file to a secure, remote server on your network. This server should be continuously available for cases where a restoration of the unit become necessary, such as during an upgrade rollback.

4 If security related files should be backed up, refer to Manual backup of security related files on page 135.

5 You have completed this procedure. Repeat this procedure on the second unit.

Rescheduling backup time

Each unit performs an automatic backup at 1:00 AM daily. Use the following procedure to change the schedule.

At the NCGL CLI or Integrated EMS client

1 Log onto the unit and change to the root user.

2 Remove the existing backup schedule from the crontab by typing

`/opt/apps/db_install/sd/uninstallBkres.sh`

3 Edit the backup schedule file by typing

`vi /opt/apps/db_install/sd/backup.cron`

The file is opened for editting.

```
# Cron data file for NGSS Backup timings
0 1 * * *        /opt/apps/db_install/sd/bkup_ngss.sh
```

4 Modify the first five fields (indicated by "0 1 * * *" in the example). The fields are identifed in order from left to right:

- minute — the minute of the hour that the command will run, values are 0 to 59
- hour — the hour of the day the command will run, values are 0 to 23 with 0 being midnight
- day — the day of the month the command will run, values are 1 to 31, an asterisk indicates to run the command all days
- month — the month of the year the command will run, values are 0 to 12, an asterisk indicates to run the command all months
- weekday — the day of the week that the command will run, values are 0 to 6, with 0 being Sunday, an asterisk indicates to run the command all weekdays

Do not modify the sixth field (/opt/.../bkup_ngss.sh).

When done, write and quit the file.

5 Install the newly created schedule in the crontab by typing

`/opt/apps/db_install/sd/installBkres.sh`

6 After the scheduled time, verify that a backupfile is created in the `/data/bkresmgr/backup` directory and that it is created at the new time, not the previously scheduled time.

7 This procedure is complete. Repeat this procedure on the second unit.

Manual backup of security related files

The automatic backup does not backup the certificate.keystore or key files. This guards against loss or theft of the backup which would compromise the key without the operating company personnel knowing about the breach.

Copy the following files to a safe location:

- /opt/base/share/ssl/certificate.keystore
- /opt/base/share/ssl/gen_cert.txt
- /opt/base/share/ssl/server.crt
- /opt/base/share/ssl/server.key
- /opt/base/share/ssl/trusted.crt
- /opt/base/synch_local/common/etc/ssh/ssh_host_dsa_key
- /opt/base/synch_local/common/etc/ssh/ssh_host_key
- /opt/base/synch_local/common/etc/ssh/ssh_host_rsa_key

The following procedure provides a suggestion of how to backup these security related files.

At the NCGL CLI or Integrated EMS client

1 Log in to either unit (usually the unit where the latest version of security certificates are stored), and change to root user.

2 Change directories to the /opt/base/share/ssl directory:

```
cd /opt/base/share/ssl
```

3 Create a new directory to store backup copies of the certificate files:

```
mkdir <SNxx_ddmmyyyy>
```

where

SNxx_ddmmyyyy
is the name of the new directory based on the currently installed release of the system software (for example SN08) and the current date in the format ddmmyyyy

4 Copy the certificates to the newly created backup directory:

```
cp * <SNxx_ddmmyyyy>
```

ATTENTION

Completing this step ensures that you have valid backup copies of the security certificates for restoring in case of an upgrade abort or rollback or for disaster recovery purposes.

5 Use the following table to determine your next step:

If	Do
you want to make backup copies of the security certificates to a remote server	Ensure that the remote host that will store the security related files is secure, that the host is unavailable to general users, and offers restricted access to personnel with security related responsibilities. Proceed to step 6
you do not want to make backup copies of the security certificates to a remote server	This procedure is complete.

6 Secure copy the files to the remote server:

```
cd <SNxx_ddmmyyyy>
scp * <user>@<remote_server>:</path>
```

where

user
is a valid user ID on the remote server

remote_server
is the IP address of the remote server

/path
is where the file will be located on the remote server

The files are copied to the remote server.

7 You have completed this procedure.

Power-Off a Session Server unit

Purpose of this procedure

This is used to power off a Session Server unit.

This procedure may be used as a standalone task or as part of a higher level activity such as a part of a controlled shutdown activity or part of a software upgrade activity.

Limitations and restrictions

CAUTION

This is a service affecting procedure. Powering off a Session Server unit prevents the node from operating in a fault-tolerant manner. Ensure that the unit you are powering off is not the active unit. Failure to do so may result in loss of call processing.

Prerequisites

Refer to procedureView the operational status of the NCGL platform on page 99 to verify that the unit to be shut down is not active.

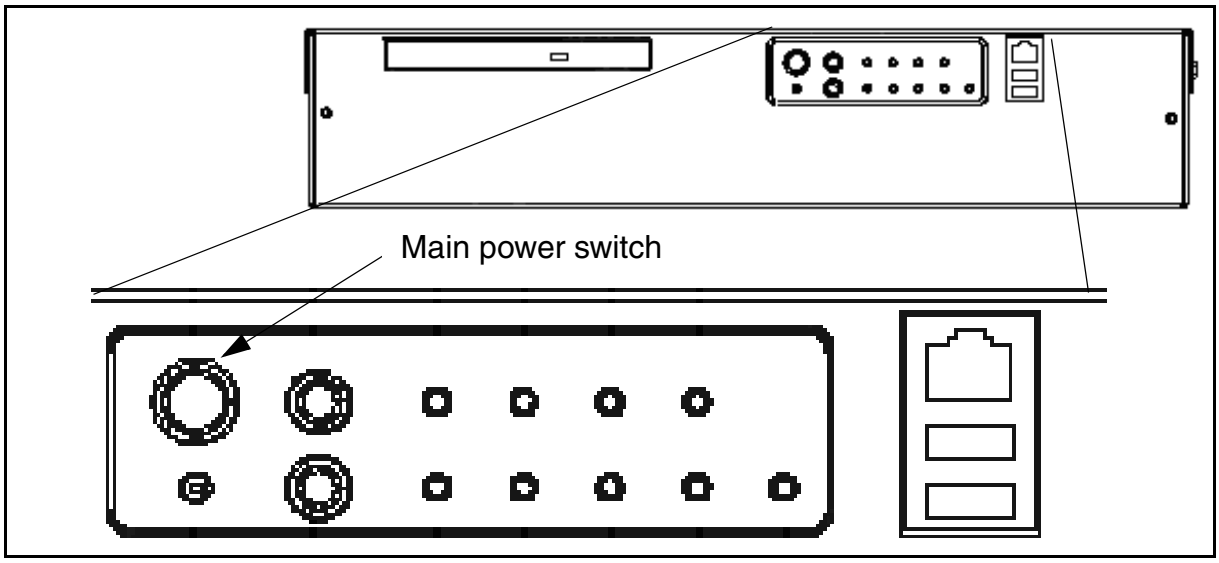
Refer to the Session Server Fault Management NTP, NN10332-911, for information about the high-level activity *Perform a controlled shutdown of a Session Server node*.

Action

At the front panel of the Session Server unit.

1 Complete procedure Halt (shutdown) a Session Server unit before powering off the unit.

2 Once the operating system has been halted, disconnect the power to the unit using the main power switch located on the front panel.



3 The procedure is complete.

Power-On and boot a Session Server unit

Purpose of this procedure

This procedure is used to power on a Session Server unit that has been installed as a replacement, or was shutdown for any other reason.

This procedure may be used as a standalone task or as part of a higher level activity such as part of a dead office recovery activity or software upgrade activity.

Limitations and restrictions

There are no restrictions on using this procedure.

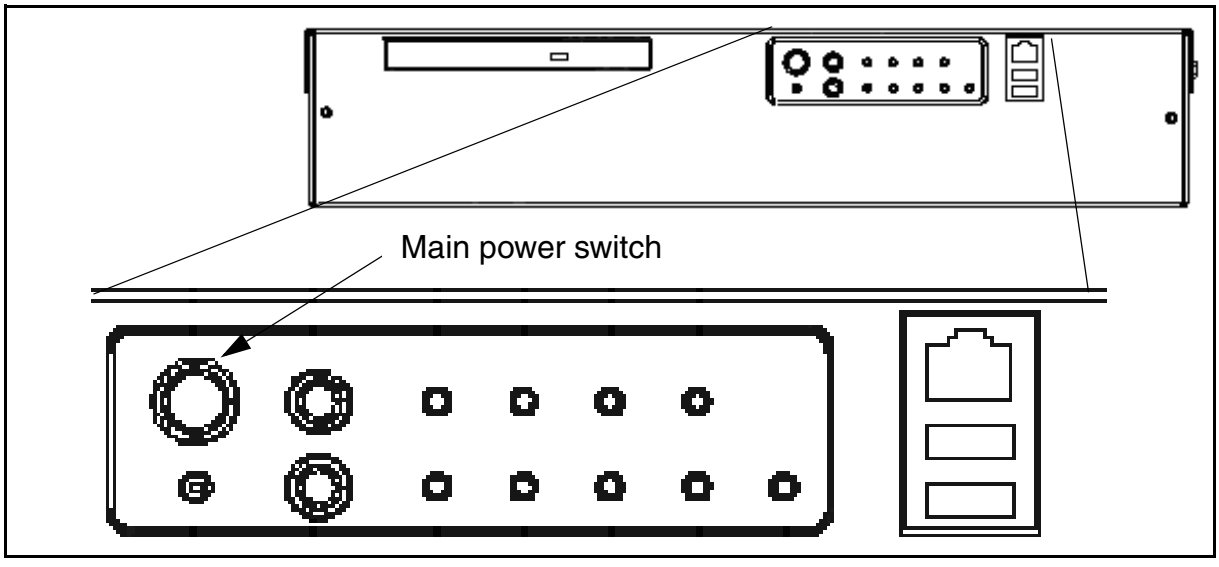
Prerequisites

If the unit was a replacement unit recently installed, ensure that all power cabling connections have been properly installed and secured at the rear of the chassis and SAM-F frame.

Action

At the front panel of the Session Server unit

1 If necessary, power on the Session Server using the main power switch located on the front panel.



2 If desired, at the Session Server console, monitor the boot progress of the unit.

3 The procedure is complete.

Back up security certificates

Purpose of this procedure

Use the following procedure to create backup copies of security certificates to a folder on the unit and make copies to a remote server location, chosen by the customer.

Use this procedure anytime new security certificates are created or when the system is changed from using self-signed certificates to CA-signed certificates. This procedure is also used as part of a major release upgrade activity.

Limitations and Restrictions

There are no limitations on performing this procedure.

Prerequisites

There are no prerequisites for this procedure.

Action

Perform the following steps to complete this procedure.

At the NCGL CLI or Integrated EMS client

1. Log onto either unit (usually the unit where the latest version of security certificates are stored), and change to root user.
2. Change directories to the /opt/base/share/ssl directory:

   ```
   cd /opt/base/share/ssl
   ```

3. Create a new directory to store backup copies of the certificate files:

   ```
   mkdir <SNxx_ddmmyyyy>
   ```

   where

   SNxx_ddmmyyyy
   is the name of the new directory based on the currently installed release of the system software (for example SN08) and the current date in the format ddmmyyyy

4 Copy the certificates to the newly created backup directory:

```
cp * <SNxx_ddmmyyyy>
```

ATTENTION

Completing this step ensures that you have valid backup copies of the security certificates for restoring in case of an upgrade abort or rollback or for disaster recovery purposes.

5 Use the following table to determine your next step:

If	Do
you want to make backup copies of the security certificates to a remote server	Ensure that the remote host that will store the security related files is secure, that the host is unavailable to general users, and offers restricted access to personnel with security related responsibilities. Proceed to step 6
you do not want to make backup copies of the security certificates to a remote server	This procedure is complete.

6 Secure copy the files to the remote server:

```
cd <SNxx_ddmmyyyy>
scp * <user>@<remote_server>:</path>
```

where

user
is a valid user ID on the remote server

remote_server
is the IP address of the remote server

/path
is where the file will be located on the remote server

The files are copied to the remote server.

7 You have completed this procedure.

Generate self-signed security certificates

Purpose of this procedure

This procedure uses the certificate management tool to generate self-signed security certificates used for both units. Use this procedure only as part of a high-level task for updating security certificates.

A successful completion of this procedure creates a self-signed certificate composed of the following files:

- server.crt - contains the local certificate
- server.key -contains the private key corresponding to the local certificate
- trusted.crt - is an empty file if it did not already exist before the certificate management tool was run
- certificate.keystore - contains the private key and local certificate

Limitations and restrictions

You must be a root user to use the certificate management tool.

ATTENTION

The certificate management tool sets the appropriate file permissions for when the certificate files are generated. Do not change these file permissions.

If the permissions are modified, the private key can be compromised. A compromise of the private key forces a re-issuing of the certificate with a new private key and re-datafilling the certificate as necessary on peer remote SIP servers.

Prerequisites

Please read the complete disclaimer, found in section Self-signed certificate security disclaimer on page 151.

Action

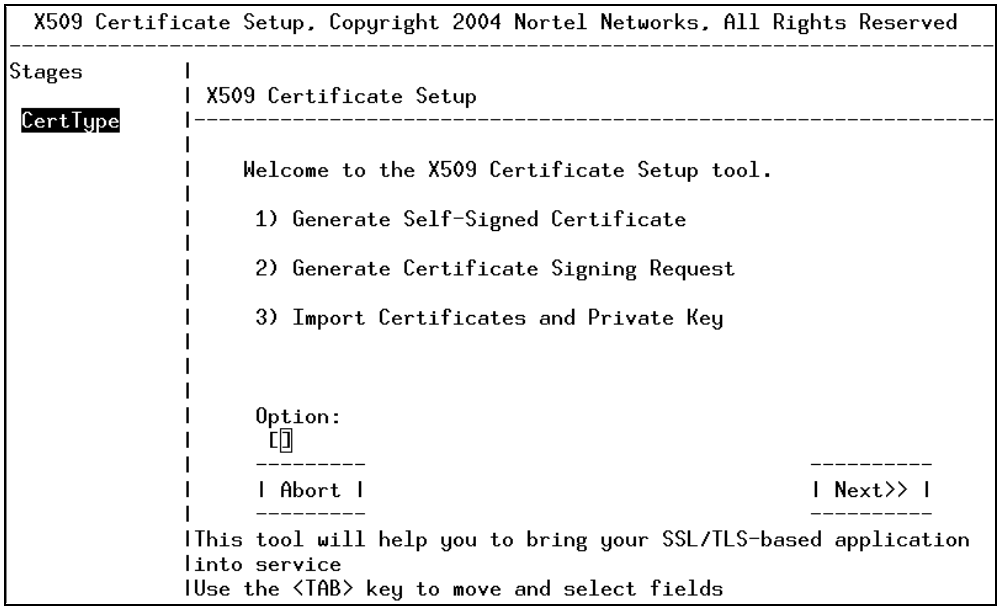
At the NCGL CLI or IEMS client

1 Log on to the standby unit and change to the root user.

2 Start the certificate management tool by typing

`/sbin/cert_mgnt`

After a few seconds the Introduction screen is displayed.



3 Type 1 for the option to generate a self-signed certificate type, position the cursor on the Next button and press Enter.

Note: In general, use the Tab key or the < and > keys to navigate between fields on the screen and use Enter to select a field or entry.

A security disclaimer screen appears.

```
  X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Stages          |
                | X509 Certificate Setup
 CertType       |-------------------------------------------------------------
                |
                |
                |
                |     PLEASE REVIEW THE FOLLOWING TERMS AND CONDITIONS
                |     REQUIRED FOR THE USE OF DIGITAL SELF-SIGNED
                |     CERTIFICATES.  MOVE BETWEEN PAGES BY USING THE 'C'
                |     AND 'B' KEYS.  IF YOU DO NOT ACCEPT THE TERMS AND
                |     CONDITIONS BELOW, YOU ARE NOT AUTHORIZED TO USE A
                |     DIGITAL SELF-SIGNED CERTIFICATE.
                |
                |     BY PRESSING 'Y' BELOW, YOU AGREE TO BE BOUND BY THE
                |     TERMS AND CONDITIONS BELOW
                |
                |
                |
                |Type (c) to continue
                |
                |
```

4 Carefully read the series of screens displaying the terms and conditions of the security certificate tool. Press c to continue to the next disclaimer page or press b to go back to the previous disclaimer page.

5 At the final disclaimer page, accept the terms and conditions of the security certificate tool by pressing y.

Otherwise you can reject the terms and conditions of the security disclaimer by pressing n. You are returned to the main menu.

The RSA modulus size screen appears.

```
  X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Stages          |
                | Configure RSA modulus size
 CertType       |-------------------------------------------------------------
 RSAModulus     |
 ExpiryDays     |    Please enter a RSA modulus size
 CountryName    |
 State          |     [ ]
 LocalityName   |
 OrgName        |
 OrgUnit        |
 CommonName     |
```

6 Enter the RSA modulus (key) size, position the cursor on the Next button and press Enter. Supported values are 1024, 1536 or 2048 bits. (1024 is recommended)

Note: The larger the key size, the stronger the private key. There can be a performance impact when using larger key sizes.

7 Use the following table to determine your next step:

If	Do
you receive the message that the RSA private key already exists and you do not want to reuse the key	step 8
you receive the message that the RSA private key already exists and you want to reuse the key	Press y and go to step 12
you do not receive any message that an RSA private key already exists	step 12

8 If you do not want to reuse the key, press n.

The system prompts that the RSA key is about to be deleted.

9 Use the following table to determine your next step:

If	Do
you do not want to delete the existing RSA key	Press n to abort the delete operation and go to step 10.
you are sure you want to proceed with deleting the existing RSA private key	Go to step 11.

10 Press any key and return to step 6.

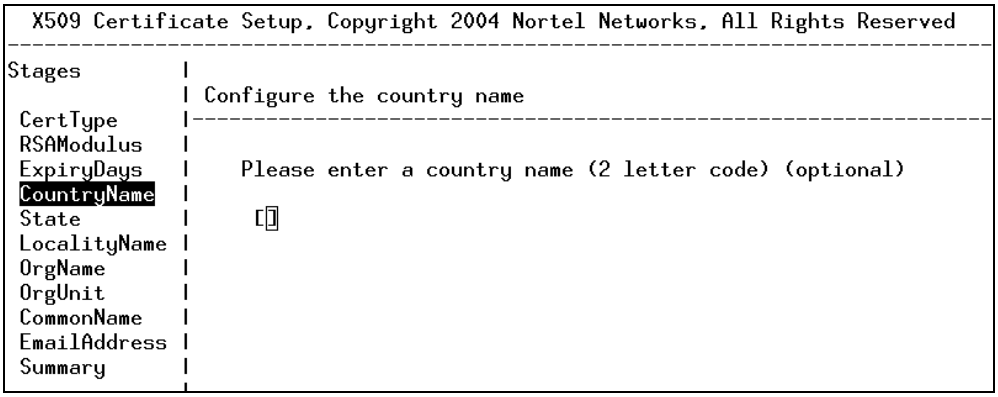
11 If you want to delete the existing RSA key, press y.

A backup of the existing key is made to a file in the same directory and a customer log is generated. The expiration configuration screen appears.

```
  X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Stages          |
                | Configure the certificate expiry days
 CertType       |----------------------------------------------------------------
 RSAModulus     |
 ExpiryDays     |    Please enter a expiry days value
 CountryName    |
 State          |     [ ]
 LocalityName   |
```

12 At the certificate expiry days screen, enter the number of days you want the certificate to be valid, position the cursor on the Next button and press Enter. Supported expiration values range from 30 (30 days from the date of creation) to 7300 (20 years from the date of creation).

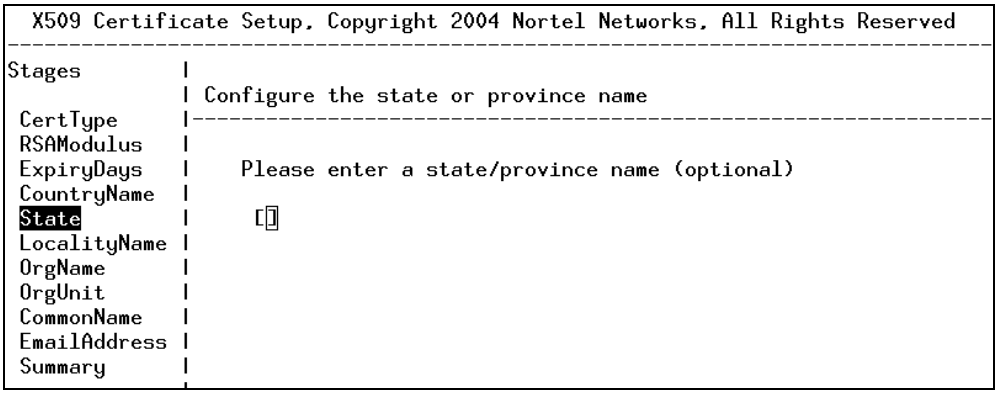
The country name configuration screen appears.



13 If applicable, enter the optional ISO 3166-1-alpha-2 two-letter country code, position the cursor on the Next button and press Enter.

Note: This entry helps identify the node to a remote entity.

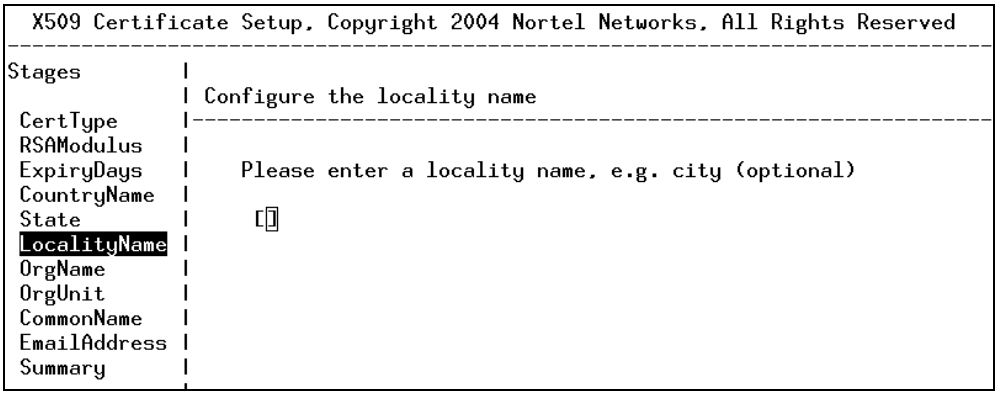
The state/province configuration screen appears.



14 If applicable, enter the optional state or province name, position the cursor on the Next button and press Enter.

Note: This entry helps identify the node to a remote entity.

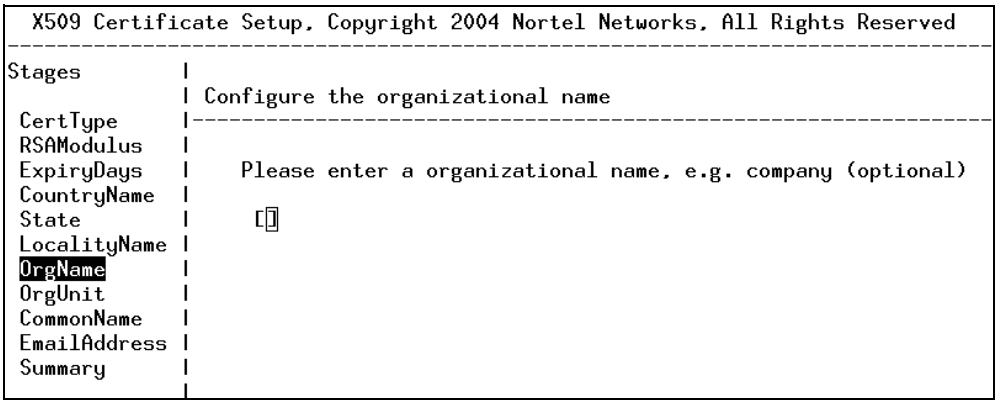
The locality configuration screen appears.



15 If applicable, enter the optional name of the locality or city, position the cursor on the Next button and press Enter.

Note: This entry helps identify the node to a remote entity.

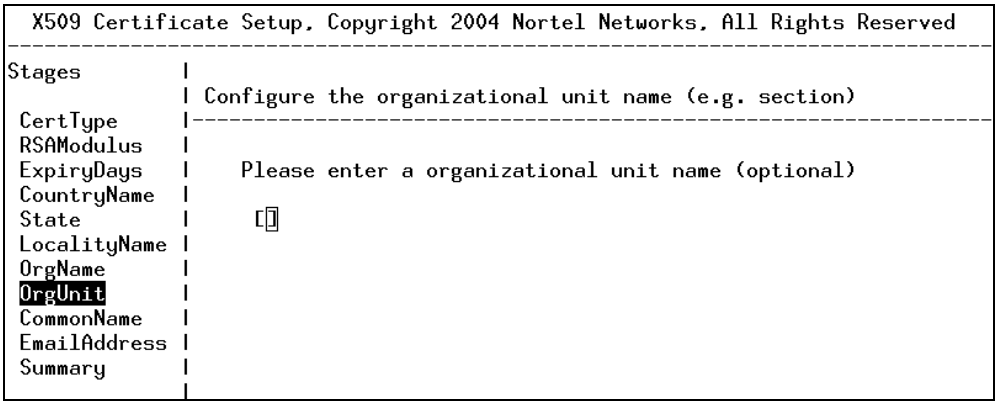
The organizational configuration screen appears.



16 If applicable, enter the optional name of the organization, position the cursor on the Next button and press Enter.

Note: This entry helps identify the node to a remote entity.

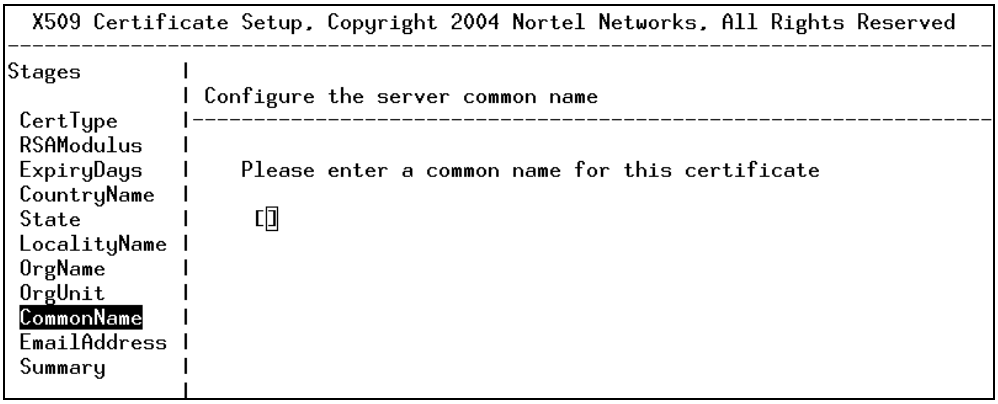
The organizational unit configuration screen appears.



17 If applicable, enter the optional name of the organizational unit, position the cursor on the Next button and press Enter.

Note: This entry helps identify the node to a remote entity.

The server common name configuration screen appears.



18 Enter a common name for the Session Server - Trunks node to which this certificate applies using one of the following methods:

- use the active IP address for the node in the format: xxx.xxx.xxx.xxx
- use a hostname of up to 64 alphanumeric characters, with hyphens, underscores and periods allowed. The hostname used must be in FQDN (fully-qualified domain name) format. If you chose to use a host name, this same hostname must also be used as in the mgcHostName field when datafilling the SIP Gateway application configuration parameters. To datafill the mgcHostName, refer to procedure "Configure SIP Gateway application parameters" in *Session Server - Trunks Configuration Management*, NN10338-511.

Note: The common name value is used for mutual authentication between the node and the remote application server. There is no validation of the common name at this stage of the configuration operation.

19 Position the cursor on the Next button and press Enter.

An email configuration screen appears.

```
  X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Stages          |
                | Configure an email address
 CertType       |----------------------------------------------------------------
 RSAModulus     |
 ExpiryDays     |    Please enter an email address (optional)
 CountryName    |
 State          |     [ ]
 LocalityName   |
 OrgName        |
 OrgUnit        |
 CommonName     |
 EmailAddress   |
 Summary        |
                |
```

20 If applicable, enter the optional email address of the organization, position the cursor on the Next button and press Enter.

Note: This entry helps identify the node to a remote entity. There is no validation of the email address.

A certificate summary information screen appears.

```
  X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Stages          |
                | Confirm the certificate information
 CertType       |----------------------------------------------------------------
 RSAModulus     |
 ExpiryDays     |    Select 'Proceed' or 'Back' to make changes.
 CountryName    |
 State          |     Modulus Size:   1024
 LocalityName   |     Expiry Days:    7300
 OrgName        |     Country Name:   CA
 OrgUnit        |     State/Province: Ontario
 CommonName     |     Locality Name:  Ottawa
 EmailAddress   |     Org. Name:
 Summary        |     Org. Unit:
                |     Common Name:    172.16.182.16
                |     Email Address:
                |
```

21 Review the information summary. Position the cursor on the Proceed button and press Enter. Otherwise, click Back to make revisions.

The system responds by creating the security certificate:

```
Exporting certificate/key pair to PKCS#12
keystore
Certificate/key pair has been successfully
exported to PKCS#12 format
Changing permissions on key file
Changing permissions on keystore file
```

22 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

Self-signed certificate security disclaimer

The following text contains the complete security disclaimer for using self-signed certificates. It is recommended that you read and understand this disclaimer before creating self-signed certificates.

“PLEASE REVIEW THE FOLLOWING TERMS AND CONDITIONS REQUIRED FOR THE USE OF DIGITAL SELF-SIGNED CERTIFICATES. MOVE BETWEEN PAGES BY USING THE 'C' AND 'B' KEYS. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS BELOW, YOU ARE NOT AUTHORIZED TO USE A DIGITAL SELF-SIGNED CERTIFICATE.”;

“DISCLAIMER OF WARRANTY: THIS DIGITAL SELF-SIGNED CERTIFICATE IS PROVIDED BY NORTEL 'AS IS' AND NEITHER NORTEL NOR ANY OF ITS SUPPLIERS MAKE, AND SPECIFICALLY DISCLAIM, ANY AND ALL REPRESENTATIONS, WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED, STATUTORY, ARISING BY USAGE OF TRADE OR OTHERWISE, INCLUDING WITHOUT LIMITATION, REPRESENTATIONS, WARRANTIES AND CONDITIONS OF MERCHANTABILITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK OF THE USE OF ANY DIGITAL SELF-SIGNED CERTIFICATE SHALL BE BORNE SOLELY BY YOU.”;

“LIMITATION OF LIABILITY: IN NO EVENT SHALL NORTEL OR ANY OF ITS SUPPLIERS AND THEIR RESPECTIVE, EMPLOYEES, OFFICERS, DIRECTORS AND AGENTS BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, EXEMPLARY, RELIANCE, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS OR BUSINESS OPPORTUNITIES, LOSS OF GOODWILL, PROFITS OR DATA, BUSINESS INTERRUPTION, LOST SAVINGS OR OTHER SIMILAR PECUNIARY LOSS, ARISING FROM OR IN CONNECTION WITH THE USE, PERFORMANCE OR NON-PERFORMANCE OF THE DIGITAL SELF-SIGNED CERTIFICATE, WHETHER ARISING IN

LAW OR EQUITY, ARISING FROM CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE) OR ANY OTHER THEORY OF LIABILITY AND REGARDLESS OF WHETHER NORTEL OR ITS SUPPLIERS WERE AWARE OF THE POSSIBILITY THEREOF. BY ENTERING 'Y', YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS JUST REVIEWED. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS JUST REVIEWED, ENTER 'N' BELOW. IF YOU DO NOT ACCEPT THESE TERMS AND CONDITIONS, YOU ARE NOT AUTHORIZED TO USE A DIGITAL SELF-SIGNED CERTIFICATE.";

Generate a certificate signing request

Purpose of this procedure

This procedure uses the certificate management tool to generate a certificate signing request or (CSR). A CSR is sent to a certificate signing authority to generate a CA-signed certificate. This procedure should only be used as part of a high level task for updating security certificates.

A successful completion of this procedure creates a certificate signing request composed of:

server.csr - contains the certificate signing request

The following certificate files are returned by the certificate signing authority upon successful processing of the certificate signing request:

- server.crt
- trusted.crt

Limitations and restrictions

Use this procedure only for CA-signed certificates.

You must be a root user to use the certificate management tool.

CAUTION
Possible service interrruption
If the unit has existing certificates in use and operating company personnel want to continue using the certificates until the certificate authority supplies the certificate information, make sure the currently used server key file is copied to a backup as described in step 2, and is restored as described in step 22. If the currently used certificate is not restored, a call processing outage can occur after SWACT, reboot, or a restart.

Prerequisites

There are no prerequisites for performing this procedure.

Action

At a Session Server command line interface (CLI)

1 Log onto the standby Session Server unit and change to the root user.

2 If existing certificates are currently in use and will continue to be used after this certificate signing request is generated, then copy the currently used server key file to a backup:

```
cd /opt/base/share/ssl
cp server.key server.key.to_restore
```

Note: The existing server key file is copied to server.key.to_restore and will be restored after the certificate signing request is generated.

3 Start the certificate management tool by typing

```
cert_mgnt
```

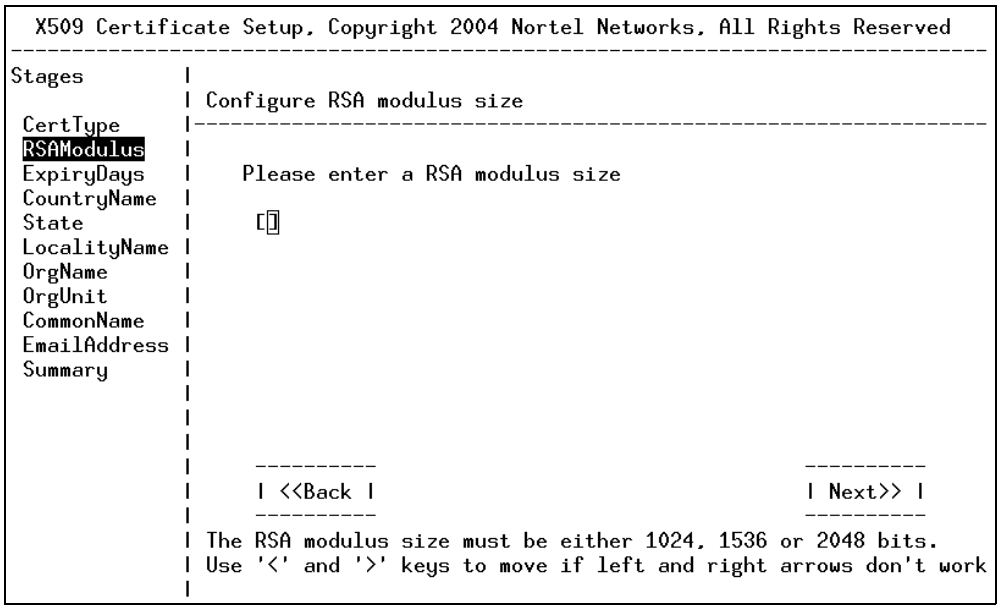
After a few seconds the Introduction screen is displayed.

```
 X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Stages          |
                | X509 Certificate Setup
 CertType       |-----------------------------------------------------------------
                |
                |    Welcome to the X509 Certificate Setup tool.
                |
                |     1) Generate Self-Signed Certificate
                |
                |     2) Generate Certificate Signing Request
                |
                |     3) Validate Certificate Chain
                |
                |
                |
                |     Option:
                |      [ ]
                |     ---------                                  ----------
                |     | Abort |                                  | Next>> |
                |     ---------                                  ----------
                |This tool will help you to bring your SSL/TLS-based application
                |into service
                |Use the <TAB> key to move and select fields
```

4 Press 2 for the option to generate a certificate signing request for a signing authority, position the cursor on the **Next** button and press **Enter**.

Note: In general, use the **Tab** key or the < and > keys to navigate between fields on the screen and use **Enter** to select a field or entry.

The RSA modulus size screen appears.



5 Enter the RSA modulus (key) size, position the cursor on the **Next** button and press **Enter**. Supported values are 1024, 1536 or 2048 bits.

Note: The larger the key size, the stronger the private key. There may be a performance impact when using larger key sizes.

6 Use the following table to determine your next step:

If	Do
you receive the message that the RSA private key already exists and you do not want to reuse the key	step 7
you receive the message that the RSA private key already exists and you want to reuse the key	Press **y** and skip to step 11
you do not receive any message that an RSA private key already exists	step 11

7 If you do not want to reuse the key, press **n**.

The system prompts that the RSA key is about to be deleted.

8 Use the following table to determine your next step:

If	Do
you do not want to delete the existing RSA key	Press **n** to abort the delete operation and go to step 9
you are sure you want to proceed with deleting the existing RSA private key	Skip to step 10.

9 Press any key and return to step 5.

10 If you want to delete the existing RSA key, press **y**.

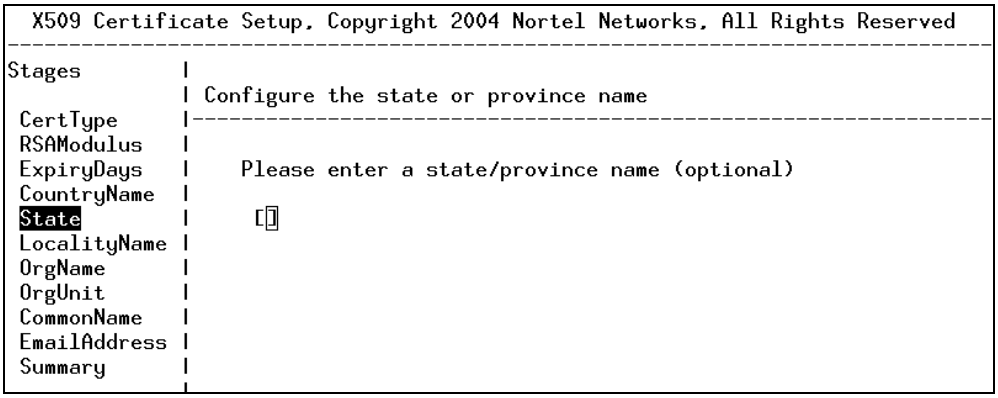
A backup of the existing key is made to a file in the same directory and a customer log is generated. The country name configuration screen appears.

```
  X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-------------------------------------------------------------------------------
Stages          |
                | Configure the country name
 CertType       |-----------------------------------------------------------------
 RSAModulus     |
 ExpiryDays     |    Please enter a country name (2 letter code) (optional)
 CountryName    |
 State          |     []
 LocalityName   |
 OrgName        |
 OrgUnit        |
 CommonName     |
 EmailAddress   |
 Summary        |
                |
                |
                |
                |     ----------                                  ----------
                |     | <<Back |                                  | Next>> |
                |     ----------                                  ----------
                | Use '<' and '>' keys to move if left and right arrows don't work
```

11 If applicable, enter the optional ISO 3166-1-alpha-2 two-letter country code, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Session Server to a remote entity.

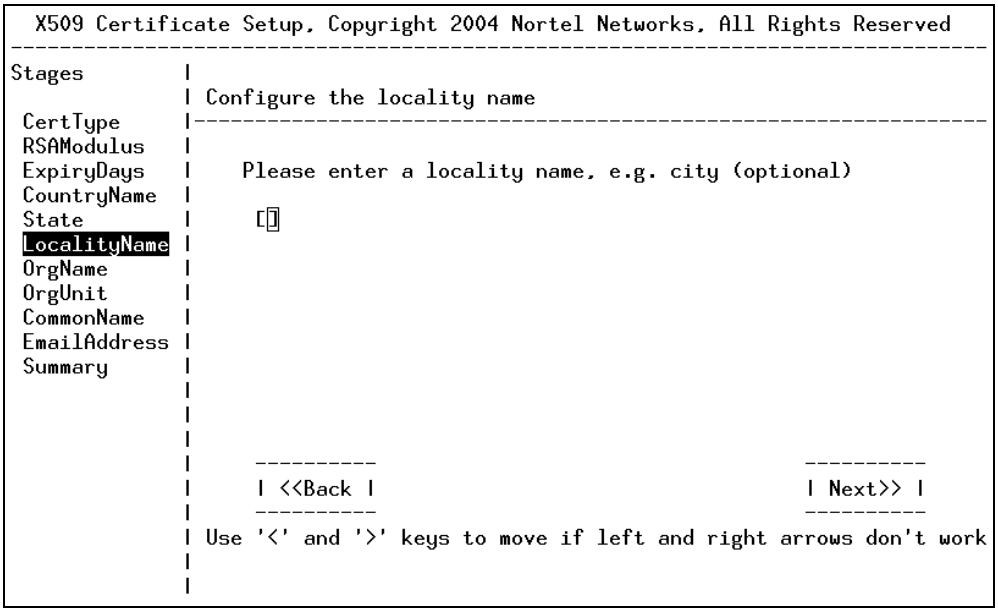
The state/province configuration screen appears.



12 If applicable, enter the optional state or province name, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Session Server to a remote entity.

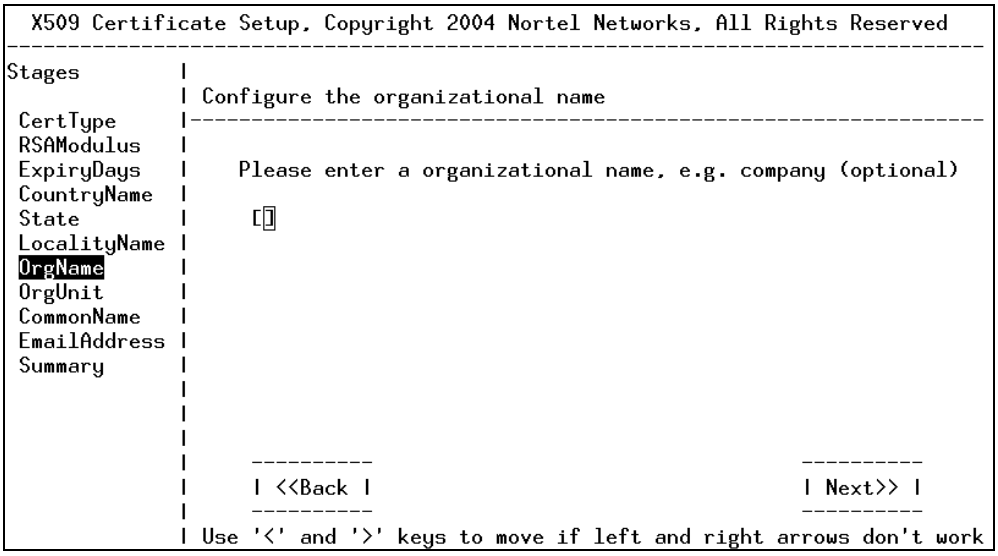
The locality configuration screen appears.



13 If applicable, enter the optional name of the locality or city, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Session Server to a remote entity.

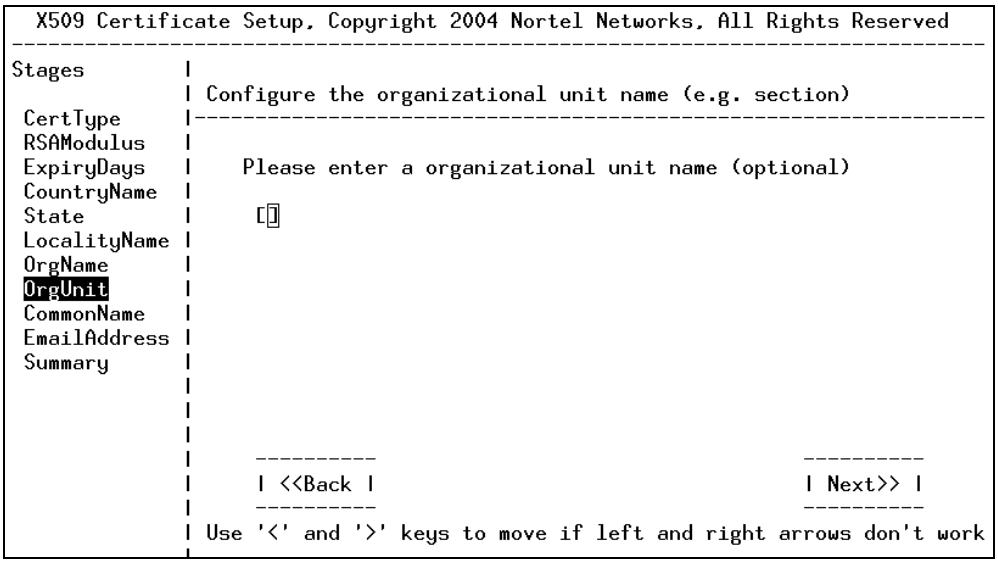
The organizational configuration screen appears.



14 If applicable, enter the optional name of the organization, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Session Server to a remote entity.

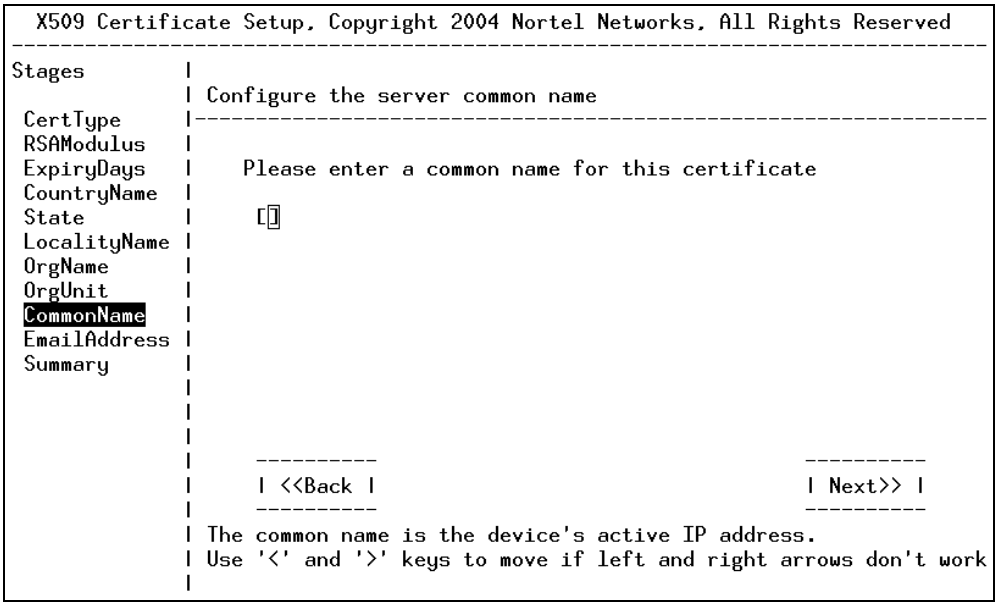
The organizational unit configuration screen appears.



15 If applicable, enter the optional name of the organizational unit, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Session Server to a remote entity.

The server common name configuration screen appears.



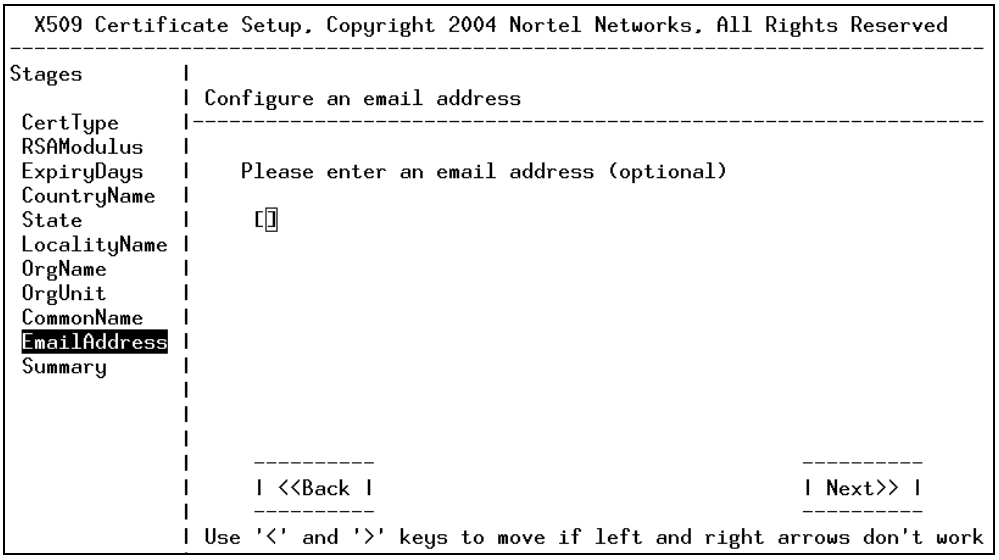
16 Enter a common name for the Session Server node to which this certificate applies using one of the following methods:

- use the active IP address for the Session Server in the format: xxx.xxx.xxx.xxx
- use a hostname of up to 64 alphanumeric characters, with hyphens, underscores and periods allowed. The hostname used must be in FQDN (fully-qualified domain name) format. If you chose to use a host name, this same hostname must also be used as in the mgcHostName field when datafilling the SIP Gateway application configuration parameters. To datafill the mgcHostName, refer to procedure Configure SIP Gateway application parameters, in NTP Session Server Configuration Management, NN10338-511.

Note: The common name value is used for mutual authentication between the Session Server and the remote application server. There is no validation of the common name at this stage of the configuration operation.

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

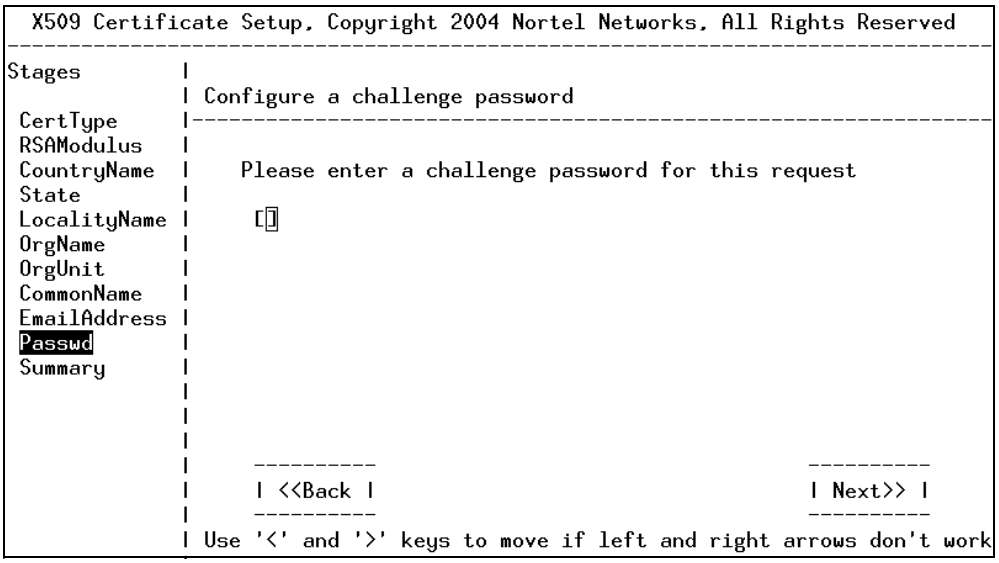
An email configuration screen appears.



18 If applicable, enter the optional email address of the organization, position the cursor on the **Next** button and press **Enter**.

Note: This entry helps identify the Session Server to a remote entity. There is no validation of the email address.

A password challenge configuration screen appears.



19 Enter a password challenge phase, position the cursor on the **Next** button and press **Enter**. The challenge password may be required if you want to revoke your certificate.

Note: This entry can be up to 16 alphanumeric characters in length and can include the underscore character.

A certificate summary information screen appears.

```
  X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
--------------------------------------------------------------------------------
Stages          |
                | Confirm the certificate information
 CertType       |-----------------------------------------------------------------
 RSAModulus     |
 ExpiryDays     |    Select 'Proceed' or 'Back' to make changes.
 CountryName    |
 State          |     Modulus Size:   1024
 LocalityName   |     Expiry Days:    7300
 OrgName        |     Country Name:   CA
 OrgUnit        |     State/Province: Ontario
 CommonName     |     Locality Name:  Ottawa
 EmailAddress   |     Org. Name:
 Summary        |     Org. Unit:
                |     Common Name:    172.16.182.16
                |     Email Address:
                |
                |     ----------                              -----------
                |     |<<Back |                               | Proceed |
                |     ----------                              -----------
                | This screen allows you to confirm that all of your
                | settings are correct.
```

20 Review the information summary. Position the cursor on the **Proceed** button and press **Enter**, otherwise click **Back** to make revisions.

The system responds by creating the security certificate:

```
Generating Certificate Signing Request
Creating Certificate Signing Request
Certificate Signing Request has been
successfully generated
Changing permissions on key file
```

A CRTM700 log report is generated if the response to step 6 *was* ***n*** *to indicate that a new private key was requested. The existing server.key file is moved to a backup copy, refer to* Additional information*.*

If the mate unit is in service a SIPS303, TLS Certificate Mismatch, alarm is raised, and the backup of the server key file made in step 2 *must be restored or a call processing outage may occur in the event of a SWACT, reboot, or restart.*

21

If	Do
y was entered in step 6 to reuse the existing server.key file	Delete the server.key.to_restore file. Since the existing key is reused, it is not needed. Go to step 23.
n was entered in step 6 to create a new server.key file	Continue to step 22 to make a copy of the newly created server.key as well as restore the server.ley file currently in use.

22 Copy the newly created server key file for safe keeping until the certificate authority sends the certificate information. In addition, restore the server key file that was backed up in step 2:

```
cd /opt/base/share/ssl
cp server.key  server.key.safekeeping
mv server.key.to_restore  server.key
```

Note: The server key file that is used when the certificate authority returns the certificate information is named server.key.safekeeping. The server key file used just before the cert_mgnt tool was used is restored to the server.key file name.

The SIPS303 alarm clears.

23 The procedure is complete. The certificate signing request is ready to submit to a certificate authority, of the customer's choosing, for signing and certificate generation. This submission process may take several weeks to complete. Once the certificate authority's certificate and the signed certificate are returned to the customer site, you must validate the certificate chain using procedure Import certificates and private key on page 166.

Additional information

When a certificate signing request is made, the existing server.key file is copied to a backup in the `/opt/base/share/ssl` directory. The backup name is related to the time of the signing request as follows:

server.key_hhmm_ddMMyyyy

hh — hour of the request, 0 to 24 and may be a single digit

mm — minute of the request, 0 to 59, and may be a single digit

dd — day of the request, 1 to 31, may be a single digit

MM — month of the request, 1 to 12, may be a single digit

yyyy — year of the request

Example
server.key_1359_352005

This backup was made at 1:59 on May 3, 2005.

Import certificates and private key

Purpose of this procedure

This procedure uses the certificate management tool to import the CA-signed certificate, the user certificate and the RSA private key to the appropriate directory.

Limitations and restrictions

The following restrictions apply to migrating CA-signed certificates:

- You must be a root user to use the certificate management tool.
- Only PEM formatted, CA-signed certificates are supported on Session Server - Trunks.
- CA chain is required in PEM format in a `trusted.crt` file, top down with the root CA at the top.
- Migrating self-signed certificates from SN07 is not supported. If upgrading from SN07 and your site uses self-signed certificates, you must create new ones during the upgrade activity.

Prerequisites

Ensure `server.crt`, `trusted.crt`, and `server.key` files are located in a temporary directory such as `/users/mtc`.

Action

At the NCGL CLI or IEMS client

1 Log on to the inactive unit and change to the root user.

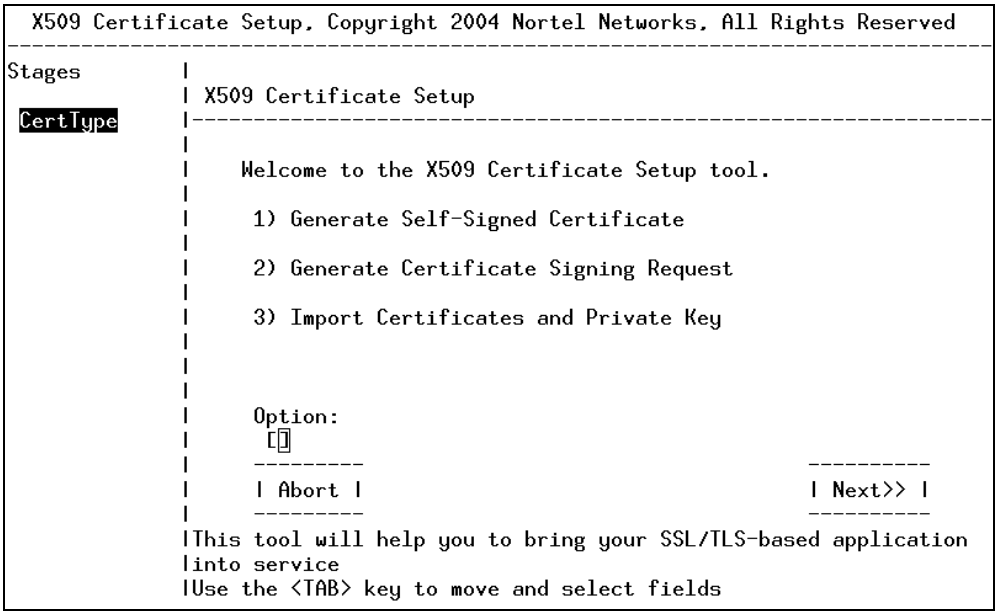
2 Change directory to the location of the certificate and key files:

```
cd /users/mtc
```

3 Start the certificate management tool by typing

```
/sbin/cert_mgnt
```

After a few seconds the Introduction screen is displayed.

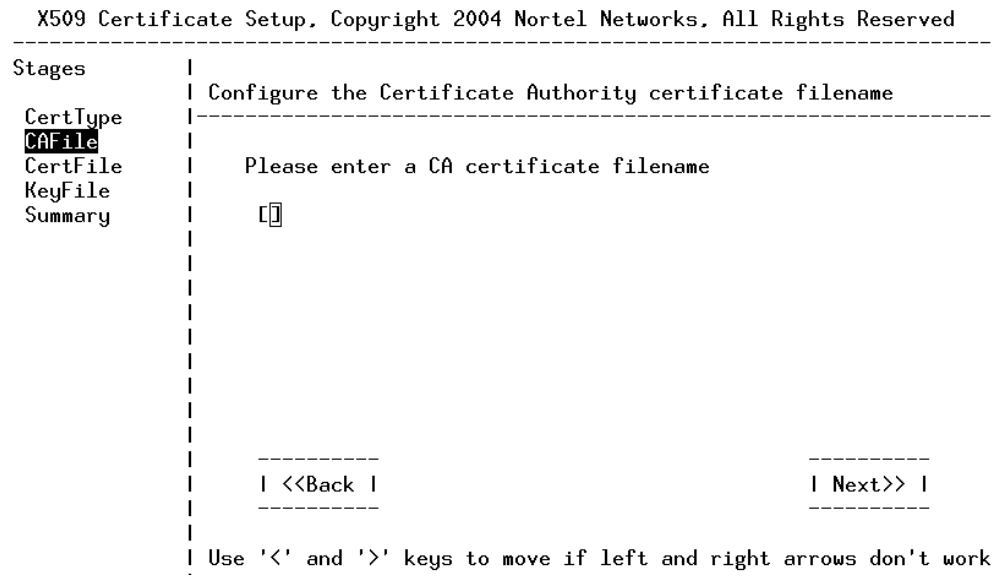


4 Press 3 for the option to import certificates and private key.

Use the Tab key to position the cursor on the Next button and press Enter.

Note: In general, use the Tab key or the < and > keys to navigate between fields on the screen and use Enter to select a field or entry.

The Configure the Certificate Authority certificate filename screen appears.



5 Enter the filename of the CA certificate by typing

`trusted.crt`

position the cursor on the Next button and press Enter.

Note 1: The tool will not proceed unless the CA certificate trusted.crt file exists in the location specified.

Note 2: If migrating self-signed certificates that were generated after SN07, then enter server.crt here and in step 6.

The Configure the CA-signed certificate filename screen appears.

```
  X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-------------------------------------------------------------------------------
Stages          |
                | Configure the CA-signed certificate filename
 CertType       |-----------------------------------------------------------
 CAFile         |
 CertFile       |    Please enter the user certificate filename
 KeyFile        |
 Summary        |     [
                |
                |
                |
                |
                |
                |
                |
                |
                |     ----------                                ----------
                |     | <<Back |                                | Next>> |
                |     ----------                                ----------
                |
                | Use '<' and '>' keys to move if left and right arrows don't work
                |
```

6 Enter the filename of the `server.crt` certificate by typing

`server.crt`

position the cursor on the Next button and press Enter.

Note: The tool will not proceed unless the file exists in the location specified.

The Configure the RSA private key filename screen appears.

```
  X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-------------------------------------------------------------------------------
Stages          |
                | Confirm the certificate/key information
 CertType       |-----------------------------------------------------------
 CAFile         |
 CertFile       |    Select 'Proceed' or 'Back' to make changes.
 KeyFile        |
 Summary        |     CACert:     server.crt
                |     UserCert:   server.crt
                |     PrivateKey: server.key
                |
                |
                |
                |
                |
                |
                |
                |     ----------                                -----------
                |     |<<Back |                                 | Proceed |
                |     ----------                                -----------
```

7 Review the information summary. Position the cursor on the Proceed button and press Enter, otherwise click Back to make revisions.

The tool validates the certificates chain and the trusted certificate files. Upon success, the tool displays the following:

```
Provisioning CA Certificate
Verifying certificate/key pair
spawn openssl verify -CAfile trusted.crt server.crt
server.crt: OK
Certificate validation succeeded
Exporting certificate/key pair to PKCS#12 keystore
Committing trusted certificate to /opt/base/share/ssl
Committing server certificate to /opt/base/share/ssl
Committing private key to /opt/base/share/ssl
Certificate/key pair has been successfully exported to PKCS#12
format
Changing permissions on key file
Changing permissions on keystore file
```

8 The procedure is complete. The cert_mgnt tool automatically copies the files to the `/opt/base/share/ssl` directory and sets the correct file permissions. If applicable return to the higher level task flow or procedure that directed you to this procedure.

Troubleshooting

The private key in the server.key file must correspond to the certificate in the server.crt file for validation to be successful. If you require assistance with completing this procedure, please contact Nortel GNPS.

Copy security certificates to the mate unit

Purpose of this procedure

The following procedure is used to copy security certificates from one unit to the mate unit.

Use this procedure any time new security certificates are created, or when the system is changed from using self-signed certificates to CA-signed certificates.

Limitations and Restrictions

There are no restrictions for performing this procedure.

Prerequisites

New certificates, either self-signed or CA-signed must be installed on the inactive unit.

Action

Perform the following steps to complete this procedure.

At the NCGL CLI or IEMS client

1 Log in to the active unit and change to the root user.

2 Change directories to the security certificates level:

```
cd /opt/base/share/ssl
```

3 Copy the security related files to the mate unit:

```
scp server.key mtc@mateblade:/users/mtc
scp certificate.keystore mtc@mateblade:/users/mtc
scp server.crt mtc@mateblade:/users/mtc
scp trusted.crt mtc@mateblade:/users/mtc
```

Note: For initial connections to the mate unit, confirm that you want to continue connecting by entering yes. Each instance of the scp command requires entering the password for the mtc account.

At your workstation CLI or IEMS client

4 Log in to the mate unit and change to the root user.

5 Change directories to /users/mtc:

```
cd /users/mtc
```

6 Determine the next action:

If the software version is	Do
SN08 or older	Continue to step 7
SN09 or newer	Enter the **cert_mgnt** command and select option 3. Performing this action will copy the files to the correct location and set the correct ownership and permissions. This procedure is complete.

7 Move the files from the /users/mtc directory to the /opt/base/share/ssl directory:

```
mv server.key /opt/base/share/ssl
mv certificate.keystore /opt/base/share/ssl
mv server.crt /opt/base/share/ssl
mv trusted.crt /opt/base/share/ssl
```

Note: If necessary, confirm overwriting any existing files by typing y and pressing Enter.

8 Change directories to the security certificates level:

```
cd /opt/base/share/ssl
```

9 Change the owner and group to root for all files:

```
chown root:root *
```

10 Set the file permissions:

```
chmod 600 server.key
chmod 600 certificate.keystore
chmod 644 server.crt
chmod 644 trusted.crt
```

11 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

If you did not complete this procedure as part of an upgrade, you must complete procedure “Apply security certificates” in the *Session Server - Trunks Security and Administration*, NN10346-611.

Apply security certificates

Purpose of this procedure

The following procedure is used to apply security certificates so that they are available to the Apache and Tomcat web services used by the Session Server GUIs and the SIP Gateway application.

Use this procedure only as part of a higher level activity such as part of an upgrade or security certificate management activity.

Limitations and Restrictions

CAUTION

This is a service affecting procedure.

Stopping and starting the Apache and Tomcat web services, causes access to the web server to be temporarily lost. Any open web connections to the web server are dropped. When executing this procedure, ensure that provisioning or maintenance activities are not occurring on any network element using the web services. Web access to the Session Server GUIs returns once the Apache and Tomcat services are restarted.

Prerequisites

This procedure has the following prerequisites:

- You must have first installed or copied any new security certificates to the cd /opt/base/share/ssl directory.

Action

Perform the following steps to complete this procedure.

At your workstation CLI or Integrated EMS client

1 Log onto the inactive Session Server unit and change to root user.

2 Stop the Apache web server by typing

```
# /usr/local/apache/bin/apachectl stop
```

and pressing the Enter key.

3 Restart the Apache web server by typing

```
# /usr/local/apache/bin/apachectl startssl
```

and pressing the Enter key.

4 Stop the Tomcat web server by typing

```
# /opt/apps/webint/tomcatd stop
```

and pressing the Enter key.

5 Restart the Tomcat web server by typing

```
# /opt/apps/webint/tomcatd start
```

and pressing the Enter key.

6 The SIP Gateway application must be stopped and restarted to allow it to work with the new security certificates. Execute procedures Lock the SIP Gateway application on page 117, Suspend the SIP Gateway application on page 124, Unsuspend the SIP Gateway application on page 128 and Unlock the SIP Gateway application on page 121, in the order listed, to stop and restart the application.

CAUTION

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

7 You have completed this procedure.

Manage Trusted Certificates

Purpose of this procedure

Use this procedure to retrieve a copy of a self-signed or a Certificate Authority certificate (root CA) and add it into a remote server's trusted certificate list. Also, use this procedure to view existing trusted certificates and to delete a certificate from the trusted certificate list.

If a certificate was replaced on a remote SIP server, delete the existing certificate for that remote SIP server, restart the SIP Gateway application, and then add the new certificate for the remote SIP server. The restart is required to remove the entry from the running SIP Gateway application.

Limitations and restrictions

If the server's own self-signed or root certificate is accidentally added as a trusted certificate, then a SIPS606 log report is generated on application startup to indicate that the certificate is rejected. The application fails to add its own certificate because the server's own certificate is added before it processes the customer defined trusted certificates.

Prerequisites

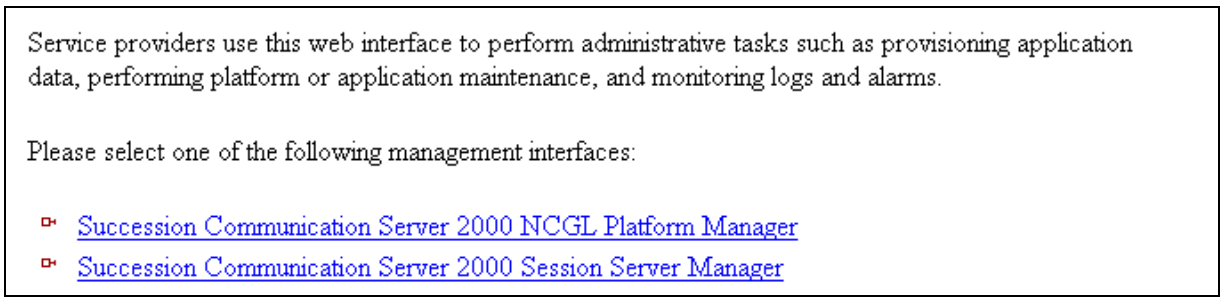
A valid self-signed or CA-signed server certificate must be installed on both Session Server - Trunks units.

When adding certificates, access to the self-signed or CA-signed certificate for the remote SIP server is needed. Step 8 requires pasting the PEM formatted certificate so it can be added as a trusted certificate.

Action

At the CS 2000 Session Server Launch Point

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



2 Select **Provisioning > Security > SIP Gateway > Certificates** from the left side menu:

3 Use the following table to determine your next step:

Note: Do not add this server's own certificate or else a SIPS606 log report will be generated on every restart to indicate that the application failed to add the trusted certificate.

If	Do
you want to add a CA-signed trusted certificate	continue to step 4 ***Note:*** If the remote SIP server and the local Session Server - Trunks node have CA-signed certificates from the same CA-signing authority, local root CA = remote root CA, then no action is required and this procedure is complete.
you want to add a self-signed trusted certificate	skip to step 5
you want to view trusted certificates currently provisioned	skip to step 9
you want to delete a trusted certificate currently provisioned	skip to step 9

4 Obtain the root CA certificate for the remote SIP server.

If the remote SIP server is a Session Server - Trunks node:

a Log in to the unit and become root. View the trusted.crt file:

```
more /opt/base/share/ssl/trusted.crt
```

b Select the text and copy it so it can be pasted as shown in PEM formatted certificate.

c Go to step 6.

5 Obtain the self-signed certificate for the remote SIP server.

If the remote SIP server is another Session Server - Trunks node, then perform procedure Display local server certificates on page 182 from the user interface for the remote node. When done with that procedure, select and copy the PEM formated certificate as shown below:

PEM formatted certificate

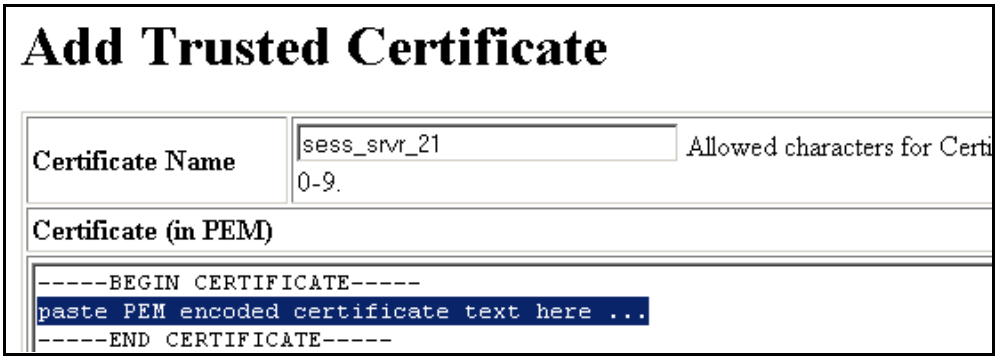
```
-----BEGIN CERTIFICATE-----
MIICkTCCAfqgAwIBAgIBADANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTkMxDDAKBgNVBAcTA1JUUDEWMBQGA1UEAxMNMTkyLjE2OC41Mi4x
MTAeFw0wNTA0MDYxNDQ3MzlaFw0wNjA0MDYxNDQ3MzlaMEAxCzAJBgNVBAYTAlVT
MQswCQYDVQQIEwJOQzEMMAoGA1UEBxMDUlRQMRYwFAYDVQQDEw0xOTIuMTY4LjUy
LjExMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfR2aAlOX8GH+n6dfZHSQJ
bTYLEK3vDIDz6k4iOl0Uv+NkB4fQdlifusE2Oia/l9+oh1QJZe/XtK56+0DmnJzK
Q+j4dxRt4pMOQjfYl02Q+sgtrXcaHmGSg3IIjtpZCqTn5+CzuciE6cr756fr/5e2
fN222mWA4wjjtKa0FHafFQIDAQABo4GaMIGXMB0GA1UdDgQWBBQk7tPqLO0MPnCw
2iEQ4oq4HVtiMTBoBgNVHSMEYTBfgBQk7tPqLO0MPnCw2iEQ4oq4HVtiMaFEpEIw
QDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk5DMQwwCgYDVQQHEwNSVFAxFjAUBgNV
BAMTDTE5Mi4xNjguNTIuMTGCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUF
AAOBgQBgAgHMvbb7kwnct94uCsQCMANyeGDkfwy/rCfUJve3ulKt9ALPy1nZRtns
DDQShszalGLOiThPsW3iwrArHAHQZ36kO1nmhMrQzUkU25NZ8GR5PgeadIADEvTa
+GGHyg0Mkxl0P7ywdujpyQEBpLVjWvptzmeABoWt9Tjp5OiNlg==
-----END CERTIFICATE-----
```

6 Click **Add Remote Trusted Certificates** from the left side menu:

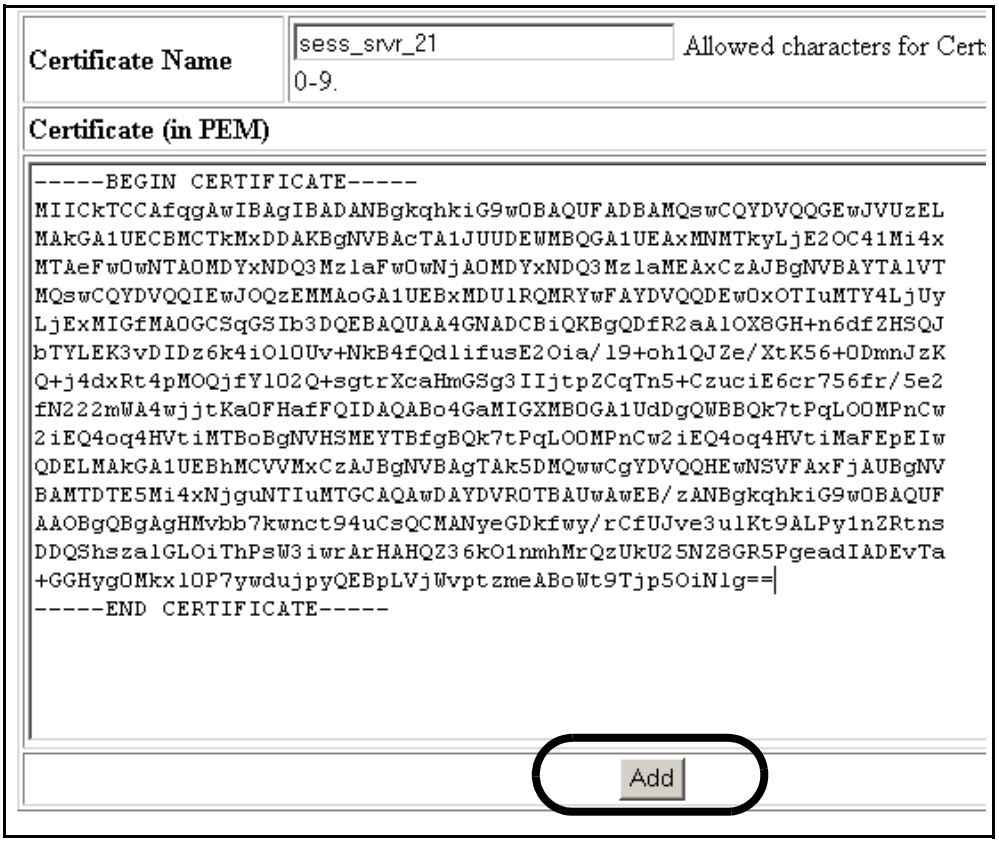
7 On the Add Trusted Certificate page, enter a name for this certificate, up to 16 alphanumeric characters in length. It is

recommended to indicate the remote SIP server associcated with the certificate.

In the certificate view, delete the highlighted line of text:

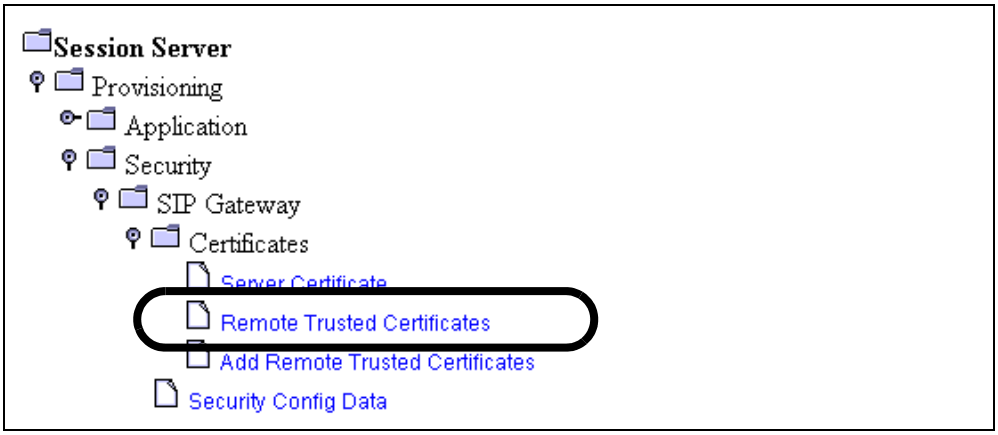


8 In the certificate view, paste the certificate you copied from the remote SIP server and click **Add**:



The certificate is added to the running SIP Gateway application and the active unit database. This certificate is automatically copied to the inactive unit database during database synchronization.

9 Click **Remote Trusted Certificates** from the left side menu:



10 On the Certificates Provisioned page, certificates are shown:

Note: The view is empty if no remote server certificates have been added.

Certificates Provisioned

This is a list of configured trusted certificates.

Deleting these certificates will take effect on the next application restart. Please contact Technical Support for assistance if needed.

Certificate Name	Certificate PEM	Delete
sess_srvr_21	-----BEGIN CERTIFICATE----- MIICkTCCAfqgAwIBAgIBADANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQGEwJVUzEL MAkGA1UECBMCTkMxDDAKBgNVBAcTA1JUUDEWMBQGA1UEAxMNMTkyLjE2OC41Mi4x MTAeFw0wNTA0MDYxNDQ3MzlaFw0wNjA0MDYxNDQ3MzlaMEAxCzAJBgNVBAYTAlVT MQswCQYDVQQIEwJOQzEMMAoGA1UEBxMDUlRQMRYwFAYDVQQDEw0xOTIuMTY4LjUy LjExMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfR2aAlOX8GH+n6dfZHSQJ bTYLEK3vDIDz6k4iOlOUv+NkB4fQdlifusE2Oia/l9+oh1QJZe/XtK56+ODmnJzK Q+j4dxRt4pMOQjfYlO2Q+sgtrXcaHmGSg3IIjtpZCqTn5+CzuciE6cr756fr/5e2 fN222mWA4wjjtKaOFHafFQIDAQABo4GaMIGXMB0GA1UdDgQWBBQk7tPqLOOMPnCw 2iEQ4oq4HVtiMTBoBgNVHSMEYTBfgBQk7tPqLOOMPnCw2iEQ4oq4HVtiMaFEpEIw QDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAk5DMQwwCgYDVQQHEwNSVFAxFjAUBgNV BAMTDTE5Mi4xNjguNTIuMTGCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUF	Delete

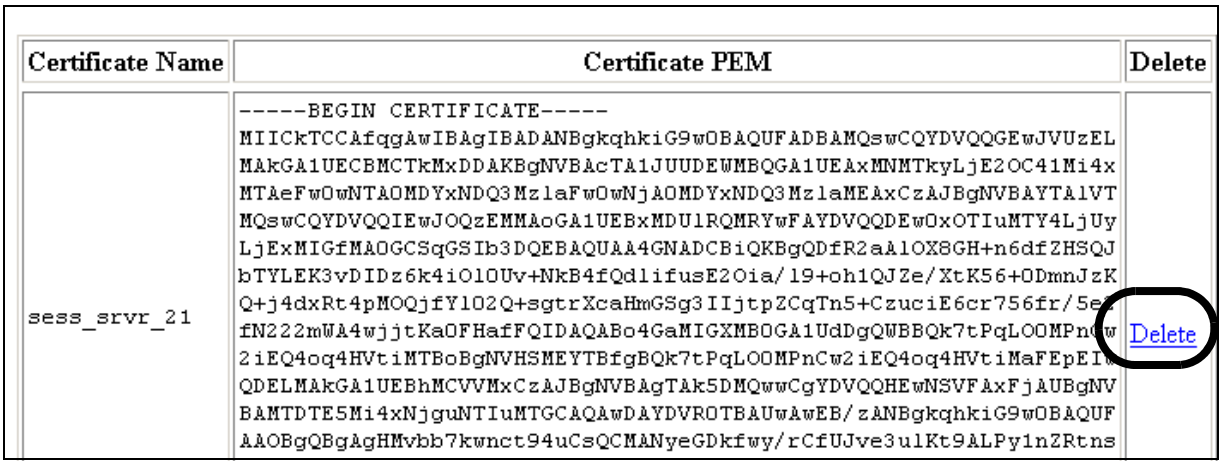
11 Use the following table to determine your next step:

If	Do
you want to delete a trusted certificate currently provisioned	continue with step 12

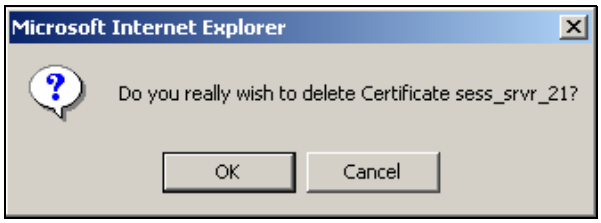
If	Do
you do not want to delete a trusted certificate currently provisioned	return to step 3

12 In the Certificates Provisioned view, delete a certificate by clicking the **Delete** link to the right of the certificate.

Note: The view is empty if no remote server certificates have been added.



13 Click **OK** to confirm the delete:



The certificate is deleted from the active unit database and is automatically removed from the inactive unit database during database synchronization. However, it is not removed from the running SIP Gateway application. A restart is required to remove the certificate from the running SIP Gateway application, with one exception: the local server's own certificate. The local server's own certificate is unnecessary in the database and should be removed if found there. Removing that particular certificate does not require a SIP Gateway application restart

14 Return to step 11.

15 The procedure is complete.

Display local server certificates

Purpose of this procedure

Use this procedure to display a local server certificate used by the Session Server - Trunks node.

Limitations and restrictions

There are no restrictions for performing this procedure.

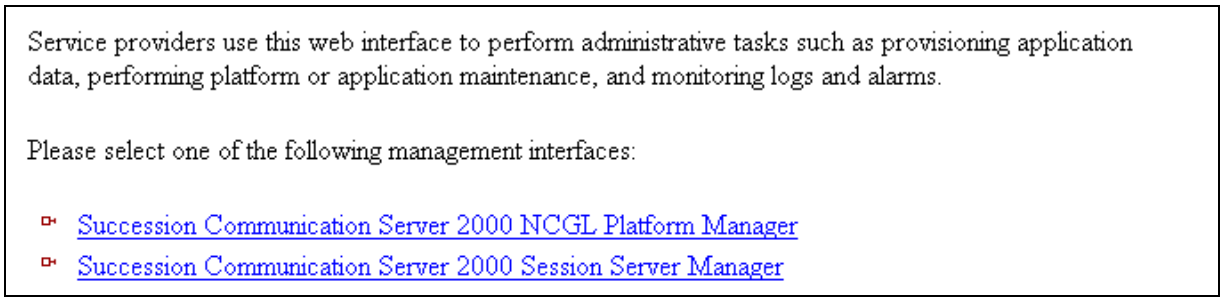
Prerequisites

There are no prerequisites for performing this procedure.

Action

At the CS 2000 Session Server Launch Point

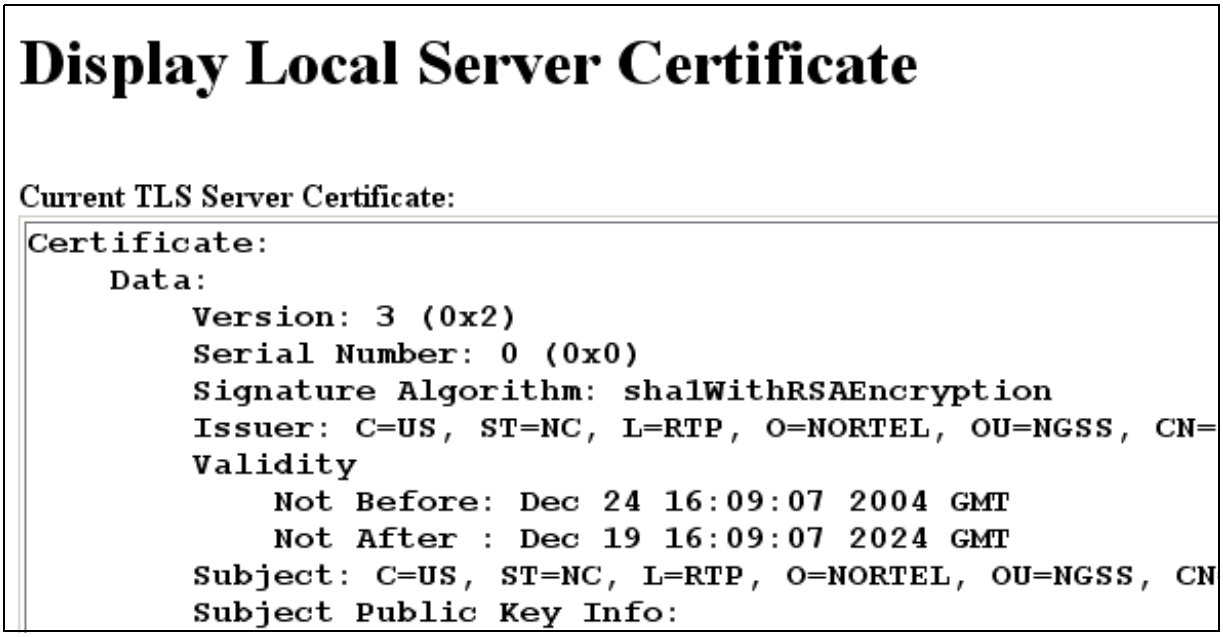
1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.



2 Select **Provisioning > Security > SIP Gateway > Certificates** from the left side menu:

3 Click **Server Certificate**.

The system displays the local server certificate page with the certificate information at the top.



Display Local Server Certificate

Current TLS Server Certificate:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=NC, L=RTP, O=NORTEL, OU=NGSS, CN=
        Validity
            Not Before: Dec 24 16:09:07 2004 GMT
            Not After : Dec 19 16:09:07 2024 GMT
        Subject: C=US, ST=NC, L=RTP, O=NORTEL, OU=NGSS, CN
        Subject Public Key Info:
```

4 Scroll down to locate and view the actual certificate:

```
-----BEGIN CERTIFICATE-----
MIICFzCCAYCgAwIBAgIBADANBgkqhkiG9w0BAQUFADAYMRYwFAYDVQQDEw(
NzQuNzQuMTg0MB4XDTA0MTIxNDE0NDU1M1oXDTI0MTIwOTE0NDU1M1owGDI
A1UEAxMNNDcuMTc0Ljc0LjE4NDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYk
sIGj91HUOZuoBttcDv6WS8uDQ2SBptgoKDGtxwDvHSp6HwSSKlh+oP7ZMP7
oS0GCXqMyw1Dz/4KbgThn43QfGgRfBMZ5OQeRKQxLZ/IUIobbOSuE9qOMcS
vg6POrj8AoY0TNvy0qd9p06KeSZpWFlilPFsmMKjPMMCAwEAAaNxMG8wHQY
BBYEFISzCW/PLt0VKQT0HhC7psaikKtpMEAGA1UdIwQ5MDeAFISzCW/PLt(
HhC7psaikKtpoRykGjAYMRYwFAYDVQQDEw00Ny4xNzQuNzQuMTg0ggEAMAw
EwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEALHw342GcEOvf22xGVczVPMM
8T21V5uOMBzjt7XlLzlU+Qt9ZFsu3CY/HJyZWlnloYGm8mTVn2HYUHhmC5i
i8d1ShFweehuW83FAJMuI0xsb9ZMM0zeZbKA4QjlPD2i5EsZf3CMp7sSimm
H9ZqvkO8OlnzJL4=
-----END CERTIFICATE-----
```

5 The procedure is complete.