



Carrier VoIP

Session Server Trunks Security and Administration

Document status: Standard
Document version: 04.02
Document date: 20 October 2006

Copyright © 2006, Nortel Networks
All Rights Reserved.

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

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are the property of their respective owners. All rights reserved.

Contents

New in This Release	5
Features	5
Other changes	5
Security and Administration overview	7
TLS Security for SIP messaging	7
Tools and utilities	8
Methods of accessing Session Server GUIs and CLI	9
Security administration of the SST	10
Managing security certificates in SN08	13
Operational administration and maintenance of the SST platform and applications	16
Determining the status of SIP access links	22
Managing SST Ethernet links	22
Performing a controlled shutdown of an SST node	23
Backing up the SIP Gateway application database	24
Individual procedures	27
Querying current number of SIP calls	28
Logging in remotely using a secure shell (SSH)	31
Accessing SST/NCGL GUIs or CLI using the IEMS	32
Accessing SST/NCGL GUIs using a proxied client	41
Managing users on the SST platform	44
Managing user passwords using an SST console CLI	47
Managing user passwords with the Session Server GUI	49
Invoking a maintenance SWACT of the SST platform	51
Invoking a manual cold SwAct of the SIP Gateway application	55
Invoking a manual switch of active links (Swlink)	59
Inhibiting a system SwAct (Jam)	62
Enabling a system SwAct (Unjam)	65
Locking network Ethernet link	68
Unlocking network Ethernet link	71
Halting (shutting down) an SST unit	74
Rebooting a unit	78
Verifying synchronization status	83

4 Contents

Viewing the operational status of the SIP Gateway application	85
Viewing the operational status of the NCGL platform	89
Locking the SIP Gateway application	104
Unlocking the SIP Gateway application	107
Suspending the SIP Gateway application	110
Unsuspending the SIP Gateway application	113
Backing up the SST	116
Powering off an SST unit	122
Powering on and booting an SST unit	124
Generating self-signed security certificates	125
Generating a certificate signing request	134
Importing certificates and the private key	144
Copying security certificates to the mate unit	148
Applying security certificates	150
Managing Trusted Certificates	152
Displaying local server certificates	158

New in This Release

The following sections list what's new in SST security and administration in this release.

Features

SST introduces no feature changes for security and administration in (I)SN09U.

Other changes

This release includes clarifications about the use of special characters in mgcHostName and HOST_MGCNAME with third-party vendor equipment.

Security and Administration overview

The security and administrative strategy for the Session Server Trunks (SST) centers around the following primary activities:

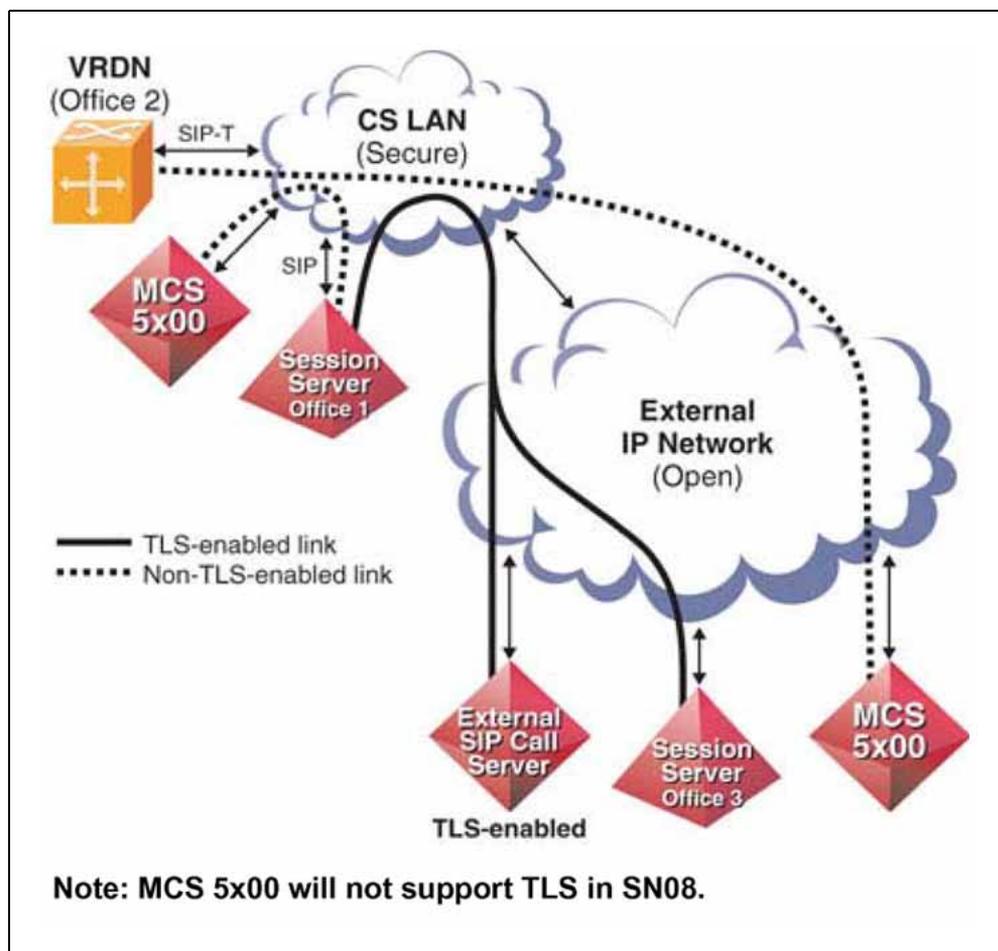
- Security administration of the SST, which includes managing user IDs and passwords, and acquiring security certificates
- Operational administration and maintenance of the SST platform and applications, which includes activities surrounding managing the SST platform Nortel Carrier-grade Linux (NCGL) 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, that is Transport Layer Security (TLS).

This protocol enables secure data transmission for inter-call server communication, such as between the SST and a remote SIP application server.

The TLS feature will allow the SST to establish TLS sessions with a remote Call Server or SIP application server that is TLS aware. With the support of TLS on the SST, 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.



Provisioning options enable UDP, TCP, or TLS (TCP) connections to be set up and utilized. For instructions about configuring TLS security, refer to *Session Server Trunks Configuration Management* (NN10338-511). The TLS Security feature also provides security-related logs, OMs, and alarms for monitoring security failures, potential attacks, and session establishment. For instructions about monitoring security-related logs and alarms, refer to *Session Server Trunks Fault Management* (NN10332-911). For instructions about monitoring security-related operational measurements, refer to *Session Server Trunks Performance Management* (NN10342-711).

Tools and utilities

Security administration and operational administration of the SST 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 command line interface (CLI) based 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.

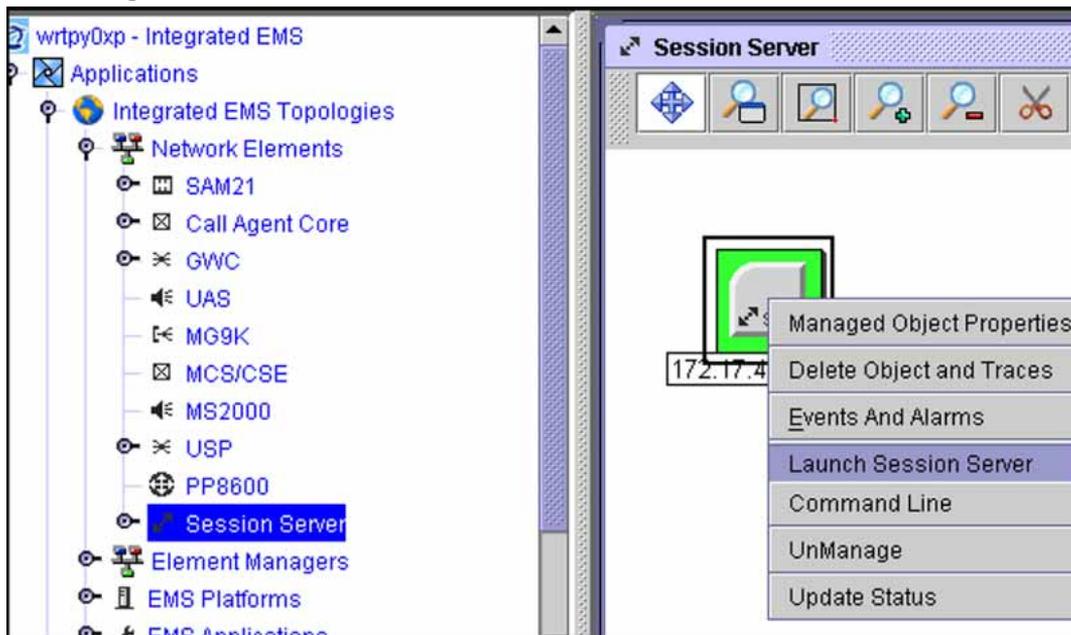


Methods of accessing Session Server GUIs and CLI

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 the active SST element from the IEMS expanded Network Elements view, as shown below.

Accessing Session Server GUIs or CLI from the IEMS



For more information, refer to the procedure "[Accessing Session Server GUIs or CLI from the IEMS](#)" (page 9). For more information about using the IEMS service, refer to *IEMS Basics* (NN10329-111).

- All GUI interfaces to the Session Server can be accessed from a remote system known to the SPFS proxy server (running on CS 2000 Management Tools server) on the CS-LAN. For more information, refer to procedure "[Accessing SST/NCGL GUIs using a proxied client](#)" (page 41). For more information about configuring a web proxy service on the SPFS, refer to *Session Server Trunks Configuration Management* (NN10338-511).
- The CLI interface can be accessed through a secure shell (SSH) connection from a remote client to the SST by way of SSH/telnet access through the SPFS server.
- For commissioning purposes, the CLI can also be accessed using a console connected to the rear of the SST active unit. In some cases, this connection is wired to a terminal box. For more information about using this CLI access method, refer to the *Session Server Trunks Configuration Management* (NN10338-511).

Security administration of the SST

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.

User and authorization categories

The following table of default groups are used on the SST, in similar fashion to the CS 2000 Management Tools Server SPFS. 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 maintenance activities. Cannot change provisioning data
mgcsprov	1013	Application provisioning user. Can modify provisioning data, but cannot take any platform maintenance actions.

Group Name	Group Number	Description
mgcrw/mgcro	1012/1015	Can view base or provisioning information but cannot initiate any changes
succssn	104	Required for all login access to the SST

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

Default user IDs on a new SST installation

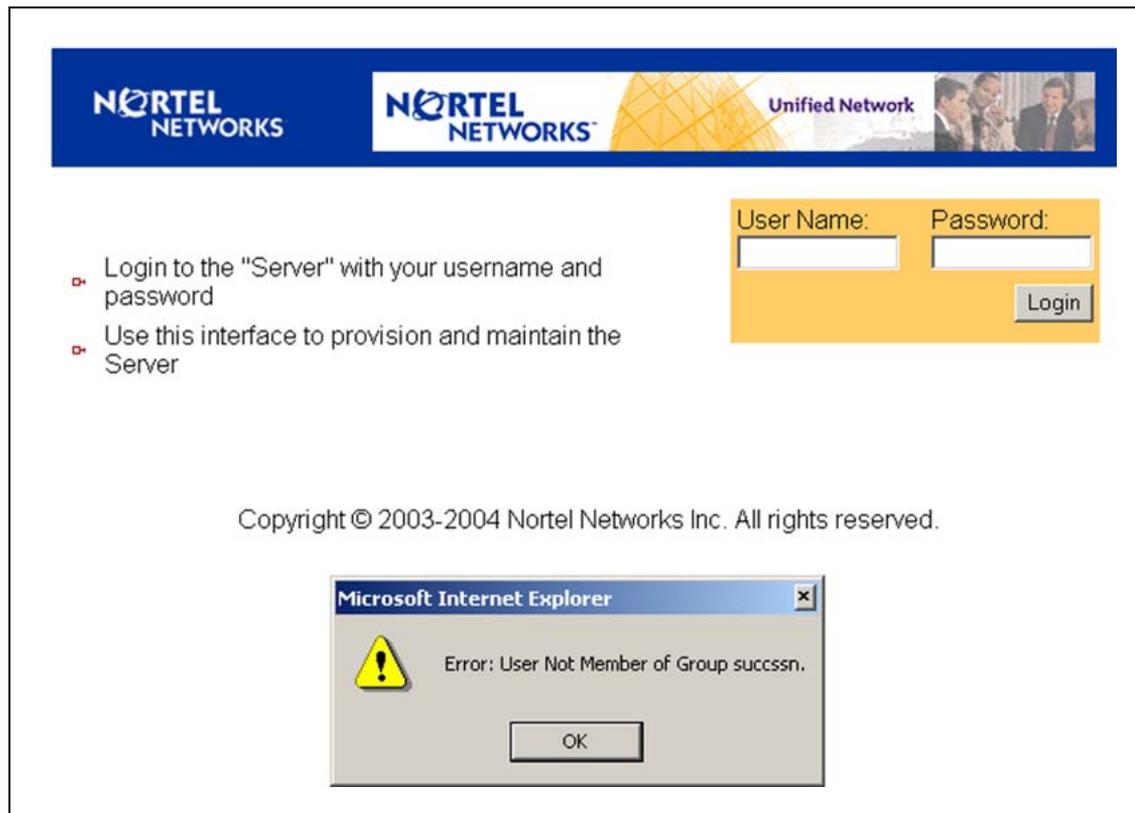
User Name	Groups	Description
root	root bin daemon sys adm disk wheel	System root user is not allowed when logging into the GUIs. Also, you cannot remotely log onto the SST console. You must log in as another user, then su (superuser) to the root user. The default root password is "sam39xts." This password should be changed during commissioning of the SST units.
mtc	succssn users mtc mgcadm mgcrw mgcsprov mgcmtc mgcro	SST platform NCGL maintenance user. The default password for mtc user is "mtc." This password should be changed during commissioning of the SST units. Note: The mtc user id should not be deleted. Doing so prevents command line interface (CLI) access from the IEMS 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 an SST console as another user type, then su to root super user. Refer to procedure "[Logging in remotely using a secure shell \(SSH\)](#)" (page 31) to perform this activity.

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 SST 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

"Managing users on the SST platform" (page 44)

"Managing user passwords using an SST console CLI" (page 47)

"Managing user passwords with the Session Server GUI" (page 49)

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 SST: 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 SST, 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 SST units, refer to the procedure "[Renewing expired CA-signed or self-signed certificates](#)" (page 13).

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.

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](#)" (page 14)
- To renew expired self-signed certificates, complete activity "[Creating new self-signed certificates](#)" (page 15)

ATTENTION

If your SST 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](#)" (page 14)
- To renew unexpired self-signed certificates, complete activity "[Creating new self-signed certificates](#)" (page 15)

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 SST to using CA-signed certificates, refer to section "[Creating new CA-signed certificates](#)" (page 14) 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 .
2	Complete the procedure " Generating a certificate signing request " (page 134).
3	Send the completed certificate signing request to a Certificate Authority for signing and certificate generation. 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 " Importing certificates and the private key " (page 144) on the inactive unit.

Step	Procedures
5	Complete the procedure "Applying security certificates" (page 150) to make the new certificates available to applications and GUIs used by the SST.
6	SwAct the units. Refer to "Invoking a maintenance SWACT of the SST platform" (page 51).
7	Complete the procedure "Copying security certificates to the mate unit" (page 148).
8	On the newly inactive unit, perform "Applying security certificates" (page 150).
9	Back up your existing security certificates using procedure Back up security certificates.

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 the procedure "Generating self-signed security certificates" (page 125) on the inactive unit.
2	Complete the procedure "Applying security certificates" (page 150) to make the new certificates available to applications and GUIs used by the SST.
3	SwAct the units. Refer to "Invoking a maintenance SWACT of the SST platform" (page 51).
4	Complete the procedure "Copying security certificates to the mate unit" (page 148).
5	On the newly inactive unit, perform "Applying security certificates" (page 150).
6	Back up your existing security certificates using procedure Back up security certificates.

Using the certificate management tool

New certificates are created and managed using the CS 2000 Session Server Manager GUI and the CLI-based *cert_mgmt* tool. The *cert_mgmt* tool is run on one SST 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 SST.

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

Procedures for managing security certificates

Procedure
"Displaying local server certificates" (page 158)
"Managing Trusted Certificates" (page 152)

Operational administration and maintenance of the SST platform and applications

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

- Managing operation of the NCGL platform and hardware for each SST 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 SST NCGL platform:

- Jam and Unjam - manually prevent a switch of activity (SwAct) to the standby unit. Jam and Unjam are performed in cases where an SST 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" \(page 19\)](#) 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 SST units.

- Network Ethernet link Lock and Unlock - shut down the Ethernet interfaces and isolate a single SST unit from the network. Refer to section "[Managing SST Ethernet links](#)" (page 22) 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

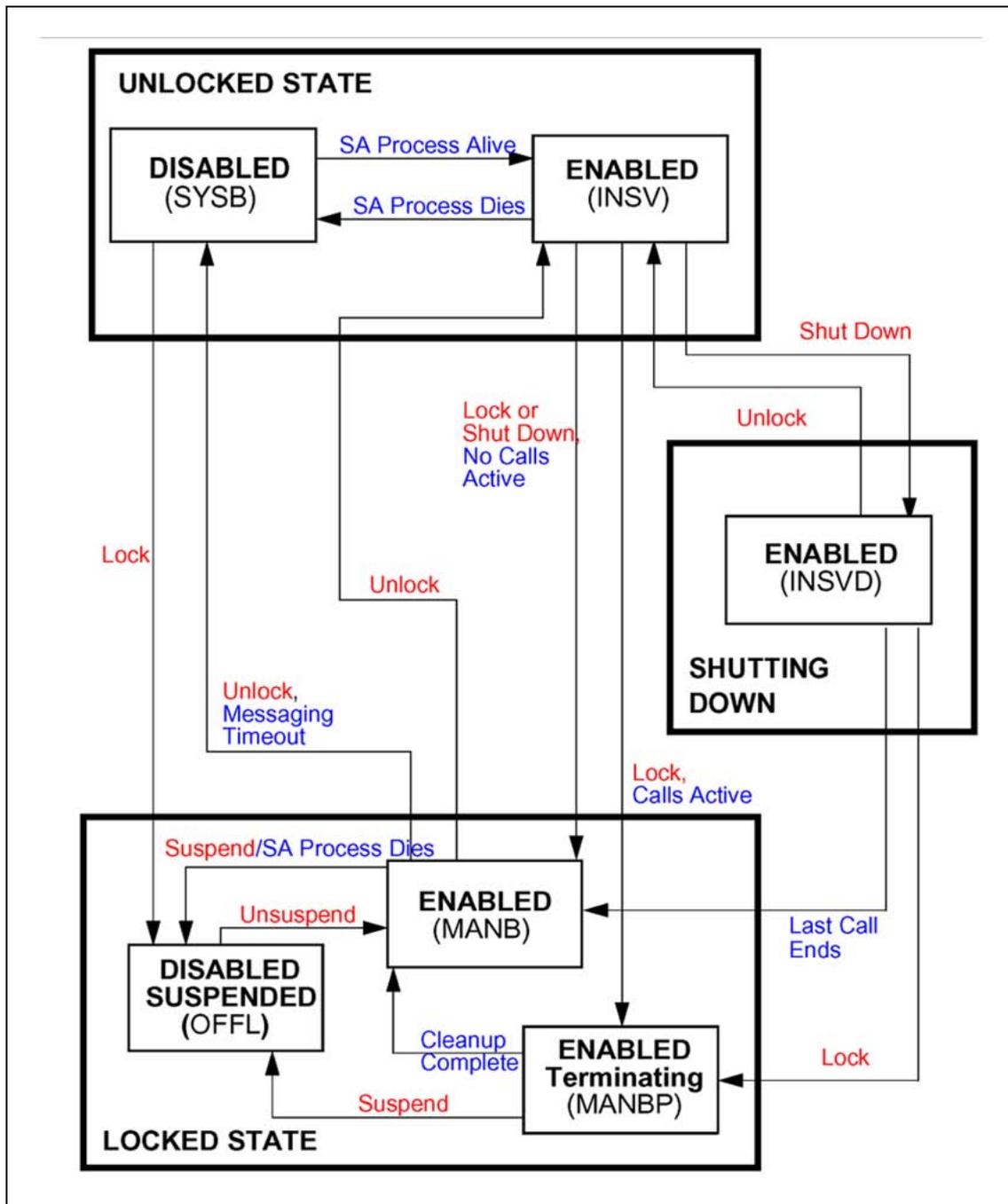
The following table explains the controls that are allowed based on the current Admin State, Operational State, and Procedural Status of the SIP Gateway application. Legacy DMS style representation is shown in parentheses to aid in understanding.

Operational	Allowed Controls		
	Admin	Procedural	Control

State	State	Status	Status	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 SST 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		Application rejects SWACT	Manual "Force" SWACT
Active	Inactive	Manual or Application requested SWACT	System Initiated 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
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

The operating system status critical alarm prevents a SwAct, but does not cause a system initiated SwAct.

For more information about faults, alarms and fault conditions, refer to *Session Server Trunks Fault Management* (NN10332-911).

Operational administration procedures for the SST platform

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

System administration procedures

Procedure
"Powering on and booting an SST unit" (page 124)
"Powering off an SST unit" (page 122)
"Halting (shutting down) an SST unit" (page 74)
"View the operational status of the NCGL platform" (page 89)
"Rebooting a unit" (page 78)
"Accessing SST/NCGL GUIs or CLI using the IEMS" (page 32)
"Accessing SST/NCGL GUIs using a proxied client" (page 41)

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
"Invoking a maintenance SWACT of the SST platform" (page 51)
"Invoking a manual cold SwAct of the SIP Gateway application" (page 55)
"Inhibiting a system SwAct (Jam)" (page 62)
"Enabling a system SwAct (Unjam)" (page 65)
"View the operational status of the SIP Gateway application" (page 85)
"Locking the SIP Gateway application" (page 104)
"Unlocking the SIP Gateway application" (page 107)
"Suspending the SIP Gateway application" (page 110)
"Unsuspending the SIP Gateway application" (page 113)
"Querying current number of SIP calls" (page 28)
"Verifying synchronization status" (page 83)

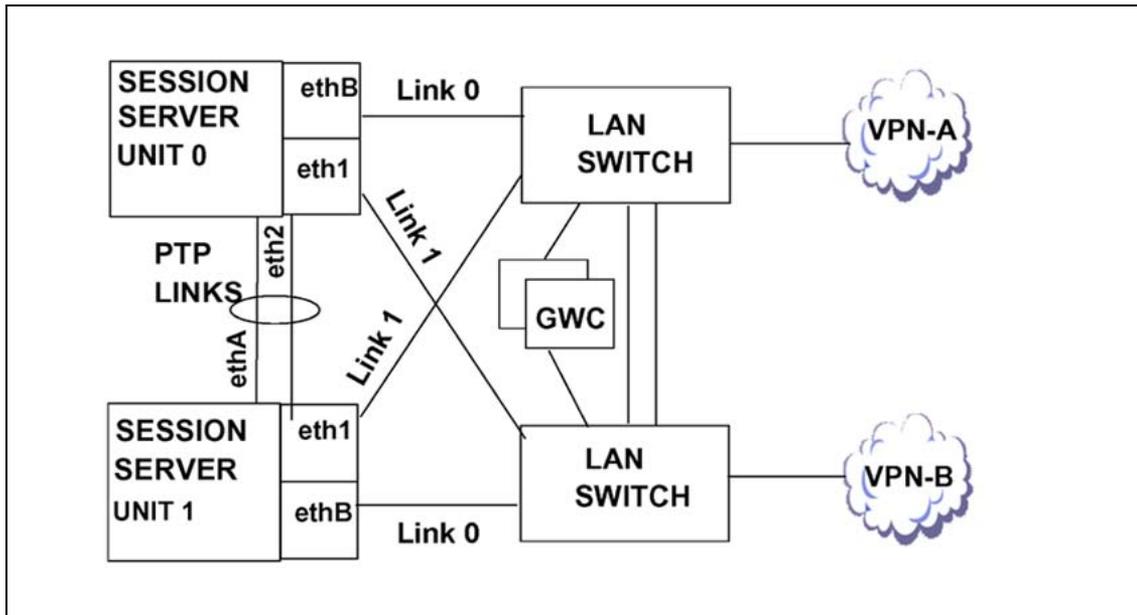
Determining the status of SIP access links

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 SST, it is dependent on receiving link status information from the SIP-T GWCs, which receive access link status messages from the SST 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 SST Ethernet links

The following figure shows each SST 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 SST Ethernet ports and link configuration



Ethernet link management procedures for SST

The following table lists the link management procedures:

Operational administration procedures

Procedure
"Invoking a manual switch of active links (Swlink)" (page 59)
"Locking network Ethernet link" (page 68)
"Unlocking network Ethernet link" (page 71)

Performing a controlled shutdown of an SST node

Execute the procedures in the following activity to perform a controlled shutdown of an SST 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 "Backing up the SST" (page 116).
2	Perform the procedure "Locking the SIP Gateway application" (page 104) on the active unit.
3	Perform the procedure "Suspending the SIP Gateway application" (page 110) on the active unit.
4	Perform the procedure "Halting (shutting down) an SST unit" (page 74) on the inactive unit. 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 the procedure "Powering off an SST unit" (page 122) on the inactive unit.
6	Perform the procedure "Halting (shutting down) an SST unit" (page 74) on the active unit. 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 the procedure "Powering off an SST unit" (page 122) 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 SST 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 SST 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 the default time of 1:00 AM each day. Refer to "[Rescheduling backup time](#)" (page 118) to customize the time of automatic backup. In addition, 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
"Backing up the SST" (page 116)

Individual procedures

ATTENTION

Although many of the modular procedures 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, in the overview section of this NTP for complete instructions for performing high level tasks.

Querying current number of SIP calls

Purpose of this procedure

Use this procedure to determine how many SIP calls are currently being processed by the SST 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

Step	Action
------	--------

At the CS 2000 Session Server Launch Point

- 1 Select **Carrier VoIP Communication Server 2000 Session Server Manager** from the launch point menu.

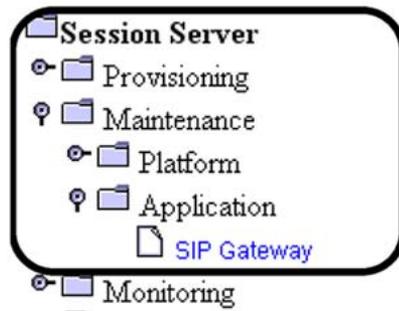
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

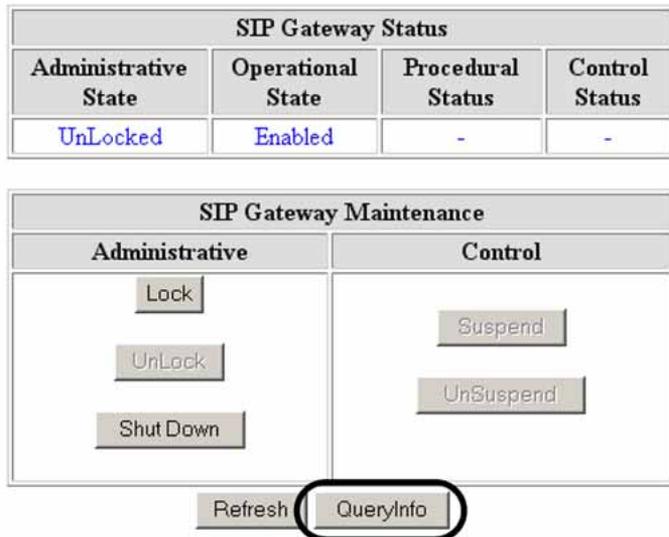
[Succession Communication Server 2000 NCGL Platform Manager](#)

[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.
 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.

Refresh

QueryInfo

Last Performed Operation: Query Number of Calls

Result: Passed

Number Of Active Calls: 0

Units #0 and #1 are: In Sync

—End—

Logging in remotely 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

Step	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.

—End—

Accessing SST/NCGL GUIs or CLI using the IEMS

Purpose of this procedure

This procedure describes how to access the SST 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 SST, 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 SST 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 SST each validate login information individually.

Prerequisites

The SST must be configured for access from the IEMS.

Action

If you want to access the active SST unit user interfaces (the unit currently controlling the node), use procedure "[Accessing the active SST unit user interfaces](#)" (page 32)

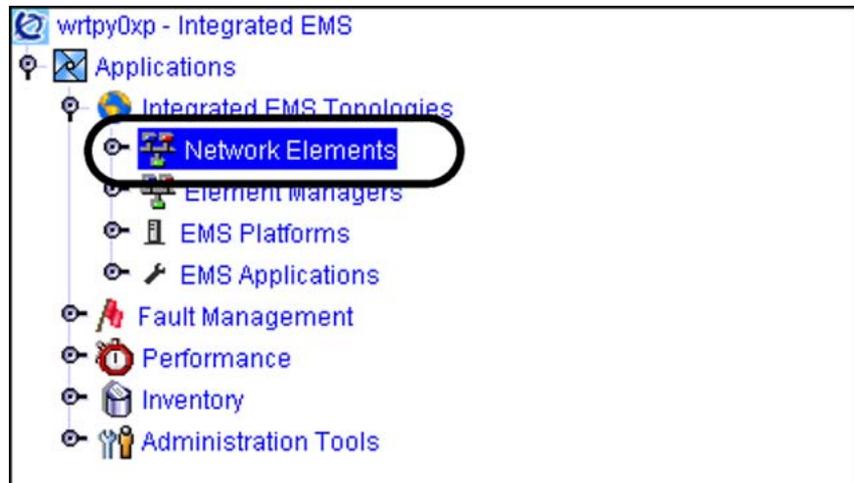
If you want to access the inactive SST unit user interfaces, use procedure "[Accessing the inactive Session Server unit user interfaces](#)" (page 36)

Accessing the active SST unit user interfaces

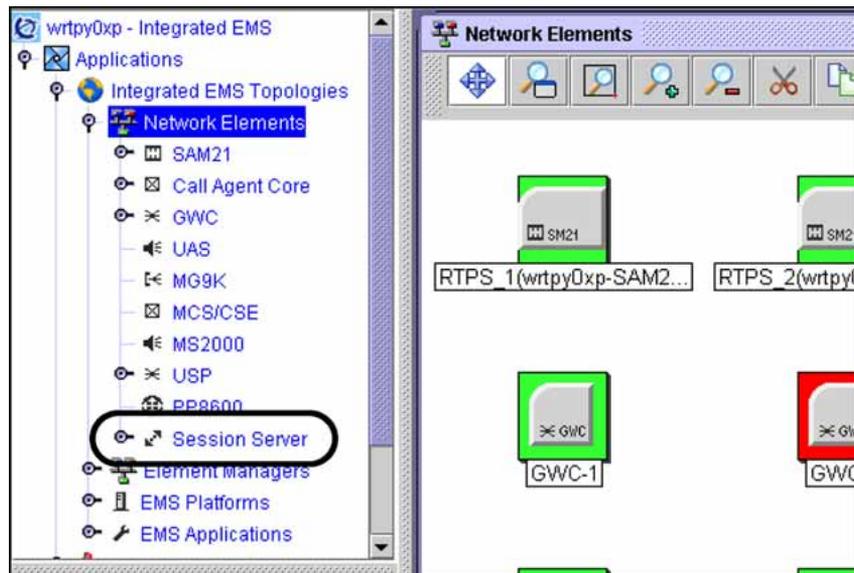
Step	Action
------	--------

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.



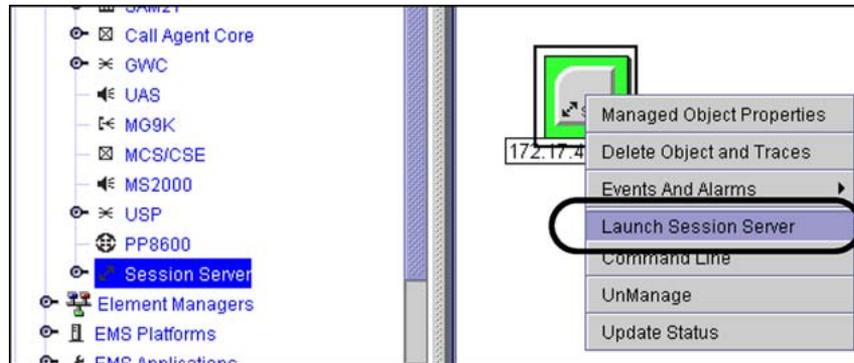
- 3 In the Network Elements view locate and click the **Session Server** element.



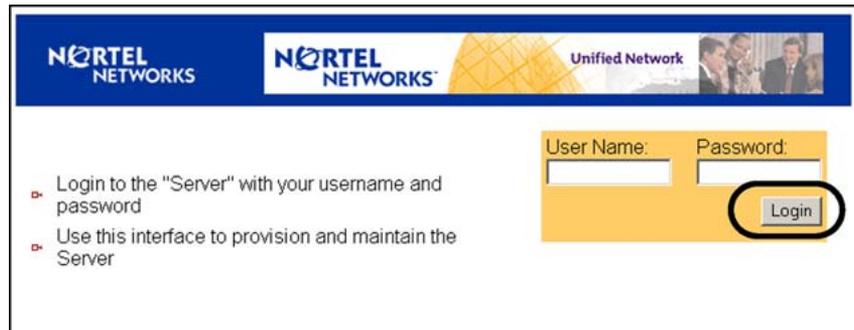
- 4 Use the following table to determine your next step.

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

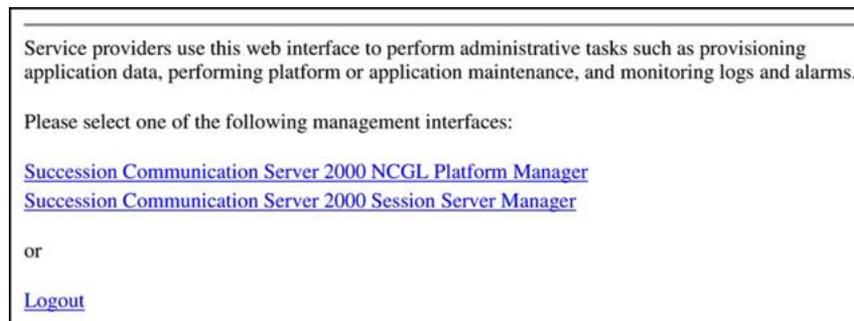
- 5 To launch either of the active unit Session Server GUIs, right-click on the Session Server Node icon and select **Launch Session Server**.



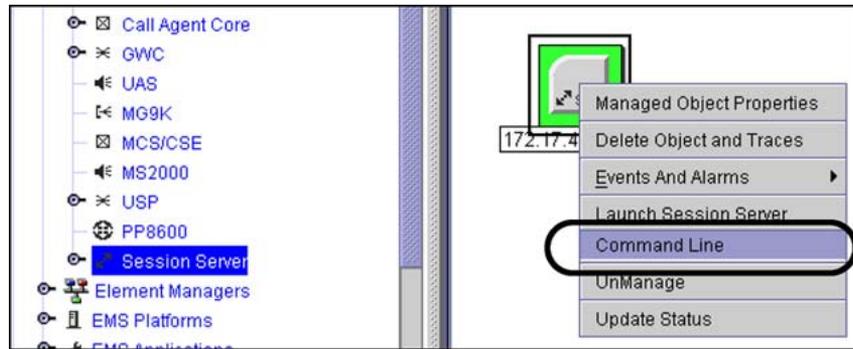
- 6 Confirm any security alerts.
- 7 At the login screen enter your user id and password, then click the **Login** button.



- 8 Select the GUI you want to launch from the **launch point** menu.



- 9 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.

- 10 If prompted to log onto the CS 2000 Management Tools server, enter the user id and password for the maintenance user.
- 11 At the login prompt enter the Session Server mtc user id and password.

—End—

Accessing the inactive SST 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.

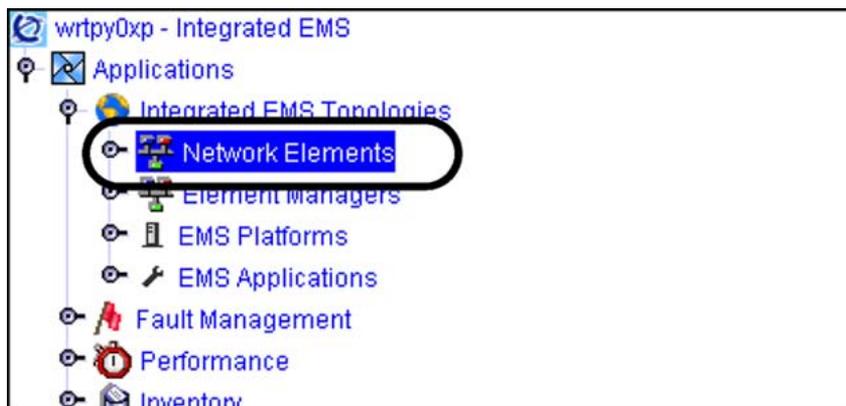
Session Server Status - Connected to Unit #1		
Unit Number	Activity State	Operational State
0	Inactive	Enabled
1	Active	Enabled

Accessing the inactive Session Server unit user interfaces

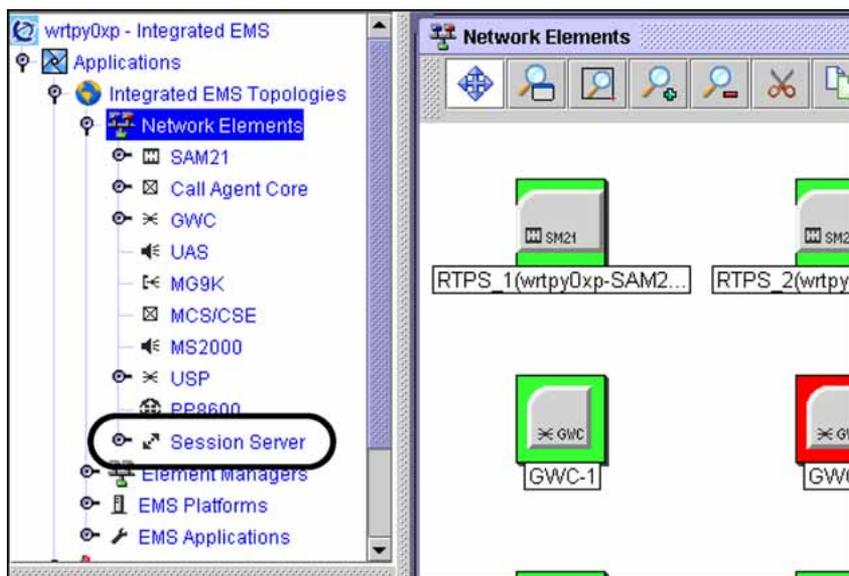
Step	Action
------	--------

At a workstation or console running the IEMS client

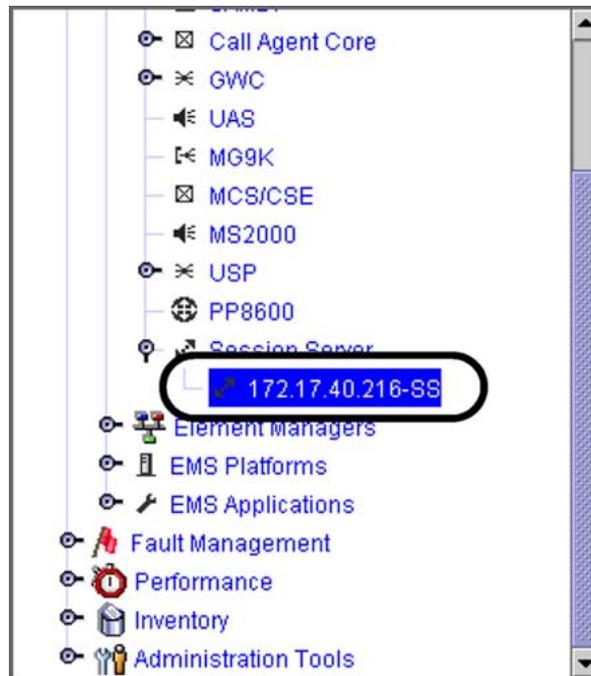
- 1 If necessary, log into the IEMS Java Webstart Client.
- 2 Select the **Network Elements** view.



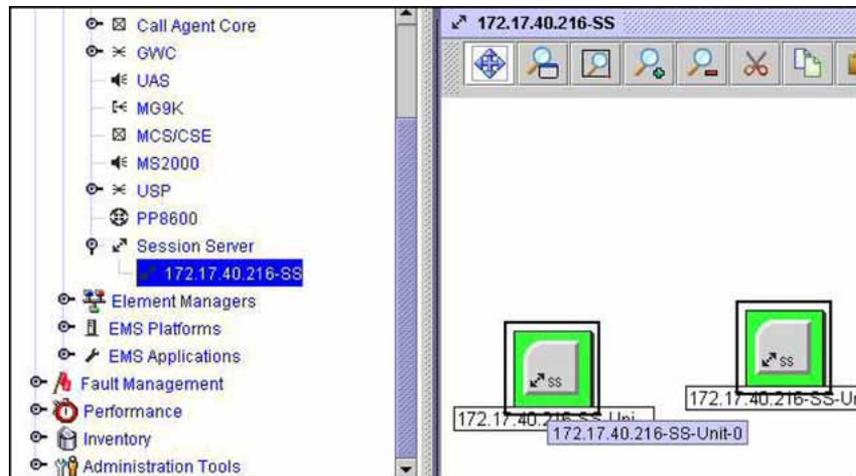
- 3 In the Network Elements view, locate and click the Session Server element.



- 4 Double-click on the Session Server IP address.



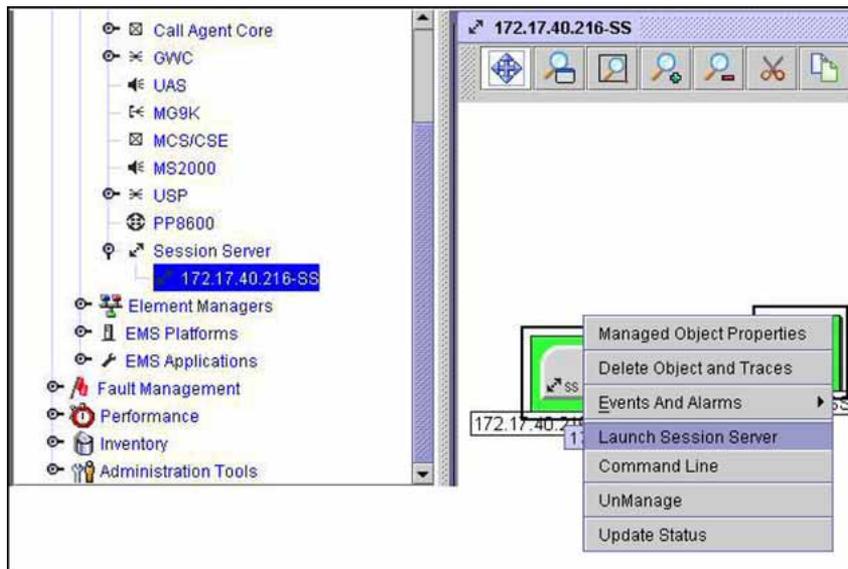
- 5 Hold the mouse pointer over the first Session Server unit icon and note its unit number. Do the same for the second unit icon.



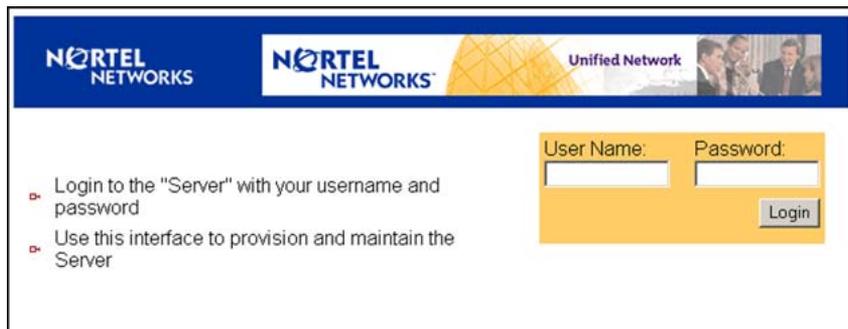
- 6 Use the following table to determine your next step.

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**.



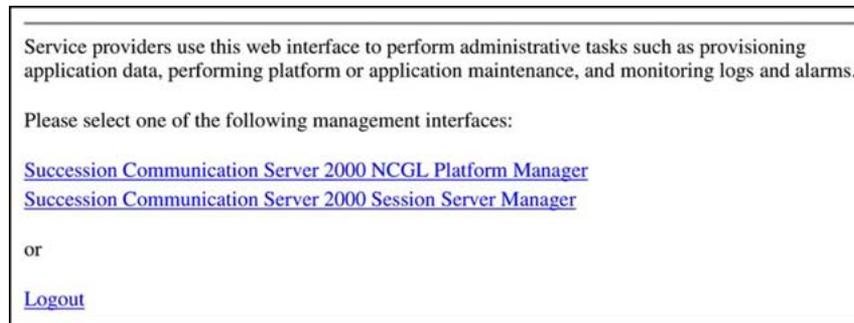
- 8 At the login screen enter your user id and password, then click the **Login** button.



- 9 Select the **Carrier VoIP Communication Server 2000 NCGL Platform Manger** link.

ATTENTION

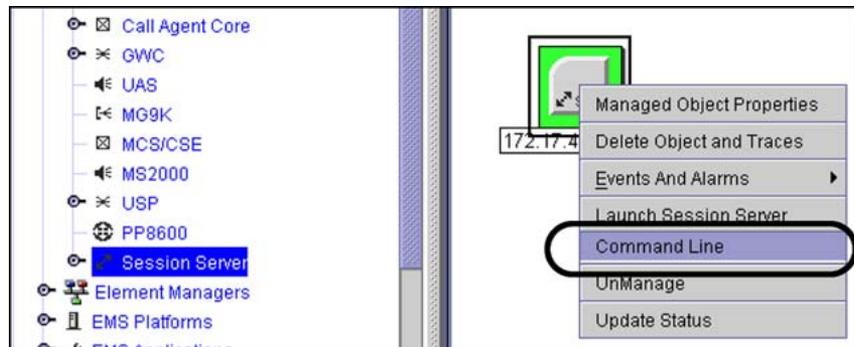
You can not access the CS 2000 Session Server Manager GUI from the inactive unit. You can only access the CS 2000 Session Server Manager GUI from the active unit. Clicking on the CS 2000 Session Server Manager GUI link from the *inactive* unit launch point will automatically take you to the CS 2000 Session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



- 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.

Unit	Activity	Jam	State	Connectivity	Host Name	Last Update T
0	Inactive	no	.	.	sp2k-1	01:45:44

- 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. The procedure is complete.
the unit you have logged onto is not the inactive unit	log off from this (active) unit, return to step 7 and select the other Session Server unit icon.

—End—

Accessing SST/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 SST.

Ensure that the SST 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 SST has not been properly configured for access through a web proxy. Refer to the procedure "Managing SPFS server web proxy setup for SST" in *Session Server Trunks Configuration Management (NN10338-511)* for instructions on configuring a web proxy to support access to the SST.

To perform provisioning of the SIP Application Gateway you must access the active SST 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 SST 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 Trunks Configuration Management (NN10338-511)* for this information.

Action

Step	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 SST 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

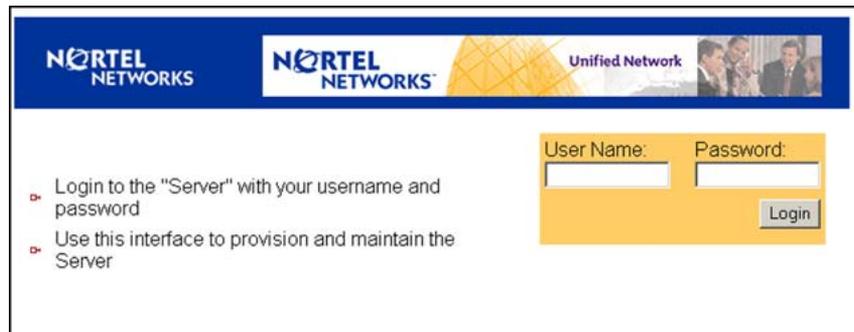
`SS_IP_address` is the IP address of the SST active or inactive unit

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.

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 SST 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.



—End—

Managing users on the SST platform

Purpose of this procedure

Use this procedure to add new users on an SST 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" (page 10).

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 SST. 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

Step	Action
------	--------

At a Session Server console interface or command line interface

- | | |
|---|--|
| 1 | Log onto the SST 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

- 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) SST unit.

**ATTENTION**

User accounts and passwords are not automatically propagated to the standby SST. 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.

---

—End—

---

# Managing user passwords using an SST 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 SST using the SST platform console command line interface (CLI).

## Limitations and Restrictions

### ATTENTION

User accounts and passwords are not automatically propagated to the standby SST. 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

| Step | Action |
|------|--------|
|------|--------|

***At a Session Server console interface or command line interface***

- 1 Open a secure shell to the SST by typing  
> `ssh -l <userid> <SS_IP_address>`

and pressing the Enter key.

where

`userid` is a valid userid (like mtc) on the SST  
`SS_IP_address` is the IP address or host name of the SST 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 SST. Perform account management activities such as setting up users, removing users, and changing passwords, on both units.

---

—End—

---

# Managing 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 SST using that user ID.

### ATTENTION

User accounts and passwords are not automatically propagated to the standby SST. 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

| Step | 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.

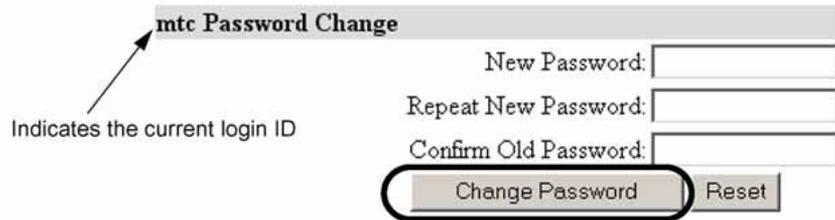
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

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.  
  
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 SST unit.

**ATTENTION**

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

---

—End—

---

---

## Invoking a maintenance SWACT of the SST 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.

#### ATTENTION

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](#)" (page 19).

### 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 "[Enabling a system SwAct \(Unjam\)](#)" (page 65) to unjam the unit.

Logins to the SST 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

| Step | Action |
|------|--------|
|------|--------|

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

- 1 Select Carrier VoIP 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 is displayed.*

- 3 Refer to the table in section "Additional status information" (page 54) 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                                                 |                                    |
|---------------------------------------------------------------------|------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="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**

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.

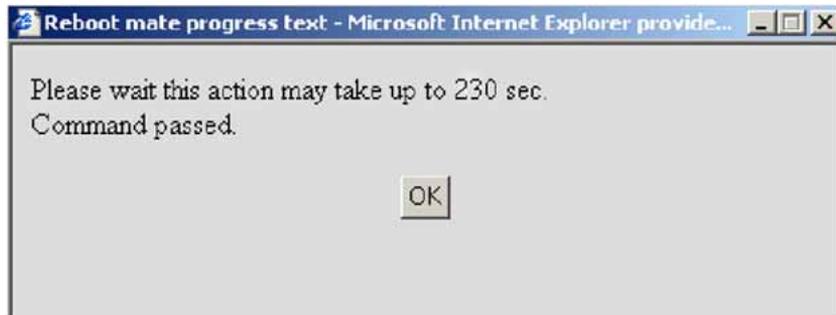
|                                                               |        |                                    |
|---------------------------------------------------------------|--------|------------------------------------|
| Enabled                                                       | Active | no                                 |
| <b>Maintenance Actions</b>                                    |        |                                    |
| <input type="checkbox"/> SWACT <input type="checkbox"/> Force |        | <input type="button" value="Jam"/> |

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

---

—End—

---

### 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.                                                                                                                                                              |

---

# Invoking 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 SST 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) SST unit is out of service. A SIP cold SwAct can only be performed when both the active and standby SST 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 "[Enabling a system SwAct \(Unjam\)](#)" (page 65) 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

| Step | Action |
|------|--------|
|------|--------|

**At the CS 2000 Session Server Launch Point**

- 1 Select **Carrier VoIP Communication Server 2000 Session Server Manager** from the launch point menu.

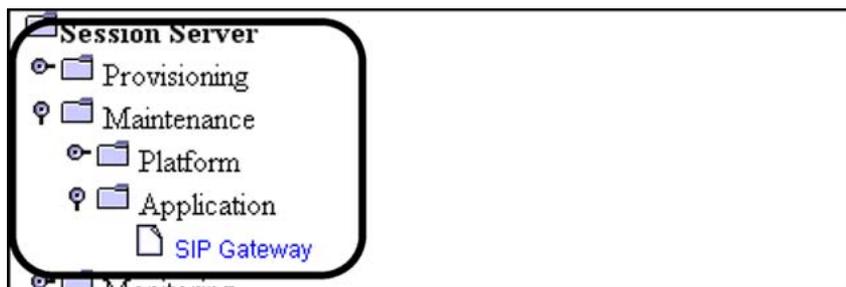
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

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           |

**SIP Gateway Status**

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

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

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

| SIP Gateway Maintenance                                                                                                  |                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Administrative                                                                                                           | Control                                                                            |
| <input type="button" value="Lock"/><br><input type="button" value="UnLock"/><br><input type="button" value="Shut Down"/> | <input type="button" value="Suspend"/><br><input type="button" value="UnSuspend"/> |
| <input type="button" value="Refresh"/> <input type="button" value="QueryInfo"/>                                          |                                                                                    |

|                                               |
|-----------------------------------------------|
| Last Performed Operation: Refresh             |
| Result: Passed                                |
| <input type="button" value="SIP Cold SwAct"/> |

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.



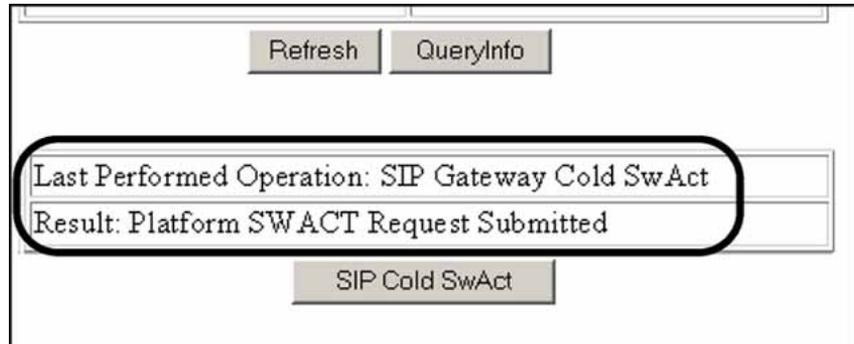
**CAUTION**

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

*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 *Session Server Trunks Fault Management* (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 the procedure "[View the operational status of the SIP Gateway application](#)" (page 85).

---

—End—

---

## Invoking 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 SST 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 SST units can be switched.

### Prerequisites

There are no prerequisites to using this procedure.

### Action

| Step | Action |
|------|--------|
|------|--------|

**At the CS 2000 Session Server Launch Point**

- 1 Select **Carrier VoIP 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 SST units.

| Unit 0 Links |             |             |             |             |
|--------------|-------------|-------------|-------------|-------------|
| Unit IP      | Active IP   | Port 0 IP   | Port 1 IP   | PTP IP      |
| 10.67.99.67  | 10.67.99.72 | 10.67.99.65 | 10.67.99.66 | 192.168.1.1 |
| Links        | Status      | Activity    | Maintenance |             |
| Link 0       | .           | Active      | Lock 0      | Swink       |
| Link 1       | .           | Inactive    | Lock 1      |             |
| PTP Links    | .           |             |             |             |

| Unit 1 Links |             |             |             |             |
|--------------|-------------|-------------|-------------|-------------|
| Unit IP      | Inactive IP | Port 0 IP   | Port 1 IP   | PTP IP      |
| 10.67.99.70  | 10.67.99.71 | 10.67.99.68 | 10.67.99.69 | 192.168.1.2 |
| Links        | Status      | Activity    |             |             |
| Link 0       | .           | Active      |             |             |
| Link 1       | .           | Inactive    |             |             |
| PTP Links    | .           |             |             |             |

- 4 Click the **Swink** button for the active link on the active unit.

| Unit 0 Links |             |             |             |        |
|--------------|-------------|-------------|-------------|--------|
| Unit IP      | Active IP   | Port 0 IP   | Port 1 IP   | PTP    |
| 10.67.99.67  | 10.67.99.72 | 10.67.99.65 | 10.67.99.66 | 192.16 |
| Links        | Status      | Activity    | Maintenance |        |
| Link 0       | .           | Active      | Lock 0      | Swink  |
| Link 1       | .           | Inactive    | Lock 1      |        |
| PTP Links    | .           |             |             |        |

| Unit 1 Links |             |             |             |        |
|--------------|-------------|-------------|-------------|--------|
| Unit IP      | Inactive IP | Port 0 IP   | Port 1 IP   | PTP    |
| 10.67.99.70  | 10.67.99.71 | 10.67.99.68 | 10.67.99.69 | 192.16 |
| Links        | Status      | Activity    |             |        |
| Link 0       | .           | Active      |             |        |
| Link 1       | .           | Inactive    |             |        |
| PTP Links    | .           |             |             |        |

*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.

| Unit 0 Links |             |             |             |        |
|--------------|-------------|-------------|-------------|--------|
| Unit IP      | Active IP   | Port 0 IP   | Port 1 IP   | PTP    |
| 10.67.99.67  | 10.67.99.72 | 10.67.99.65 | 10.67.99.66 | 192.16 |
| Links        | Status      | Activity    | Maintenance |        |
| Link 0       | .           | Active      | Lock 0      | Swink  |
| Link 1       | .           | Inactive    | Lock 1      |        |
| PTP Links    | .           |             |             |        |

—End—

## Inhibiting 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

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

| Step | Action |
|------|--------|
|------|--------|

#### *At the CS 2000 Session Server Manager or IEMS workstation*

- 1 Select Carrier VoIP 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 Yes, then the unit is already jammed and you are done with this procedure. If it is No, then continue with the next step.

| Unit 0          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Inactive | no        |

| Unit 1          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Active   | no        |

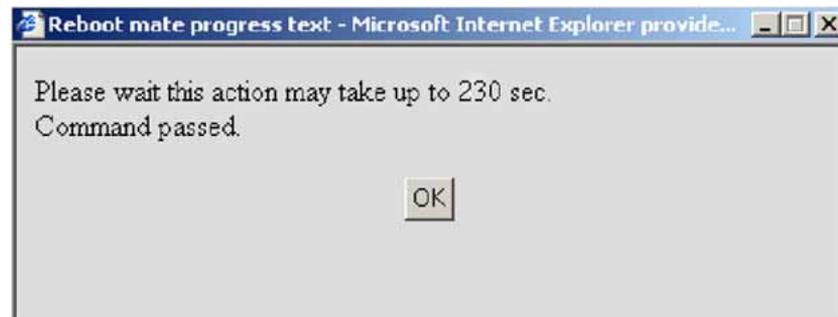
| Maintenance Actions                                                 |                                                                   |
|---------------------------------------------------------------------|-------------------------------------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="Jam"/> <input type="checkbox"/> Force |

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

—End—

## 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 SST node could occur on the if the active unit fails.

## Enabling 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

| Step | Action |
|------|--------|
|------|--------|

#### *At the CS 2000 NCGL Platform Manager or IEMS client*

- 1 Select Carrier VoIP 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](#).

| Unit 0          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Inactive | yes       |

| Unit 1          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Active   | no        |

| Maintenance Actions                                                 |                                      |
|---------------------------------------------------------------------|--------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="Unjam"/> |

- 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 Jlnact alarm clears.*

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

—End—



## Locking network Ethernet link

### Purpose of this procedure

This procedure is used to lock (shut down) the inactive Ethernet link on an SST unit, preventing a switch of link activity (Swlnk) to the inactive link. These links allow the SST 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 SST node from operating in a fully fault-tolerant mode.

### Prerequisites

There are no prerequisites to using this procedure.

### Action

| Step | Action |
|------|--------|
|------|--------|

#### *At the CS 2000 Session Server Launch Point*

- 1 Select **Carrier VoIP 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 SST units.

| Unit 0 Links |             |             |             |             |
|--------------|-------------|-------------|-------------|-------------|
| Unit IP      | Active IP   | Port 0 IP   | Port 1 IP   | PTP         |
| 10.67.99.67  | 10.67.99.72 | 10.67.99.65 | 10.67.99.66 | 192.168.1.1 |
| Links        | Status      | Activity    | Maintenance |             |
| Link 0       | .           | Active      | Lock 0      | Swink       |
| Link 1       | .           | Inactive    | Lock 1      |             |
| PTP Links    |             |             |             |             |

| Unit 1 Links |             |             |             |             |
|--------------|-------------|-------------|-------------|-------------|
| Unit IP      | Inactive IP | Port 0 IP   | Port 1 IP   | PTP         |
| 10.67.99.70  | 10.67.99.71 | 10.67.99.68 | 10.67.99.69 | 192.168.1.2 |
| Links        | Status      | Activity    |             |             |
| Link 0       | .           | Active      |             |             |
| Link 1       | .           | Inactive    |             |             |
| PTP Links    |             |             |             |             |

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

| Unit 0 Links |             |             |             |             |
|--------------|-------------|-------------|-------------|-------------|
| Unit IP      | Active IP   | Port 0 IP   | Port 1 IP   | PTP         |
| 10.67.99.67  | 10.67.99.72 | 10.67.99.65 | 10.67.99.66 | 192.168.1.1 |
| Links        | Status      | Activity    | Maintenance |             |
| Link 0       | .           | Active      | Lock 0      | Swink       |
| Link 1       | .           | Inactive    | Lock 1      |             |
| PTP Links    |             |             |             |             |

The system responds:

Info: Lock Link X - Command passed.

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

| Unit 1 Links |             |             |             |             |
|--------------|-------------|-------------|-------------|-------------|
| Unit IP      | Inactive IP | Port 0 IP   | Port 1 IP   | PTP IP      |
| 10.67.99.70  | 10.67.99.72 | 10.67.99.68 | 10.67.99.69 | 192.168.1.2 |
| Links        | Status      | Activity    | Maintenance |             |
| Link 0       | .           | Active      | Lock 0      | Swink       |
| Link 1       | M           | Inactive    | Unlock 1    |             |
| PTP Links    |             |             |             |             |

—End—



## Unlocking network Ethernet link

### Purpose of this procedure

This procedure is used to unlock (start) an SST 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

| Step                                              | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>At the CS 2000 Session Server Launch Point</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 1                                                 | Select <b>Carrier VoIP Communication Server NCGL Platform Manager</b> from the launch point menu.                                                                                                                                                                                                                                                                                                                                                                                                      |
|                                                   | <div style="border: 1px solid black; padding: 5px;"> <p>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.</p> <p>Please select one of the following management interfaces:</p> <p><a href="#">Succession Communication Server 2000 NCGL Platform Manager</a><br/> <a href="#">Succession Communication Server 2000 Session Server Manager</a></p> </div> |
| 2                                                 | Click the <b>Network Connectivity</b> link.<br><i>The Network Connectivity page is displayed.</i>                                                                                                                                                                                                                                                                                                                                                                                                      |
| 3                                                 | Review the link state of the active SST unit.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Unit 0 Links |             |             |             |             |
|--------------|-------------|-------------|-------------|-------------|
| Unit IP      | Inactive IP | Port 0 IP   | Port 1 IP   | PTP IP      |
| 10.67.99.67  | 10.67.99.71 | 10.67.99.65 | 10.67.99.66 | 192.168.1.1 |
| Links        | Status      | Activity    |             |             |
| Link 0       | Unavailable | Unavailable |             |             |
| Link 1       | Unavailable | Unavailable |             |             |
| PTP Links    | Disabled    |             |             |             |

| Unit 1 Links |             |             |             |             |
|--------------|-------------|-------------|-------------|-------------|
| Unit IP      | Active IP   | Port 0 IP   | Port 1 IP   | PTP IP      |
| 10.67.99.70  | 10.67.99.72 | 10.67.99.68 | 10.67.99.69 | 192.168.1.2 |
| Links        | Status      | Activity    | Maintenance |             |
| Link 0       | .           | Active      | Lock 0      | Swink       |
| Link 1       | M           | Inactive    | Unlock 1    |             |
| PTP Links    | S           |             |             |             |

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

| Unit 1 Links |             |             |             |             |
|--------------|-------------|-------------|-------------|-------------|
| Unit IP      | Active IP   | Port 0 IP   | Port 1 IP   | PTP IP      |
| 10.67.99.70  | 10.67.99.72 | 10.67.99.68 | 10.67.99.69 | 192.168.1.2 |
| Links        | Status      | Activity    | Maintenance |             |
| Link 0       | .           | Active      | Lock 0      | Swink       |
| Link 1       | M           | Inactive    | Unlock 1    |             |
| PTP Links    | S           |             |             |             |

*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**

| Unit 0 Links |             |             |                                       |                                      |
|--------------|-------------|-------------|---------------------------------------|--------------------------------------|
| Unit IP      | Active IP   | Port 0 IP   | Port 1 IP                             | PTP                                  |
| 10.67.99.67  | 10.67.99.72 | 10.67.99.65 | 10.67.99.66                           | 192.168                              |
| Links        | Status      | Activity    | Maintenance                           |                                      |
| Link 0       | .           | Active      | <input type="button" value="Lock 0"/> | <input type="button" value="Swink"/> |
| Link 1       | .           | Inactive    | <input type="button" value="Lock 1"/> |                                      |
| PTP Links    | .           |             |                                       |                                      |

—End—

## Halting (shutting down) an SST unit

### Purpose of this procedure

This procedure is used to perform a graceful shutdown an SST 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 SST unit.

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



#### CAUTION

This procedure halts all call processing activity and billing record generation on the affected unit, and prevents the SST 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](#)" (page 89) to check for any disk array rebuilds in progress. Wait for the rebuild to complete before executing this procedure.

### Action

| Step | Action |
|------|--------|
|------|--------|

#### *At the Session Server GUI or IEMS client*

- 1 Select **Carrier VoIP 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.

| Bootload Management                       |          |                                         |                  |      |
|-------------------------------------------|----------|-----------------------------------------|------------------|------|
| Bootload                                  |          |                                         | Maintenance      |      |
| 5.20.1.0.0405122209                       |          |                                         | Default Bootload |      |
| Software Upgrade                          |          |                                         |                  |      |
| Protocol                                  | Login ID | Password                                | IP address       | File |
|                                           |          |                                         |                  |      |
| Server Maintenance                        |          |                                         |                  |      |
| Unit 0 - Active                           |          |                                         |                  |      |
| Reboot <input type="checkbox"/> Force     |          | Halt <input type="checkbox"/> Force     |                  |      |
| Unit 1 - Inactive                         |          |                                         |                  |      |
| RebootMate <input type="checkbox"/> Force |          | HaltMate <input type="checkbox"/> Force |                  |      |

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

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

#### ATTENTION

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.

| 5.20.1.0.0405122209                       |          |                                         | Default Bootload |      |
|-------------------------------------------|----------|-----------------------------------------|------------------|------|
| Software Upgrade                          |          |                                         |                  |      |
| Protocol                                  | Login ID | Password                                | IP address       | File |
|                                           |          |                                         |                  |      |
| Server Maintenance                        |          |                                         |                  |      |
| Unit 0 - Active                           |          |                                         |                  |      |
| Reboot <input type="checkbox"/> Force     |          | Halt <input type="checkbox"/> Force     |                  |      |
| Unit 1 - Inactive                         |          |                                         |                  |      |
| RebootMate <input type="checkbox"/> Force |          | HaltMate <input type="checkbox"/> Force |                  |      |

*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 SST 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 the procedure "[Powering off an SST unit](#)" ([page 122](#)) to disconnect power from the unit.

---

—End—

---

## 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 "[Limits and Restrictions](#)" ([page 65](#)) apply to using this procedure.

---

#### Step Action

---

*At Session Server CLI or IEMS client*

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

```
mtcli haltmate
```

 (to shutdown the inactive unit)  
 or  

```
mtcli halt
```

 (to shutdown the active unit operating in simplex mode)  
 and pressing the **Enter** key.
- 3 If applicable, complete the procedure "[Powering off an SST unit](#)" ([page 122](#)) to disconnect power from the unit.

---

—End—

---

## Rebooting 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

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 "[Viewing the operational status of the NCGL platform](#)" (page 89) 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

| Step                                                                           | Action                                                                                            |
|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <i>At the CS 2000 NCGL Platform Manager or IEMS client for the active unit</i> |                                                                                                   |
| 1                                                                              | Select <b>Carrier VoIP Communication Server NCGL Platform Manager</b> 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.

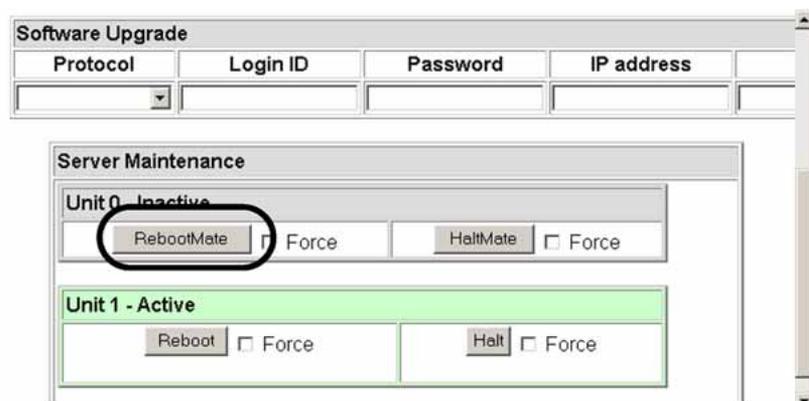
*The Administration page is displayed.*

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

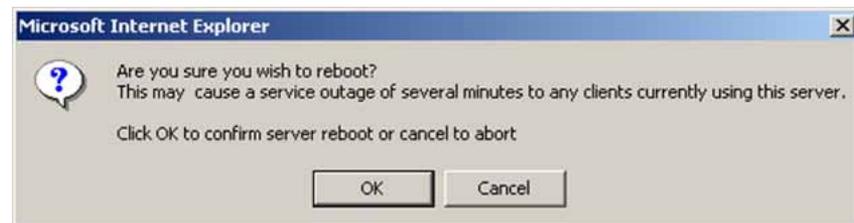
- 4 Click RebootMate to reboot the inactive unit, or Reboot to reboot the active unit.

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

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

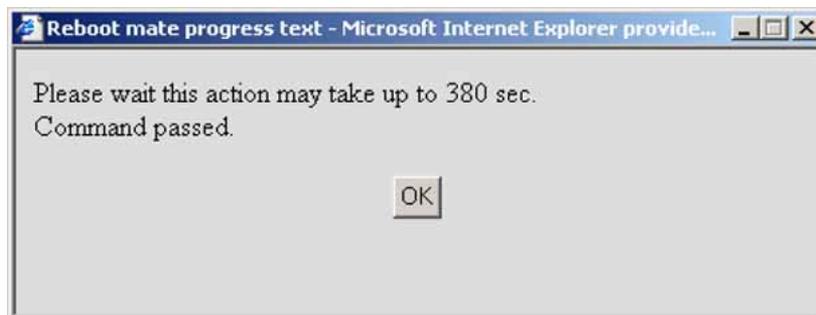


*The system responds with the following message box. If pop up windows are disabled in the web browser, the message box does not appear.*



- 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 "[Viewing the operational status of the NCGL platform](#)" (page 89) 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.

| Unit | Activity | Jam | State         | Connectivity | Host Name      | Last Update Time |
|------|----------|-----|---------------|--------------|----------------|------------------|
| 1    | Active   | no  | simple<br>3M+ | MatCon<br>M  | rtpsngss1unit1 | 01:52:38         |

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

—End—

## Alternate command line interface (CLI) method



### CAUTION

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 "[Limitations and Restrictions](#)" (page 78) apply when using this procedure.

---

| Step                              | Action                                                                                                                                                                                    |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>At NCGL CLI or IEMS client</b> |                                                                                                                                                                                           |
| 1                                 | Log on to the active unit and change to the root user.                                                                                                                                    |
| 2                                 | Reboot the selected unit by typing<br><pre># mtccli rebootmate (to reboot the inactive unit)</pre> or<br><pre># mtccli reboot (to reboot the active unit operating in simplex mode)</pre> |
| 3                                 | Use procedure " <a href="#">Viewing the operational status of the NCGL platform</a> " (page 89) to confirm the recovery of the unit after reboot.                                         |
| 4                                 | If applicable, return to the higher level task flow or procedure that directed you to this procedure.                                                                                     |

---

—End—

---

## 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](#)" (page 80).

**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.

## Verifying 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

| Step | Action |
|------|--------|
|------|--------|

*At the CS 2000 Session Server Manager or IEMS client*

- 1 Select **Carrier VoIP Communication Server 2000 Session Server Manager** from the launch point menu.

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

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select **Session Server > 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.

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

| SIP Gateway Maintenance                    |                                 |
|--------------------------------------------|---------------------------------|
| Administrative                             | Control                         |
| <p>Lock</p> <p>UnLock</p> <p>Shut Down</p> | <p>Suspend</p> <p>UnSuspend</p> |
| Refresh                                    | QueryInfo                       |

- 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.

|                                                 |
|-------------------------------------------------|
| Last Performed Operation: Query Number of Calls |
| Result: Passed                                  |
| Number Of Active Calls: 0                       |
| SIP Gateway is: In Sync                         |
| SIP Gateway Cold SwAct                          |

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

—End—

## Viewing the operational status of the SIP Gateway application

### Purpose of this procedure

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

### Limitations and restrictions

This procedure provides instructions for determining the service status of the SIP Gateway application software only. For instructions on determining the status of the platform and operating system, refer to procedure "[Viewing the operational status of the NCGL platform](#)" (page 89).

### Prerequisites

There are no prerequisites for this procedure.

### Action

| Step | Action |
|------|--------|
|------|--------|

***At the CS 2000 Session Server Manager or IEMS client***

- 1 Select Carrier VoIP Communication Server 2000 Session Server Manager from the launch point menu.

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

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

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



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

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

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

| SIP Gateway Maintenance                                                                                                  |                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Administrative                                                                                                           | Control                                                                            |
| <input type="button" value="Lock"/><br><input type="button" value="UnLock"/><br><input type="button" value="Shut Down"/> | <input type="button" value="Suspend"/><br><input type="button" value="UnSuspend"/> |
| <input type="button" value="Refresh"/> <input type="button" value="QueryInfo"/>                                          |                                                                                    |

|                                   |
|-----------------------------------|
| Last Performed Operation: Refresh |
| Result: Passed                    |

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

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](#)" (page 87) to review the description of the various fields of this view.

For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section of "[Interpreting SIP Gateway application states](#)" (page 17).

- 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.

|                                                 |
|-------------------------------------------------|
| Last Performed Operation: Query Number of Calls |
| Result: Passed                                  |
| Number Of Active Calls: 0                       |
| SIP Gateway is: In Sync                         |
| SIP Gateway Cold SwAct                          |

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

—End—

## Interpreting SIP Gateway application status and maintenance fields

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

### Node status field descriptions

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

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

#### SIP Gateway application Status field descriptions

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

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

#### SIP Gateway Maintenance field descriptions and interpretation of service states

| Administrative State | Operational State | Procedural Status | Control Status | DMS style Service States         |
|----------------------|-------------------|-------------------|----------------|----------------------------------|
| Locked               | Disabled          | -                 | Suspended      | Offline (OFFL)                   |
| Locked               | Enabled           | -                 | -              | Manual Busy(MANB)                |
| Locked               | Enabled           | Terminating       | -              | Manual Busy Transitioning(MANBP) |
| Unlocked             | Enabled           | -                 | -              | In Service(INSV)                 |
| Unlocked             | Disabled          | -                 | -              | System Busy(SYSB)                |
| Shutting Down        | Enabled           | -                 | -              | Going out of service(INSVD)      |

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

## Viewing the operational status of the NCGL platform

### Purpose of this procedure

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

### Limitations and restrictions

This procedure provides instructions for determining the service status of the SST NCGL platform only. For instructions on determining the status of the SIP Gateway application, refer to "[Viewing the operational status of the SIP Gateway application](#)" (page 85).

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 NCGL 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

| Step | Action |
|------|--------|
|------|--------|

***At the CS 2000 NCGL Platform Manager or IEMS client***

- |   |                                                                                                 |
|---|-------------------------------------------------------------------------------------------------|
| 1 | Select Carrier VoIP Communication Server 2000 NCGL Platform Manager from the launch point menu. |
|---|-------------------------------------------------------------------------------------------------|

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

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

*The Platform Main Page menu is displayed.*

## 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 <a href="#">step 3</a> .                                                                                  |
| you want to review existing platform alarms                                                                    | Go to <a href="#">step 17</a> and go to procedure "Viewing SST alarms" in <i>Session Server Trunks Fault Management</i> (NN10332-911).                |
| you want to review node maintenance status                                                                     | Click the Node Maintenance link and go to <a href="#">step 5</a> .                                                                                    |
| 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 <a href="#">step 7</a> .                                                                                       |
| you want to review the connectivity status of the network links.                                               | Click the Network Connectivity link and go to <a href="#">step 9</a> .                                                                                |
| you want to review storage related information including array status, disk capacity and disk alarm thresholds | Click the Disk Services link and go to <a href="#">step 10</a> .                                                                                      |
| you want to review details about platform services including the network time protocol servers                 | Click the Services link and go to <a href="#">step 12</a> .                                                                                           |
| you want to review platform version information only                                                           | Click the Administration link and go to <a href="#">step 14</a> .                                                                                     |
| you want to review customer logs                                                                               | Go to <a href="#">step 17</a> and refer to <i>Session Server Trunks Fault Management</i> (NN10332-911).                                               |
| you want to change root passwords                                                                              | Go to <a href="#">step 17</a> and refer to "Managing user passwords with the Session Server GUI" (page 49).                                           |
| you want to view TLS security information or manage security certificates                                      | Go to <a href="#">step 17</a> and refer to "Managing TLS Security Parameters" in <i>Session Server Trunks Configuration Management</i> (NN10338-511). |
| you are finished reviewing information and want to log out from the GUI                                        | <a href="#">step 16</a> .                                                                                                                             |

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

### ATTENTION

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

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

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

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

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

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

- 4 When you have completed reviewing System Information page, return to [step 2](#).
- 5 Review the Node Maintenance page and use the following table to review the description of the various fields of the Node Maintenance page:

The Node Maintenance panel updates every 45 seconds  
Datestamp of last update: Wednesday April 06th 2005 09:19:40 AM EDT

| Unit 0          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Inactive | no        |

| Unit 1          |          |           |
|-----------------|----------|-----------|
| Operation State | Activity | Jam State |
| Enabled         | Active   | no        |

| Maintenance Actions                                                 |                                                                   |
|---------------------------------------------------------------------|-------------------------------------------------------------------|
| <input type="button" value="SWACT"/> <input type="checkbox"/> Force | <input type="button" value="Jam"/> <input type="checkbox"/> Force |

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 the maintenance and manual cold SWACT procedures in this document. |

- 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            | Major alarm threshold            | Critical alarm threshold            |
| 2.20                        | 1.99                         | 1.86                         | 5 min.                           | 20 min.                          | 30 min.                             |
|                             |                              |                              | 95.00%                           | 99.00%                           | 99.00%                              |
| Process Information         |                              |                              |                                  |                                  |                                     |
| Number of processes         | Number of zombie process(es) | Zombie                       |                                  |                                  |                                     |
|                             |                              | Minor alarm threshold value  | Major alarm threshold value      | Critical alarm threshold value   |                                     |
| 192                         | 1                            | 5                            | 10                               | 15                               |                                     |
| Memory Information          |                              |                              |                                  |                                  |                                     |
| Total memory (MB)           | Free memory (MB)             | Available memory (MB)        | Minor alarm threshold value (MB) | Major alarm threshold value (MB) | Critical alarm threshold value (MB) |
| 3,790.29                    | 2,945.21                     | 3,294.78                     | 500.00                           | 250.00                           | 100.00                              |

The Chassis Information panel is not automatically refreshed.

| Field                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Chassis information: Self Test                          | status of the self test performed on the platform at boot up                                                                                                                                                                                                                                                                                                                                      |
| Chassis 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 SST Platform                                                                                                                                                                                                                                                                                                                     |
| Process Information: Number of zombie processes         | number of defunct or terminated NCGL zombie processes<br><br><b>Note:</b> A zombie process is a process that has terminated either because it has been killed by a signal or because it has called an <code>exit()</code> 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                                                                                                                                                                                                                                                |
| 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                                                                                                                                                                                                                                                |

| Field                                                      | Description                                                                                                                                           |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 SST 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                      |

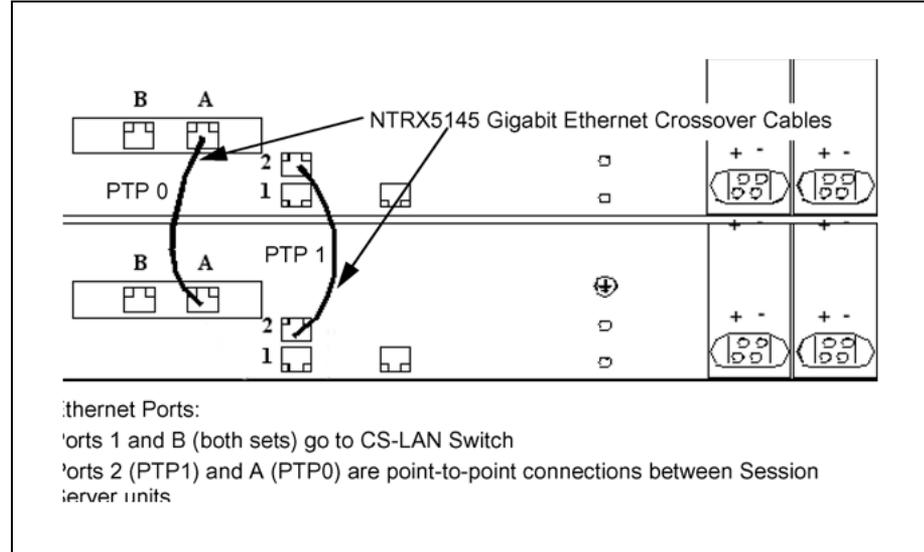
- 8 When you have completed reviewing the System Status, return to [step 2](#).
- 9 Review the Network Connectivity page and use the following table to review the description of the various fields of the Network Connectivity page:

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        | Swink       |
| 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 Swink |
| Unit 0,1 PTP Links status | status of the PTP links between both units in the node                                                      |
| Unit IP                   | network IP address of the SST unit                                                                          |
| Active IP                 | IP address of the local (active) SST unit                                                                   |
| Inactive IP               | IP address of the mate (inactive) SST unit                                                                  |
| Port 0 IP                 | IP address of the active or inactive Ethernet port 0                                                        |
| Port 1 IP                 | IP address of the active or inactive Ethernet port 1                                                        |
| PTP IP                    | IP address of the active or inactive PTP link                                                               |

**Crossover and LAN Ethernet cable connections for SST units**

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

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

To create and remove file systems, refer to 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                 | 95.00                | 0.00                       | 0.00                      | 85.00                     | 95.00                     | 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/sawd             | .            | 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                             |                                                  |
|------------------------------------------------------|--------------------------------------------------|
| <input type="button" value="Create New Filesystem"/> | <input type="button" value="Remove Filesystem"/> |

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

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

| Field                                              | Description                                                                                                                                                                                           |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RAID Array Status: Status                          | Indicates the status of the array. Values are:<br>- The array is operating normally<br>- Missing<br>- Failed<br>- 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                                                                                                                                          |
| 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                                                               |

| Field                                                   | Description                                                                                                                                |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Filesystem Information:<br>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:<br>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:<br>Volume Group Name          | name of the volume group in the array                                                                                                      |
| Volume Group Information:<br>Volume Group Size (GB)     | total size of the volume group in the array                                                                                                |
| Volume Group Information:<br>Total Space Allocated (GB) | amount of volume group space, in gigabytes, currently allocated to filesystems                                                             |
| Volume Group Information:<br>Total Space Allocated (%)  | amount of volume group space (in %) currently allocated to filesystems                                                                     |
| Volume Group Information:<br>Total Space Available (GB) | amount of unallocated volume group space, in gigabytes, available for filesystems                                                          |
| Volume Group Information:<br>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:

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<br>in sync | 47.140.206.50<br>in sync | undefined | 2                       | 2                  | 2                    |

| Field                                                           | Description                                                                                                       |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Network Services:<br>Number of Active Command Line Sessions     | number of command line interface (CLI) sessions (both remote and local) on the unit                               |
| Network Services:<br>Number of Clients with Active Web Sessions | number of clients running one or more web GUI sessions                                                            |
| NTP Information:<br>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:<br>Total Number of Servers                     | number of NTP servers registered with the CS-LAN network                                                          |
| NTP Information:<br>Accessible Servers                          | number of NTP servers accessible to the SST                                                                       |
| NTP Information:<br>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:  
The Administration panel does not update automatically. Click the link again to update it.

| Bootload Management |  |                  |        |
|---------------------|--|------------------|--------|
| Bootload            |  | Maintenance      |        |
| 8.08.1.0.0502231439 |  | Default Bootload |        |
| 7.09.1.0.0502281015 |  | Set default      | Delete |
| 5.36.2.1.0411021023 |  | Set default      | Delete |

| Software Upgrade |          |          |            |
|------------------|----------|----------|------------|
| Protocol         | Login ID | Password | IP address |
|                  |          |          |            |

| Server Maintenance                        |                                         |
|-------------------------------------------|-----------------------------------------|
| <b>Unit 0 - Inactive</b>                  |                                         |
| RebootMate <input type="checkbox"/> Force | HaltMate <input type="checkbox"/> Force |
| <b>Unit 1 - Active</b>                    |                                         |
| Reboot <input type="checkbox"/> Force     | Halt <input type="checkbox"/> Force     |

| 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 bootloader 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.                                                              |
| Software Upgrade: Password       | If a password is required to access the upgrade platform load from another server in the network, a password can be entered here.                                                              |
| Software Upgrade: IP Address     | If it is required to access the upgrade platform load from another server in the network, an IP address can be entered here.                                                                   |

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

- 15** When you have completed reviewing the Administration page, return to [step 2](#), or continue with [step 16](#).
- 16** If you want to logout from CS 2000 NCGL Platform Manager, click the Logout button.  
*You are returned to the login page*
- 17** If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

---

## Locking the SIP Gateway application

---

### Purpose of this procedure

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

### Limitations and restrictions

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



#### CAUTION

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

### Prerequisites

There are no prerequisites for this procedure.

### Action

---

| Step | Action |
|------|--------|
|------|--------|

---

#### *At the CS 2000 Session Server Manager or IEMS client*

- 1 Select **Carrier VoIP Communication Server 2000 Session Server Manager** from the launch point menu.

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

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

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



- 3 In the SIP Gateway panel click the Lock button.

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

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

| SIP Gateway Maintenance                                                                                                                                                                                                                                                           |                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrative                                                                                                                                                                                                                                                                    | Control                                                                                                                                                                                               |
| <div style="text-align: center;"> <input type="button" value="Lock"/> </div> <div style="text-align: center; margin-top: 10px;"> <input type="button" value="UnLock"/> </div> <div style="text-align: center; margin-top: 10px;"> <input type="button" value="Shut Down"/> </div> | <div style="text-align: center; margin-top: 20px;"> <input type="button" value="Suspend"/> </div> <div style="text-align: center; margin-top: 10px;"> <input type="button" value="UnSuspend"/> </div> |

*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.

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

| SIP Gateway Maintenance                  |                                          |
|------------------------------------------|------------------------------------------|
| Administrative                           | Control                                  |
| <input type="button" value="Lock"/>      | <input type="button" value="Suspend"/>   |
| <input type="button" value="UnLock"/>    | <input type="button" value="UnSuspend"/> |
| <input type="button" value="Shut Down"/> |                                          |

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

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

---

—End—

---

# Unlocking the SIP Gateway application

## Purpose of this procedure

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

For more detailed information about SIP Gateway application services states and administrative functions, refer to "[Operational administration and maintenance of the SST platform and applications](#)" (page 16).

## 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 "[Viewing the operational status of the NCGl platform](#)" (page 89).

## Prerequisites

The active unit must be in a locked Administrative state. If it is not locked or you are uncertain of the state of the application, refer to procedure "[Locking the SIP Gateway application](#)" (page 104).

## Action

| Step | Action |
|------|--------|
|------|--------|

*At the CS 2000 Session Server Manager or IEMS client*

- 1 Select **Carrier VoIP Communication Server 2000 Session Server Manager** from the launch point menu.

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

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

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



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

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

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

| SIP Gateway Maintenance                                                         |                                 |
|---------------------------------------------------------------------------------|---------------------------------|
| Administrative                                                                  | Control                         |
| <p>Lock</p> <p><b>UnLock</b> (highlighted with a red oval)</p> <p>Shut Down</p> | <p>Suspend</p> <p>UnSuspend</p> |

- 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                                                                                |
| <input type="button" value="Lock"/><br><br><input type="button" value="UnLock"/><br><br><input type="button" value="Shut Down"/> | <input type="button" value="Suspend"/><br><br><input type="button" value="UnSuspend"/> |

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

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

---

—End—

---

## Suspending the SIP Gateway application

### Purpose of this procedure

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

For more detailed information about SIP Gateway application services states and administrative functions, refer to "[Interpreting SIP Gateway application states](#)" (page 17).

### Limitations and restrictions

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

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

### Prerequisites

The SIP Gateway application must previously have been locked. If it is not locked or you are uncertain of the state of the application, refer to procedure "[Locking the SIP Gateway application](#)" (page 104).

### Action

---

#### Step Action

---

*At the CS 2000 Session Server Manager or IEMS client*

- 1 Select **Carrier VoIP Communication Server 2000 Session Server Manager** from the launch point menu.

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

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

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



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

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

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

| SIP Gateway Maintenance                    |                                 |
|--------------------------------------------|---------------------------------|
| Administrative                             | Control                         |
| <p>Lock</p> <p>UnLock</p> <p>Shut Down</p> | <p>Suspend</p> <p>UnSuspend</p> |

- 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

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| Locked               | Disabled          | -                 | Suspended      |

| SIP Gateway Maintenance                                                                                                  |                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Administrative                                                                                                           | Control                                                                            |
| <input type="button" value="Lock"/><br><input type="button" value="UnLock"/><br><input type="button" value="Shut Down"/> | <input type="button" value="Suspend"/><br><input type="button" value="UnSuspend"/> |
| <input type="button" value="Refresh"/>                                                                                   | <input type="button" value="QueryInfo"/>                                           |

- 5 If applicable, restart the SIP Gateway application by executing procedures ["Unsuspending the SIP Gateway application"](#) (page 113) and ["Unlocking the SIP Gateway application"](#) (page 107), in the order shown.
- 6 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

—End—

---

# Unsuspending the SIP Gateway application

## Purpose of this procedure

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

For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section "[Interpreting SIP Gateway application states](#)" (page 17).

## Limitations and restrictions

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

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

## Prerequisites

The SIP Gateway application must previously have been suspended. If it is not suspended or you are uncertain of the state of the application, refer to procedure "[Suspending the SIP Gateway application](#)" (page 110).

## Action

---

### Step Action

---

#### *At the CS 2000 Session Server Manager or IEMS client*

- 1 Select **Carrier VoIP Communication Server 2000 Session Server Manager** from the launch point menu.

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

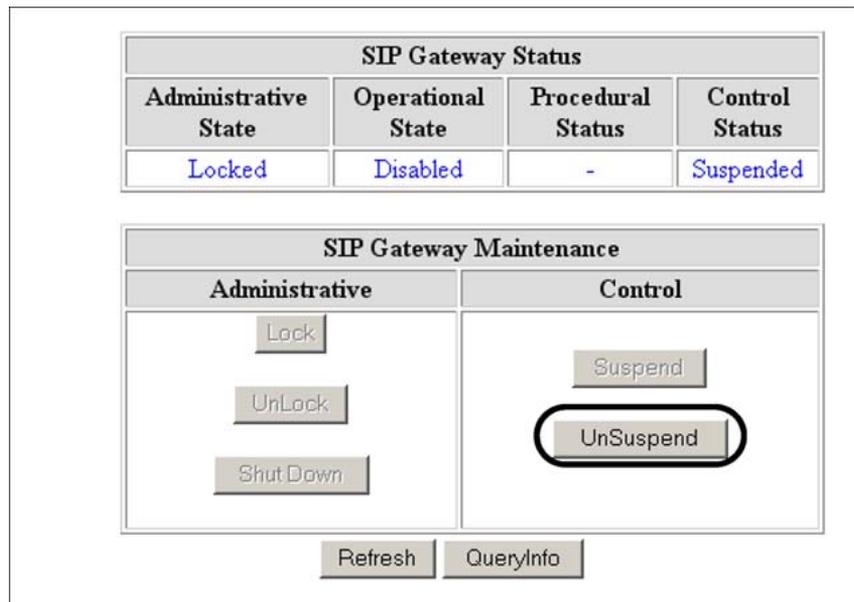
Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select **Session Server > 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                         |
| <p>Lock</p> <p>UnLock</p> <p>Shut Down</p> | <p>Suspend</p> <p>UnSuspend</p> |

- 5 If necessary, bring the SIP Gateway application back into service by executing procedure "Unlocking the SIP Gateway application" (page 107).
- 6 If applicable, return to the higher level task flow or procedure that directed you to this procedure.

—End—

## Backing up the SST

By default, the unit performs a backup of the database and critical files every day at 1:00 AM. Refer to ["Rescheduling backup time"](#) (page 118) 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 ["Backing up security related files manually"](#) (page 119).

### 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 ["Verifying synchronization status"](#) (page 83).

### Making a backup

Follow this procedure to make an immediate backup.

| Step | Action |
|------|--------|
|------|--------|

*At the NCGL CLI or IEMS 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/bkresmgr/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.

```

data/bkresmgr/temp/
data/bkresmgr/temp/gen_cert.txt
data/bkresmgr/temp/server.crt
data/bkresmgr/temp/trusted.crt
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_SSPPFS.jsp
data/bkresmgr/temp/redirect_no-SSPPFS.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 identified 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 "[Backing up security related files manually](#)" (page 119).
- 5 Repeat this procedure on the second unit.

---

—End—

---

**Rescheduling backup time**

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

---

| Step | Action |
|------|--------|
|------|--------|

---

***At the NCGL CLI or IEMS 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 editing.*

```
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 identified 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 backup file is created in the `/data/bkresmgr/backup` directory and that it is created at the new time, not the previously scheduled time.
- 7 Repeat this procedure on the second unit.

---

—End—

---

## Backing up security related files manually

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.

---

**Step Action**


---

**At the NCGL CLI or IEMS 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 <a href="#">Step 6</a> |
| 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.*

---

—End—

---

## Powering off an SST unit

### Purpose of this procedure

This is used to power off an SST 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 an SST 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 procedure "[Viewing the operational status of the NCGL platform](#)" (page 89) to verify that the unit to be shut down is not active.

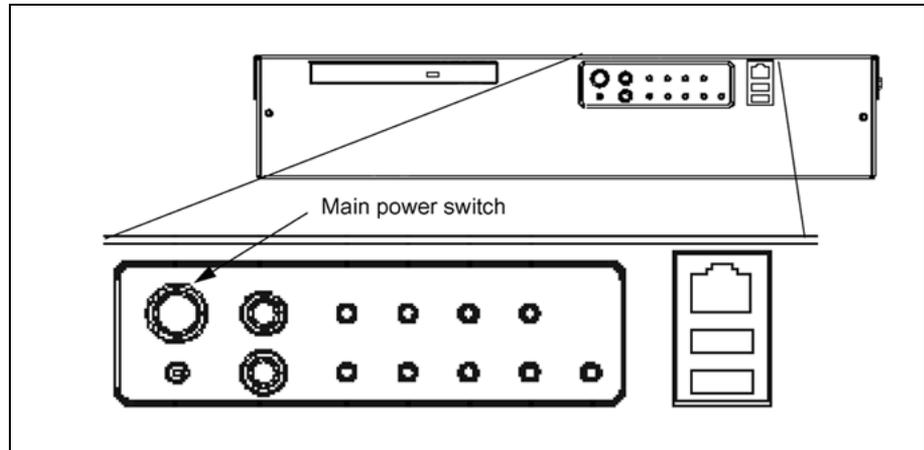
For information about the high-level activity, refer to the procedure "Performing a controlled shutdown of an SST node" in *Session Server Trunks Fault Management* (NN10332-911).

### Action

| Step | Action |
|------|--------|
|------|--------|

***At the front panel of the SST unit.***

- |   |                                                                                                                                     |
|---|-------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Complete the procedure " <a href="#">Halting (shutting down) an SST unit</a> " (page 74) 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. |



—End—

## Powering on and booting an SST unit

### Purpose of this procedure

This procedure is used to power on an SST 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

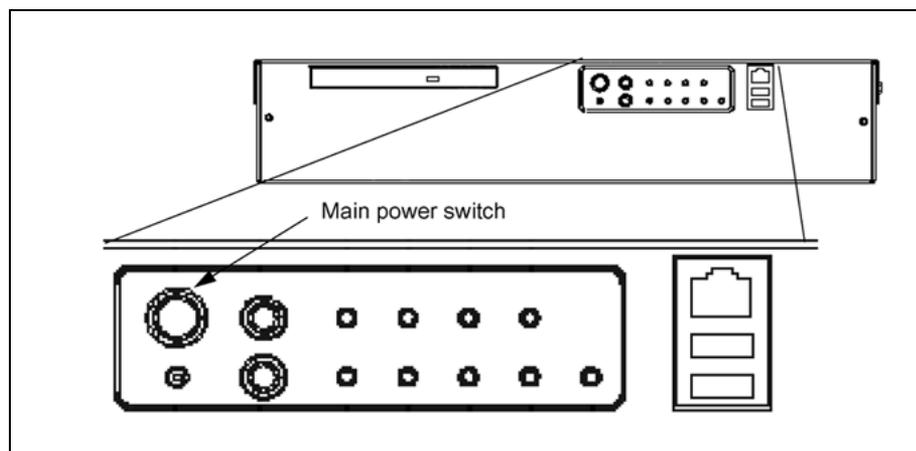
There are no restrictions on using this procedure.

### 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

| Step                                      | Action                                                                                 |
|-------------------------------------------|----------------------------------------------------------------------------------------|
| <b>At the front panel of the SST unit</b> |                                                                                        |
| 1                                         | If necessary, power on the SST using the main power switch located on the front panel. |
| 2                                         | If desired, at the SST console, monitor the boot progress of the unit.                 |






—End—

## Generating 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, in section "[Self-signed certificate security disclaimer](#)" (page 132).

### Action

| Step | 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_mgmt
```

*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) Import Certificates and Private Key
|
|
| Option:
[]

This tool will help you to bring your SSL/TLS-based application
into service
Use the <TAB> key to move and select fields

```

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

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

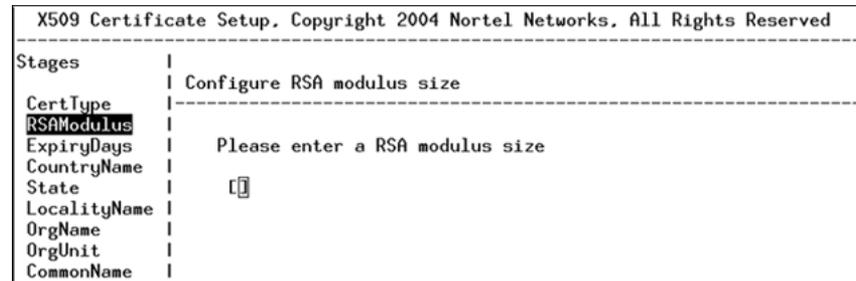
Stages |
| X509 Certificate Setup
CertType |-----
|
|
| PLEASE REVIEW THE FOLLOWING TERMS AND CONDITIONS
| REQUIRED FOR THE USE OF DIGITAL SELF-SIGNED
| CERTIFICATES. MOVE BETWEEN PAGES BY USING THE 'C'
| AND 'B' KEYS. IF YOU DO NOT ACCEPT THE TERMS AND
| CONDITIONS BELOW, YOU ARE NOT AUTHORIZED TO USE 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.



- 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)

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 | <a href="#">step 8</a>                    |
| you receive the message that the RSA private key already exists and you want to reuse the key        | Press y and go to <a href="#">step 12</a> |
| you do not receive any message that an RSA private key already exists                                | <a href="#">step 12</a>                   |

- 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 <a href="#">step 10</a> . |
| you are sure you want to proceed with deleting the existing RSA private key | Go to <a href="#">step 11</a> .                                           |

- 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 |
RSA modulus |
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.*

```

X509 Certificate Setup. Copyright 2004 Nortel Networks. All Rights Reserved

Stages |
 | Configure the country name

CertType |
RSA modulus |
ExpiryDays | Please enter a country name (2 letter code) (optional)
CountryName |
State |
LocalityName |
OrgName |
OrgUnit |
CommonName |
EmailAddress |
Summary |

```

- 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**.

This entry helps identify the node to a remote entity.

*The state/province configuration screen appears.*

```

X509 Certificate Setup. Copyright 2004 Nortel Networks. All Rights Reserved

Stages |
 | Configure the state or province name

CertType |
RSA modulus |
ExpiryDays | Please enter a state/province name (optional)
CountryName |
State |
LocalityName |
OrgName |
OrgUnit |
CommonName |
EmailAddress |
Summary |

```

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

This entry helps identify the node to a remote entity.

*The locality configuration screen appears.*

```

X509 Certificate Setup. Copyright 2004 Nortel Networks. All Rights Reserved

Stages |
 | Configure the locality name

CertType |
RSAModulus |
ExpiryDays | Please enter a locality name, e.g. city (optional)
CountryName |
State |
LocalityName |
OrgName |
OrgUnit |
CommonName |
EmailAddress |
Summary |

```

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

This entry helps identify the node to a remote entity.

*The organizational configuration screen appears.*

```

X509 Certificate Setup. Copyright 2004 Nortel Networks. All Rights Reserved

Stages |
 | Configure the organizational name

CertType |
RSAModulus |
ExpiryDays | Please enter a organizational name, e.g. company (optional)
CountryName |
State |
LocalityName |
OrgName |
OrgUnit |
CommonName |
EmailAddress |
Summary |

```

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

This entry helps identify the node to a remote entity.

*The organizational unit configuration screen appears.*

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved

Stages |
 | Configure the organizational unit name (e.g. section)

CertType |
RSAModulus |
ExpiryDays | Please enter a organizational unit name (optional)
CountryName |
State | []
LocalityName |
OrgName |
OrgUnit |
CommonName |
EmailAddress |
Summary |

```

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

This entry helps identify the node to a remote entity.

*The server common name configuration screen appears.*

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved

Stages |
 | Configure the server common name

CertType |
RSAModulus |
ExpiryDays | Please enter a common name for this certificate
CountryName |
State | []
LocalityName |
OrgName |
OrgUnit |
CommonName |
EmailAddress |
Summary |

```

- 18 Enter a common name for the SST 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. 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 "Configuring SIP Gateway application parameters" in *Session Server Trunks Configuration Management* (NN10338-511).



#### CAUTION

Using special characters other than the '-' and '.' for mgcHostName and HOST\_MGCNAME may cause conflicts with third-party vendor equipment that strictly adheres to the RFC recommendation.

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**.

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

---

—End—

---

## 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.";

## Generating 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

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

---

#### Step Action

---

#### *At a Session Server command line interface (CLI)*

- 1 Log onto the standby SST 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
```

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
CertType

X509 Certificate Setup

Welcome to the X509 Certificate Setup tool.

1) Generate Self-Signed Certificate
2) Generate Certificate Signing Request
3) Validate Certificate Chain

Option:
 [2]

| 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**.

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.*



8 Use the following table to determine your next step:

| If                                                                          | Do                                                                            |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| you <u>do not</u> want to delete the existing RSA key                       | Press <b>n</b> to abort the delete operation and go to <a href="#">step 9</a> |
| you are sure you want to proceed with deleting the existing RSA private key | Skip to <a href="#">step 10</a> .                                             |

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**.

This entry helps identify the SST to a remote entity.

*The state/province configuration screen appears.*

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved

Stages |
Configure the state or province name
CertType |
RSAModulus |
ExpiryDays | Please enter a state/province name (optional)
CountryName |
State | []
LocalityName |
OrgName |
OrgUnit |
CommonName |
EmailAddress |
Summary |

```

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

This entry helps identify the SST to a remote entity.

*The locality configuration screen appears.*

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved

Stages |
Configure the locality name
CertType |
RSAModulus |
ExpiryDays | Please enter a locality name, e.g. city (optional)
CountryName |
State | []
LocalityName |
OrgName |
OrgUnit |
CommonName |
EmailAddress |
Summary |

| <<Back | | Next>> |

| Use '<' and '>' keys to move if left and right arrows don't work
|

```

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

This entry helps identify the SST to a remote entity.

*The organizational configuration screen appears.*



```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved

Stages |
Configure the server common name
CertType |
RSAModulus |
ExpiryDays | Please enter a common name for this certificate
CountryName |
State | []
LocalityName |
OrgName |
OrgUnit |
CommonName |
EmailAddress |
Summary |

| <<Back | | Next>> |

The common name is the device's active IP address.
Use '<' and '>' keys to move if left and right arrows don't work

```

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

- use the active IP address for the SST in the format:  
xxx.xxx.xxx.xxx
- use a hostname of up to 64 alphanumeric characters. 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).



**CAUTION**

Using special characters other than the '-' and '.' for mgcHostName and HOST\_MGCNAME may cause conflicts with third-party vendor equipment that strictly adheres to the RFC recommendation.

The common name value is used for mutual authentication between the SST 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.*

```

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 |
 |
 | -----
 | | <<Back | | Next>> |
 | -----
 | Use '<' and '>' keys to move if left and right arrows don't work

```

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

This entry helps identify the SST to a remote entity. There is no validation of the e-mail address.

*A password challenge configuration screen appears.*

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved

Stages |
 | Configure a challenge password

CertType |
RSAModulus |
CountryName | Please enter a challenge password for this request
State |
LocalityName | []
OrgName |
OrgUnit |
CommonName |
EmailAddress |
Password |
Summary |
 |
 | -----
 | | <<Back | | Next>> |
 | -----
 | Use '<' and '>' keys to move if left and right arrows don't work

```

- 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.

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
CountryName
State
LocalityName
OrgName
OrgUnit
CommonName
EmailAddress
Summary
Common Name: 172.16.182.16
Email Address:

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](#)" (page 143).*

*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 <a href="#">step 6</a> 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 22.                                   |
| n was entered in <a href="#">step 6</a> to create a new server.key file       | Continue to <a href="#">step 22</a> to make a copy of the newly created server.key as well as restore the server.key 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
```

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.*

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 "[Importing certificates and the private key](#)" (page 144).

---

—End—

---

### 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.

---

## Importing certificates and the 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 SST.
- CA chain is required in PEM format in a `trusted.crt` file, top down with the root CA at the top.

### Prerequisites

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

### Action

---

| Step | 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:<br><code>cd /users/mtc</code>                                                    |
| 3 | Start the certificate management tool by typing<br><code>/sbin/cert_mgnt</code><br><i>After a few seconds the Introduction screen is displayed.</i> |

```

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) Import Certificates and Private Key
Option:
[]

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 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**.

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.*

```

X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved

Stages |
Configure the Certificate Authority certificate filename
CertType
CAFile
CertFile
KeyFile
Summary
Please enter a CA certificate filename
[]

Use '<' and '>' keys to move if left and right arrows don't work

```

- 5 Enter the filename of the CA certificate by typing **trusted.crt** position the cursor on the **Next** button and press **Enter**.

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



```
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\_mgmt 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.

---

—End—

---

## 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.

## Copying 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.

---

#### Step Action

---

##### *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`

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 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
```

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

- 7 Change directories to the security certificates level:

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

- 8 Change the owner and group to root for all files:

```
chown root:root *
```

- 9 Set the file permissions:

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

- 10 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 the procedure ["Applying security certificates"](#) (page 150).

---

—End—

---

## Applying 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.

| Step | Action |
|------|--------|
|------|--------|

#### *At your workstation CLI or IEMS client*

- |   |                                                                                                                              |
|---|------------------------------------------------------------------------------------------------------------------------------|
| 1 | Log onto the inactive SST unit and change to root user.                                                                      |
| 2 | Stop the Apache web server by typing<br><pre># /usr/local/apache/bin/apachectl stop</pre> and pressing the Enter key.        |
| 3 | Restart the Apache web server by typing<br><pre># /usr/local/apache/bin/apachectl startssl</pre> 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 the following procedures in the order listed to stop and restart the application.
  - a. "Locking the SIP Gateway application" (page 104)
  - b. "Suspending the SIP Gateway application" (page 110)
  - c. "Unsuspending the SIP Gateway application" (page 113)
  - d. "Unlocking the SIP Gateway application" (page 107)

**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.

---

—End—

---

## Managing 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 SST units.

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

### Action

| Step | Action |
|------|--------|
|------|--------|

***At the CS 2000 Session Server Launch Point***

- 1 Select **Carrier VoIP Communication Server 2000 Session Server Manager** from the launch point menu.

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

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

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



- 3 Use the following table to determine your next step:  
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 <a href="#">step 4</a><br><br><b>Note:</b> If the remote SIP server and the local SST 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 <a href="#">step 5</a>                                                                                                                                                                                                                                    |
| you want to view trusted certificates currently provisioned    | skip to <a href="#">step 9</a>                                                                                                                                                                                                                                    |
| you want to delete a trusted certificate currently provisioned | skip to <a href="#">step 9</a>                                                                                                                                                                                                                                    |

- 4 Obtain the root CA certificate for the remote SIP server.  
If the remote SIP server is an SST 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](#)" (page 154).
  - c. Go to [step 6](#).

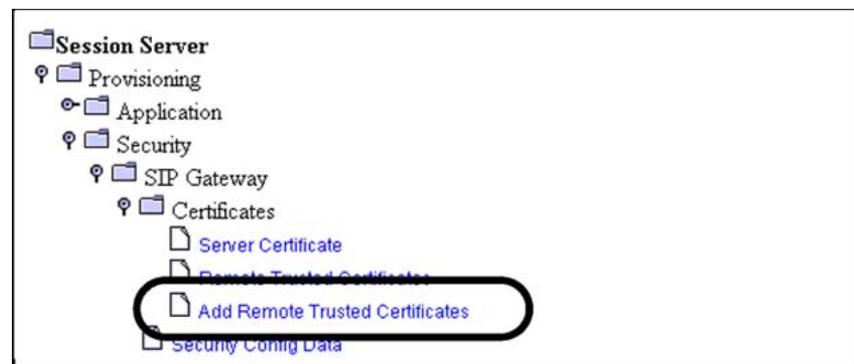
- 5 Obtain the self-signed certificate for the remote SIP server.

If the remote SIP server is another SST node, then perform procedure "Displaying local server certificates" (page 158) from the user interface for the remote node. When done with that procedure, select and copy the PEM formatted certificate as shown below:

#### PEM formatted certificate

```
-----BEGIN CERTIFICATE-----
MIICKTCCAfqgAwIBAgIBADANBgkqhkiG9w0BAQUFADBAMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTkxkNDQ3Mz1aFw0wNjA0MDYxNDQ3Mz1aMEAxChZAJBgNVBAYTA1VT
MQswCQYDVQQIEwJQZEMMAoGA1UEBxMDU1RQMRyYwFAYDVOQDEw0xOTUuMTY4LjUy
LjE4MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfr2aA1OX8GH+n6dfZHSQJ
bTYLEK3vDIDz6k4io10Uv+NkB4fQdlifuse20ia/19+ohlQJZe/XtK56+0DmnJzK
Q+j4dxRt4pMOQjfy102Q+sgtrXcaHmGSg3IIjtpZCqTn5+Czucie6cr756fr/5e2
fn222mWA4wjJtKa0FHafFQIDAQABO4GAmIGXMB0GA1UdDgQWBQk7tPqLO0MPnCW
2iEQ4oq4HVtIMTBoBgNVHSMeyTbfgBQk7tPqLO0MPnCW2iEQ4oq4HVtIMaFepEiw
QDELMAkGA1UEBhMCFVVMxChZAJBgNVBAGTAk5DMQwwCgYDVQQHEwNSVFAXFjAUBGNV
BAMTDTE5Mi4xNjguNTUuMTGCAQAwDAYSYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUF
AAOBgQBGAghMvbb7kwncT94uCsQCMANyeGdkfwy/rCFUJve3u1kt9ALPy1nZrtns
DDQShszalGLOiThpsW3iwrArHAHQZ36k01nmhMrQzUkU25NZ8GR5PgeadIADevTa
+GGHyg0Mkx10P7yWdujpyQEBpLVjWvptzmeABOwt9Tjp50iNlg==
-----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 associated with the certificate.

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

## Add Trusted Certificate

|                                                                                                              |              |                                               |
|--------------------------------------------------------------------------------------------------------------|--------------|-----------------------------------------------|
| Certificate Name                                                                                             | sess_srvr_21 | Allowed characters for Certificate Name: 0-9. |
| Certificate (in PEM)                                                                                         |              |                                               |
| <pre>-----BEGIN CERTIFICATE----- paste PEM encoded certificate text here ... -----END CERTIFICATE-----</pre> |              |                                               |

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

Certificate Name:  Allowed characters for Cert: 0-9.

Certificate (in PEM)

```

-----BEGIN CERTIFICATE-----
MIICkTCCAfqgAwIBAgIBADANBgkqhkiG9wOBAQUFADBAMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTkxkDDAKBgNVBAcTA1JUUEUWMBQGA1UEAxMNMTkyLjE2OC41M14x
MTAeFw0wNTA0MDYxNDQzMzlaFw0wNjA0MDYxNDQzMzlaMEAxChAJBgNVBAYTA1VT
MQswCQYDVQQIEwJQZzEMMAoGA1UEBxMDU1RQMRYwFAyDVQQDEw0xOTIuMTY4LjUy
LjExMIGfMAOGCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDfR2aA1OX8GH+n6dfZHSQJ
bTYLEK3vDIDz6k4iO1OUv+Nk4fQd1ifusE2Oia/19+oh1QJZe/XtK56+0DmnJzK
Q+j4dxRt4pMOQjFY102Q+sgtrXcaHmGSg3IIjtp2CqTn5+CzuciE6cr756fr/5e2
fN222mWA4wjttKaOFHafFQIDAQABo4GAMIGXMB0GA1UdDgQWBQBk7tPqLOOMPnCw
2iEQ4oq4HVtiMtbOgNVHSMeyTbfgBQk7tPqLOOMPnCw2iEQ4oq4HVtiMaFEPeIw
QDELMAKGA1UEBhMCMVVMxkCzAJBgNVBAGTAk5DMQwwCgYDVQQHEwNSVFAXFjAUBgNV
BANTDTE5Mi4xNjguNTIuMTGCAQAuDAYDVROTBAAUwAwEB/zANBgkqhkiG9wOBAQUF
AAOBgQBGA1UEBhMmVbb7kwnct94uCsQCMANyeGDkfwy/rCfUJve3ulKt9ALPyInZRtns
DDQShszalGLOiThPsW3iwrArHAHQZ36kO1mmhMrQzUkU25N28GR5PgeadIADEvTa
+GGHygOMkx1OP7ywdujpyQEEpLVjWvptzmeABoWt9Tjps0iNlg=
-----END CERTIFICATE-----

```

**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:  
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     | <pre> -----BEGIN CERTIFICATE----- MIICKTCCAfqgAwIBAgIBADANBgkqhkiG9wOBAQUFADBAMQswCQYDVQQGEwJVUzEL MAkGA1UECBMCKmxDAAKBgNVBACATA1JUUEDEWMBQGA1UEAxMNNTkyLjE2OC41Mi4x MTAeFw0wNTA0NDYxNDQ3Hz1eFw0wNjA0NDYxNDQ3Hz1eMEAxCzAJBgNVBAYTA1VT MQswCQYDVQQIEwJQOzEMMAoGA1UEBxMDU1RQMRYwFAYDVQQDEw0xOTIuNTY4LjUy LjExMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDFR2aA1OX8GH+n6df2HSQJ bTYLEK3vDIz6k4i010Uv+Nk84fQd1ifusE20ia/19+oh1QJZe/XtK56+OdmnJzK Q+j4dxRt4pMOQjFY102Q+sgtrXcaHmGSg3IIjtp2CqTn5+Czuc1E6cr756fr/5e2 fN222mWA4wjtKaOFHafFQIDAQABo4GAMIGXMB0GA1UdDgQWBBQk7tPqLOOMPncw 21EQ4oq4HVtiNTBoBgNVHSEYTBfgBQk7tPqLOOMPncw21EQ4oq4HVtiMaFpE1w QDELMAkGA1UEBhMCMVVMxMzAJBgNVBAGTAk5DMQswCgYDVQHEwNSVFAXFjAUBGNV BAHTDTESHi4xNjguNTIuHTGCAQAwdAYDVROTBAAUwAwEB/zANBgkqhkiG9wOBAQUF AAOBgQBgAgHvbb7kwnc294ucQCMANyeGdkfwy/rCzUJve3ulRt9ALPy1nZrtns                     </pre> | <a href="#">Delete</a> |

11 Use the following table to determine your next step:

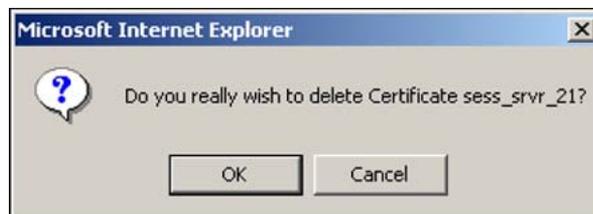
| If                                                                    | Do                                    |
|-----------------------------------------------------------------------|---------------------------------------|
| you want to delete a trusted certificate currently provisioned        | continue with <a href="#">step 12</a> |
| you do not want to delete a trusted certificate currently provisioned | return to <a href="#">step 3</a>      |

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

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

| Certificate Name | Certificate PEM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Delete                 |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| sess_srvr_21     | <pre> -----BEGIN CERTIFICATE----- MIICKTCCAfqgAwIBAgIBADANBgkqhkiG9wOBAQUFADBAMQswCQYDVQQGEwJVUzEL MAkGA1UECBMCKmxDAAKBgNVBACATA1JUUEDEWMBQGA1UEAxMNNTkyLjE2OC41Mi4x MTAeFw0wNTA0NDYxNDQ3Hz1eFw0wNjA0NDYxNDQ3Hz1eMEAxCzAJBgNVBAYTA1VT MQswCQYDVQQIEwJQOzEMMAoGA1UEBxMDU1RQMRYwFAYDVQQDEw0xOTIuNTY4LjUy LjExMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDFR2aA1OX8GH+n6df2HSQJ bTYLEK3vDIz6k4i010Uv+Nk84fQd1ifusE20ia/19+oh1QJZe/XtK56+OdmnJzK Q+j4dxRt4pMOQjFY102Q+sgtrXcaHmGSg3IIjtp2CqTn5+Czuc1E6cr756fr/5e2 fN222mWA4wjtKaOFHafFQIDAQABo4GAMIGXMB0GA1UdDgQWBBQk7tPqLOOMPncw 21EQ4oq4HVtiNTBoBgNVHSEYTBfgBQk7tPqLOOMPncw21EQ4oq4HVtiMaFpE1w QDELMAkGA1UEBhMCMVVMxMzAJBgNVBAGTAk5DMQswCgYDVQHEwNSVFAXFjAUBGNV BAHTDTESHi4xNjguNTIuHTGCAQAwdAYDVROTBAAUwAwEB/zANBgkqhkiG9wOBAQUF AAOBgQBgAgHvbb7kwnc294ucQCMANyeGdkfwy/rCzUJve3ulRt9ALPy1nZrtns                     </pre> | <a href="#">Delete</a> |

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](#).

---

—End—

---

## Displaying local server certificates

### Purpose of this procedure

Use this procedure to display a local server certificate used by the SST node.

### Limitations and restrictions

There are no restrictions for performing this procedure.

### Prerequisites

There are no prerequisites for performing this procedure.

### Action

| Step | Action |
|------|--------|
|------|--------|

**At the CS 2000 Session Server Launch Point**

- 1 Select **Carrier VoIP Communication Server 2000 Session Server Manager** from the launch point menu.

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

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select **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
NzQuNzQuMTg0MB4XDTA0MTIxNDE0NDU1Ml0XDTI0MTIwOTE0NDU1Ml0wGDF
ALUEAxMNNDcuMTc0Ljc0LjE4NDcBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYI
sIGj91HUOZuoBttcDv6WS8uDQ2SBptgoKDGtxwDvHSp6HwSSklh+oP7ZMP
oS0GCXqMyw1Dz/4KbgThn43QfGgRfBMZ50QeRKQxLZ/IUIobbOSuE9qOMc
vg6POrj8AoY0TNvy0qd9p06KeSZpWFlilPFsmMKjPMMCAwEAAAaxMG8wHQY
BBYEFISzCW/PLt0VKQT0Hhc7psaikKtpMEAGA1UdIwQ5MDeAFISzCW/PLt
HhC7psaikKtpoRykGjAYMRYwFAYDVQQDEw0Ny4xNzQuNzQuMTg0ggEAMAV
EwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEALHw342GcEOvf22xGVczVPM
8T21V5uOMBzjt7XLLz1U+Qt9ZFsu3CY/HJyZWlnloYGm8mTVn2HYUHhmC5
i8dlShFweehuW83FAJMuI0xsb9ZMM0zeZbKA4QjLPD2i5EsZf3CMp7sSim
H9ZqvK080lnzJL4=
-----END CERTIFICATE-----
```

—End—





Carrier VoIP

## Session Server Trunks Security and Administration

Copyright © 2006, Nortel Networks  
All Rights Reserved.

Publication: NN10346-611  
Document status: Standard  
Document version: 04.02  
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to [www.nortel.com/documentfeedback](http://www.nortel.com/documentfeedback).

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

The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose it only to its employees with a need to know, and shall protect it, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

This is the Way, This is Nortel, Nortel, the Nortel logo, the globemark design, and the NORTEL NETWORKS corporate logo, are trademarks of Nortel Networks. All other trademarks are property of their respective owners. All rights reserved.

