Session Server Upgrades

What's new in (I)SN08 Session Server upgrades and patching

The following feature related enhancements and changes have been documented in this NTP:

- An in-service major release upgrade activity supports upgrading existing Session Server-SIP application nodes from SN07 to SN08.
- Features A00008383 and A00007275 - Support for Multiple HTTPS connections to the Session Server through SSPFS.This feature provides support for multiple proxy https connections from IEMS/SSPFS and allows multiple Session Server nodes to reside on the CS-LAN.
- Feature A00006893 - adds transport layer security (TLS) to the SIP Gateway application. In SN08, TLS is used to secure SIP messaging communications between the SIP Gateway application and a remote SIP device such as an application server.

General upgrade strategies in (I)SN08

Activities and procedures are available in this NTP for performing major release upgrades, patching activities and maintenance release upgrade activities. Activities for aborting and rolling back an upgrade are also provided. Release notes provided with the patch files or maintenance release images offer additional release-specific information about performing these activities.

For performing a major software upgrade to SN08, Session Server upgrades from releases previous to SN07 are not supported. The process of performing a major release upgrade is similar to performing a maintenance release upgrade. In the event of a problem encountered during a major upgrade activity, a rollback process is provided.

Tools and utilities for maintenance releases and patching

Upgrading and patching the Session Server is performed using several interfaces depending on the activity required. The interface needed is called out at the beginning each procedure. The following interfaces are

used in accomplishing the tasks described in this NTP and are accessed through network workstations running the Integrated EMS:

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

Tools for applying maintenance releases

The following interfaces are used through the Integrated EMS in applying maintenance releases:

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

Tools for applying patches

Patching is performed manually using the NCGL command line interface (CLI) accessible from the Integrated EMS. Each unit in the node must be patched. If multiple nodes are installed in the network in SN08, then all nodes must be similarly patched.

Removing obsolete NCGL bootload versions

By default, the Session Server units retain previous NCGL bootloads. For housekeeping purposes, older bootload versions may be manually removed by clicking the **Remove** button. You cannot delete the bootload that is set to be the default bootload, nor can you delete the currently running bootload.

If a bootload image upgrade is requested and insufficient disk space is available in the `/boot` directory, the NCGL software deletes the oldest bootload from the `/boot` directory and performs the requested bootload image upgrade. The system can not delete a bootload that is set to be the default bootload.

Bootload Management		
Bootload	**Maintenance**	
4.0.0.0303171003	Default Bootload	
4.0.0.0303101433	Set default	Remove
4.0.0.0303051030	Set default	Remove
4.0.0.0303051012	Set default	Remove

Upgrade and patching activities found in this NTP

The following high-level activities are available in this NTP for the SN08 release:

Activity
Upgrading from a previous major release - SN07 to SN08 on page 4
Abort a major release upgrade on page 18
Perform a major release rollback activity on page 22
Applying a maintenance release upgrade on page 28
Abort a maintenance release upgrade on page 40
Perform an emergency maintenance release rollback activity on page 44
Patching the NCGL operating system on page 50

Upgrading from a previous major release - SN07 to SN08

This section describes how to perform an in-service major release upgrade of the Session Server units. It also describes how to perform a rollback of a partial or complete major release upgrade in cases where a major release fails or causes problems with the system.

Major release upgrade strategy

A major release upgrade impacts both the Session Server NCGL platform and the SIP Gateway application.

- A Session Server NCGL platform software release consists of release notes, CS 2000 NCGL Platform Manager software, NCGL software and optional CS 2000 NCGL Platform Manager patches.

  Using the CS 2000 NCGL Platform Manager GUI you can select an image to upgrade to. You can upgrade the Session Server load from the local DVD-ROM drive, from an ISO image located on a remote system, or from a local file on the Session Server disk drive. Space is available on the local hard drive to maintain approximately 2 loads in case fallback to a previous load is necessary. Partial and complete rollbacks of a failed upgrade can be performed.

- A Session Server SIP Gateway application software release consists of release notes, CS 2000 NCGL Platform Manager software, and SIP Gateway application software.

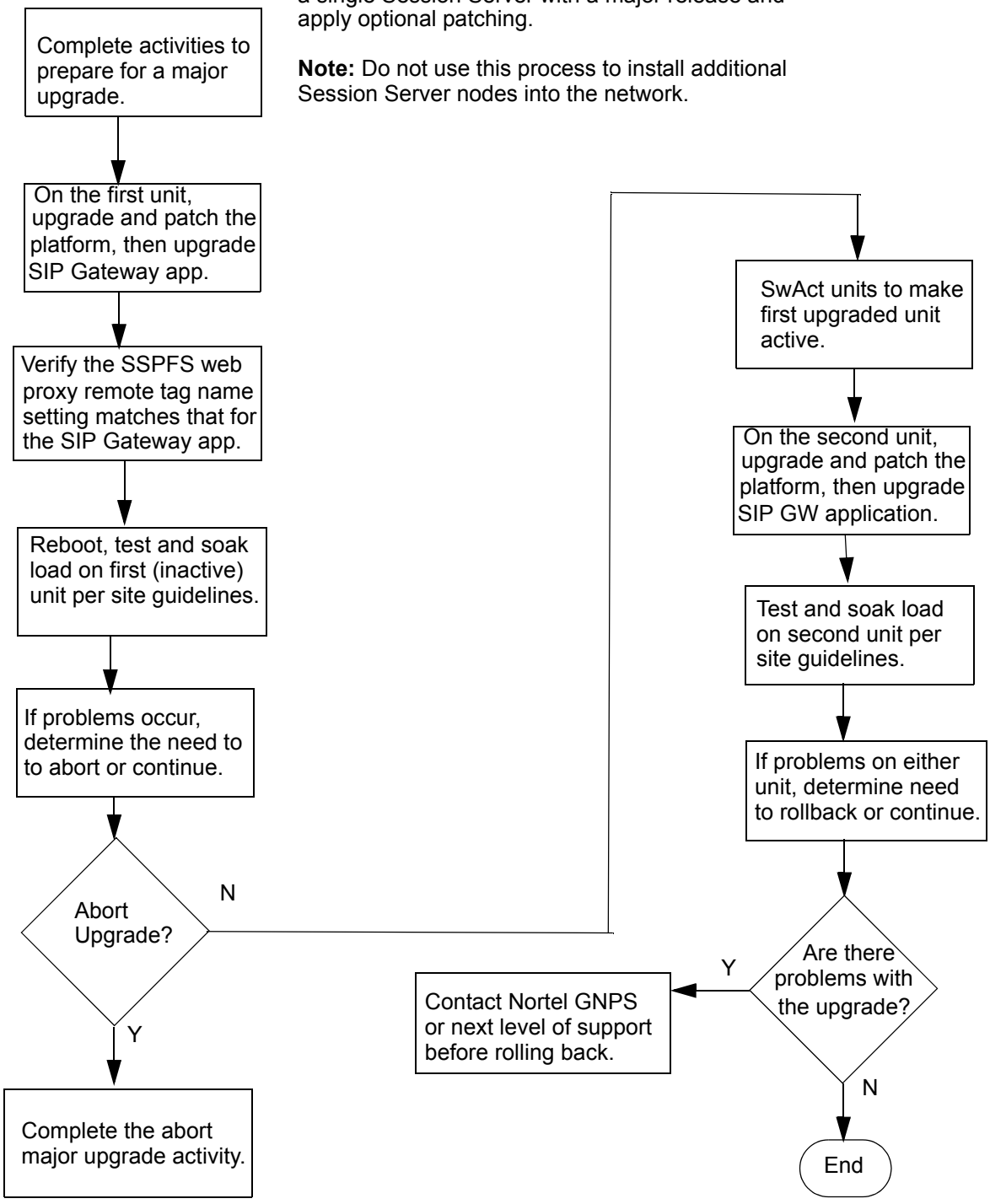
  Using both the CS 2000 NCGL Platform Manager GUI and the Session Server command line interface (CLI), you can upgrade the SIP Gateway application.

Refer to the following activity diagram for a high-level view of the upgrade process for the Session Server units.

Major release upgrade of Session Server with patching

Use the following high-level process to upgrade a single Session Server with a major release and apply optional patching.

Note: Do not use this process to install additional Session Server nodes into the network.



Network upgrade order for Session Server-SIP Gateway application

For all applicable solutions, Session Server with SIP Gateway application should be upgraded before the DPT-GWCs. Verify the upgrade order by referring to the Carrier Voice over IP Network Upgrade Overview NTP, NN10440-450.

Time required for a major upgrade

The approximate time to complete a major upgrade for a Session Server node running the SIP Gateway application is 2-1/2 hours.

Major release upgrade limitations and restrictions

The following general limitations apply to performing a major release upgrade or rollback of a major release upgrade.

- While a major upgrade is a full in-service activity, performing a full rollback of a major upgrade is an out-of-service activity. All call processing and billing information generation is terminated for part of the rollback activity.
- Patches can only be applied using the CLI (command line interface).

Software delivery methods for major releases

Major release software is delivered on a data CD/DVD disk or using Electronic Software Delivery (ESD,) where a compressed ISO image is delivered to an electronic drop-box on the customer network from Nortel Networks.

Major release upgrades using ESD delivery require that the upgrade package be transferred onto both Session Server units and put in the /opt/swd directory using a secure file transfer program such as scp. After the Major release upgrade of the NCGL platform, the bootload file is stored in the /boot directory.

In order to receive Major release software from Nortel using ESD, the operating company must have an ESD agreement with Nortel. When the agreement is established, the operating company furnishes Nortel with the location of an electronic dropbox, an email address for notification and a username and password pair for delivering software loads. When Nortel delivers a software load to the dropbox, an electronic mail notification is sent to the e-mail address specified by the operating company.

Software installation methods for major releases

You can upgrade the Session Server NCGL load from the local DVD-ROM drive, or from an ISO image located on a remote system, or

copied to a local directory. The following upgrade protocols (methods) are selectable from the CS 2000 NCGL Platform Manager GUI:

- Local CDROM - the local DVD-ROM drive (labeled in the software as the local CD-ROM).
- Local file - an iso image, or load.tgz file copied from the local DVD-ROM drive to the hard drive using the secure copy program, **scp**, to transfer the data.
- Remote file using FTP or anonymous FTP - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP service. If the workstation or server is configured to allow anonymous FTP, use anonymous FTP to avoid sending username and password information in cleartext format across the network. This is not a recommended method.
- Remote file using HTTP or HTTPS - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP or HTTPS service. This is not a recommended method.

You can upgrade the Session Server SIP Gateway application from the local DVD-ROM drive, or from an ISO image copied to a local directory. Most of the time the software load for the SIP Gateway application is on the same CD/DVD disk or copied ISO image as the NCGL platform load; however, some customers may receive a separate software load for the SIP Gateway application. Consult your release notes for details.

Managing security certificates in SN08

When upgrading from SN07 to SN08, updating security certificates may be required, depending on the type of certificates currently being used on the Session Server.

Depending on the type of security certificates installed on your system and the status of those certificates, one of the following activities will apply when upgrading from SN07 to SN08:

- If you are using the original, temporary certificates supplied during initial installation, you will need to use the certificate management tool to create new certificates.
- If you already have certificate authority (CA) signed certificates for either Apache or Tomcat, then you can migrate the CA-signed certificate from SN07 to SN08 using the certificate management tool. Some preparation is required.
- If you already have self-signed certificates for both Apache and Tomcat, then you will need to create new self-signed certificates

during the upgrade activity. Migrating self-signed certificates from SN07 to SN08 is not supported.

- If you have CA-signed security certificates that are about to expire, you can import the certificates into SN08; however, TLS calls should not be setup until you have renewed your certificates.

Migrating from self-signed to CA-signed certificates

If you are using self-signed certificates and want to migrate your Session Server-SIP to CA-signed certificates, you must first complete upgrading to SN08. You cannot migrate from self-signed to CA-signed certificates during a major release (SN07-to-SN08) upgrade.

Migrating self-signed certificates from SN07 to SN08

Migrating self-signed certificates from SN07 to SN08 is not supported. You must create new self-signed certificates. This applies to self-signed certificates that are about to expire.

Prepare for a major release upgrade

Complete the steps for following activity, to prepare for a major release upgrade:

Major release upgrade preparation activity

Step	Procedure or activity
1	Verify the component network order in which the Session Server node will be upgraded for the end-to-end upgrade strategy.
2 (new)	Refer to section Managing security certificates in SN08 on page 7 and determine the kind of certificates you currently have (customer self-signed or purchased from a certificate authority). You will need this information during the upgrade and after the upgrade is complete.
3	If you have purchased security certificates from a Certificate Authority or created self-signed certificates, use procedure Back up security certificates on page 58 to ensure that you have made a backup copy of the security certificate files on both Session Server units and to make a backup to a secure remote server location.
4	If you have purchased security certificates from a Certificate Authority, you must prepare to validate your existing certificate chain using procedure Prepare to validate a certificate chain on page 62.

Major release upgrade preparation activity

Step	Procedure or activity
5	Back up the SIP Gateway application database on the active unit using procedure Perform a manual backup of the Session Server database on page 69.
6	Acquire the appropriate major release software from Nortel either using ESD delivery to a customer dropbox/repository server or from a major release CD/DVD disk.
7	If you are performing a major release upgrade using an ISO image acquired using ESD, complete procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 71 to copy the ISO files to hard drive of each unit.
8	Use procedure View release notes for a release on page 74 to check release notes for upgrade issues.
9	Locate and have available the original Session Server software CD/DVD disk along with a copy of the existing version of the SIP Gateway application installed on your system. The existing version may be from the last maintenance release image installed from a CD/DVD disk or an ESD downloaded image file.
10	Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
11	You have completed this high-level activity.

Perform a major release upgrade

Complete the steps in the order listed, to perform an in-service major release upgrade and optional patching of the NCGL platform.

Major release upgrade activity

Step	Procedure or activity
Upgrade the NCGL platform load on first unit (inactive)	
1	Ensure that you have completed section Prepare for a major release upgrade on page 8 before continuing.
2	Determine what version of the NCGL platform load is currently installed on your Session Server node by going to the **System Information** page of the CS 2000 NCGL Platform manager and using procedure Determine the current version of the NCGL platform software load on page 77, to determine if any maintenance releases must be applied before performing a major upgrade. Determine what version of the SIP Gateway application software (listed as Session Server load info) is currently installed on your Session Server node using procedure Determine the current version of software loads on page 80, to determine if any maintenance releases must be applied before performing a major upgrade.
3	If applying a major upgrade using a CD/DVD disk, insert the disk into the disk drive of the inactive unit.
4	At the active unit, use procedure Inhibit a system SwAct (Jam) on page 85 to jam the units.
5	At the NCGL Platform Manager for the physical unit which is inactive, upgrade the NCGL platform software using procedure Upgrade Session Server NCGL platform software on page 90. Ensure that you set the new NCGL load as the default boot load. For instance, if unit 0 is the active unit, log into the NCGL Platform Manager GUI for unit 1.
6	From the active unit, use procedure Reboot a Session Server unit on page 98 to perform a **RebootMate** of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.

Major release upgrade activity

Step	Procedure or activity
7	If your site uses certificates signed by a Certificate Authority, at the inactive unit complete procedure Validate a certificate chain on page 104. If your site uses self-signed certificates, at the inactive unit complete procedure Generate self-signed security certificates on page 108. **Note:** You cannot migrate from self-signed to CA-signed certificates during this upgrade.
8	On the inactive unit make a backup copy of your new security certificates using procedure Back up security certificates on page 58.
9	Log into the inactive unit NCGL Platform Manager and go to the **System Information** page. Use procedure View the operational status of a Session Server NCGL platform on page 119 for assistance with this task. If you can access the NCGL Platform Manager GUI, then the security certificates are properly installed. **Note:** If you cannot access the NCGL Platform Manager, then there is a problem with your security certificates. Contact your next level of support, Nortel GNPS or Nortel's emergency response team.
Apply and commit NCGL patches to the first unit	
10	Use procedure View release notes for a release on page 74 to identify the required NCGL platform patches (if any) for the new release.
11	Log onto the active unit and use procedure Inhibit a system SwAct (Jam) on page 85 to verify that the units are jammed. If they are not, then jam the units.
12	Use procedure Acquire patch files on page 139 to copy all required patches from the CD/DVD disk or the ESD delivered ISO image file to the patching holding directory on the unit.
13	Use procedure Apply and commit an NCGL patch on page 146 to apply and commit NCGL patches to the inactive unit.

Major release upgrade activity

Step	Procedure or activity
Upgrade the SIP Gateway application on the first unit	
14	If an NCGL upgrade was not necessary and the inactive unit was not jammed as described in the step 11 on page 9, follow procedure Inhibit a system SwAct (Jam) on page 85 before proceeding.
15	On the inactive unit, upgrade the SIP Gateway application software using procedure Upgrade/rollback/reinstall a Session Server application on page 156.
16	If necessary, use procedure View web proxy settings in SSPFS for Session Server on page 151 to determine the tag name you are using for this Session Server node.
17	From the active unit, use procedure Reboot a Session Server unit on page 98 to perform a **RebootMate** of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.
18	After the inactive unit completes rebooting, log into the inactive unit's CLI and verify that the current version of the SIP Gateway application matches the expected SN08 version by executing the following command: **cat /opt/apps/webint/version_info.txt.** Refer to procedure Determine the current version of software loads on page 80 for assistance with this task.
Activate and soak the new load on the first unit	
19	From the active unit, verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 164.
20	Use procedure Enable a system SwAct (Unjam) on page 167 to unjam the units.

Major release upgrade activity

Step	Procedure or activity
21	As applicable to your site, check the new software on upgraded unit, still inactive. • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
22	From the active unit, perform a SwAct using procedure Invoke a maintenance SwAct of the Session Server platform on page 170. All calls will continue to be processed on the (non-upgraded) active unit up to the time that the active IP address is switched to the inactive (upgraded) unit.
23	From the active unit, re-verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 164.
24	As applicable to your site, test new software on upgraded unit, now active. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
25	If all software tests are successful, continue with the next step in this procedure to upgrade the second (mate) unit (now inactive). Otherwise, if the active unit (with newly upgraded load) experiences problems with call processing, abort this upgrade procedure and complete activity *Abort a major release upgrade* in the Session Server Upgrades NTP, NN10349-461, and contact your next level of support or Nortel GNPS.

Major release upgrade activity

Step	Procedure or activity
Upgrade the NCGL platform load on second unit (now inactive)	
26	Verify that all applicable activities in Section Prepare for a major release upgrade on page 8 have been completed for the second unit.
27	If applying a major upgrade using a CD/DVD disk, insert the disk into the disk drive of the inactive unit.
28	At the active unit use procedure Inhibit a system SwAct (Jam) on page 85 to jam the units.
29	On the NCGL Platform Manager for the physical unit which is inactive, upgrade the NCGL platform software using procedure Upgrade Session Server NCGL platform software on page 90. Ensure that you set the new NCGL load to be the default boot load. For instance, if unit 0 is the active unit, log into the NCGL Platform Manager GUI for unit 1.
30	On the active unit, copy the new certificates to the mate (inactive) unit using procedure Copy security certificates to the mate unit on page 175.
31	On the inactive unit make a backup copy of the new security certificates using procedure Back up security certificates on page 58.
32	From the active unit, use procedure Reboot a Session Server unit on page 98 to perform a **RebootMate** of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.
Apply and commit NCGL patches to the second unit	
33	Use procedure View release notes for a release on page 74 to identify the required NCGL platform patches for the new release.
34	Log onto the active unit and use procedure Inhibit a system SwAct (Jam) on page 85 to verify that the units are jammed. If they are not, then jam the units.

Major release upgrade activity

Step	Procedure or activity
35	Use procedure Acquire patch files on page 139 to copy all required patches from the CD/DVD disk or the ESD delivered ISO image file to the patching holding directory on the unit.
36	Use procedure Apply and commit an NCGL patch on page 146 to apply and commit NCGL patches to the inactive unit.
Upgrade the SIP Gateway application software on the second unit	
37	At the inactive unit, upgrade the SIP Gateway application software using procedure Upgrade/rollback/reinstall a Session Server application on page 156. **Note:** As indicated in the procedure, when entering the remote tag name, use the same tag name as the one entered for the first unit. Both units in the node must use the same remote tag name.
38	From the active unit, use procedure Reboot a Session Server unit on page 98 to perform a **RebootMate** of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.
39	After the inactive unit completes rebooting, log into the inactive unit's CLI and verify that the current version of the SIP Gateway application matches the expected new version by executing the following command: **cat /opt/apps/webint/version_info.txt.**
Activate and soak the new load on the second unit	
40	From the active unit, verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 164.
41	Use procedure Enable a system SwAct (Unjam) on page 167 to unjam the units.

Major release upgrade activity

Step	Procedure or activity
42	As applicable to your site, check the new software on the upgraded unit, still inactive. • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
43	From the active unit perform a SwAct of the units using procedure Invoke a maintenance SwAct of the Session Server platform on page 170.
44	As applicable to your site, test new software on the upgraded unit, now active. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
45	If all software tests are successful, continue with the next step in this activity to upgrade. Otherwise, if the active unit (with newly upgraded load) experiences problems with call processing, abort this upgrade procedure. Go to and complete procedure *Perform a major release rollback activity* in the Session Server Upgrades NTP, NN10349-461, and contact your next level of support, Nortel GNPS or Nortel's emergency response team.
46	From the active unit, verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 164.

Major release upgrade activity

Step	Procedure or activity
47	Monitor the system for an appropriate period per your site guidelines before declaring this major upgrade complete. In SN08, multiple Session Server nodes can be installed in your network. However, ensure that all upgrade related issues are resolved for this Session Server node before installing any additional nodes in your network. Once additional nodes are installed in your network, you cannot roll back to SN07.
48	Edit the object properties in the IEMS for the Session Server you just upgraded to reflect the new software version. Refer to either of the procedures that follow to update the software version in the Device Version field. • Editing and viewing object properties using Java Web Client on page 217 • Editing and viewing object properties using Web Client on page 223
49	You have completed the major release upgrade activity.

Abort a major release upgrade

Complete the steps for the following activity, in the order indicated, to abort a major release upgrade activity in progress.

ATTENTION
This high-level activity assumes that you have not upgraded the second unit in the node to SN08. If you have already upgraded both units to SN08, then contact your next level of support or Nortel GNPS.

Abort major release upgrade activity

Step	Procedure or activity
1	If necessary, use procedure Enable a system SwAct (Unjam) on page 167 to unjam the units.
2	If necessary, complete procedure Invoke a maintenance SwAct of the Session Server platform on page 170 to revert call processing to the non-upgraded unit (the unit that is operating with the SN07 release load).
3	Use procedure Inhibit a system SwAct (Jam) on page 85 to jam the units.
4	Log onto the inactive unit and use procedure Rollback a Session Server NCGL platform software upgrade on page 183 to set the default NCGL bootfile to the SN07 load the unit was running prior to the major upgrade.
5	At the active Session Server unit, use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a FORCED reboot (RebootMate) of the inactive (mate) unit. Refer to procedure Reboot a Session Server unit on page 98 for assistance. ***Note:*** All applied and committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying and committing patches is not required.

Abort major release upgrade activity

Step	Procedure or activity
6	On the inactive unit CLI, use the SN07 DVD-ROM or ISO image with the latest maintenance release of the SIP Gateway application to downgrade the SIP Gateway application software using procedure Upgrade/rollback/reinstall a Session Server application on page 156.
7	From the active unit, use procedure Reboot a Session Server unit on page 98 to perform a **RebootMate** of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.
8	After the inactive unit reboots, go to the active unit and verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 164.
9	Once the databases are in-sync, release the JAM on the units using procedure Enable a system SwAct (Unjam) on page 167.
10	Complete procedure Invoke a maintenance SwAct of the Session Server platform on page 170 to make the downgraded unit active.
11	As applicable to your site, test the software on the downgraded unit, now active. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.

Abort major release upgrade activity

Step	Procedure or activity
12	Monitor the system for an appropriate period per your site guidelines before declaring this abort major release activity a success. If all software tests are successful, continue with the next step in this activity. Otherwise, if the active unit (with downgraded load) experiences problems with call processing, perform the following tasks in order: • complete procedure Invoke a maintenance SwAct of the Session Server platform on page 170 • complete procedure Inhibit a system SwAct (Jam) on page 85 • contact your next level of support or Nortel GNPS.
13	You have completed this high-level abort activity.

Perform a major release rollback activity

Complete the steps for the following activity, in the order indicated, to roll back a major release upgrade activity (SN08 to SN07) that has been performed on both units in the node.

CAUTION

You cannot perform a rollback to SN07 if you have installed additional Session Server nodes into your network. If you attempt to rollback from SN8 to SN07, you will experience service outages for SIP calls.

CAUTION

This is a service affecting activity. Performing this rollback activity causes approximately an hour long service interruption to all SIP-related call traffic and billing activity.

CAUTION

Ensure that you have a recent SN07 backup copy of the SIP Gateway application database available. If an SN07 backup version of the database is not available, the first unit to be rolled back must be recommissioned and the SIP Gateway application reprovisioned.

Major release rollback activity

Step	Procedure or activity
1	Locate and have available the previous Session Server software DVD-ROM or an ESD downloaded image file of the previous major release. Ensure that you have available a recent SN07 backup copy of the SIP application database.
2	If performing a major release rollback using an ISO image acquired using ESD, verify that the applicable ISO files are copied to the hard drive of each unit. If necessary, use procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 71.
3	At the active unit CLI complete procedure Drop database synchronization for the SIP Gateway application on page 187 executed from the current release of the Session Server software DVD-ROM or from the currently installed ISO image. ***Note:*** Once executed, this script drops call processing and application database synchronization between the active and inactive units. The SIP Gateway application maintains this non-synchronized state until a manual SwAct is performed, later in the procedure.
4	Log onto the NCGL Platform Manager for the physical unit which is inactive and use procedure Rollback a Session Server NCGL platform software upgrade on page 183 to set the default NCGL bootfile to the SN07 load the unit was running prior to the major upgrade. ***Note:*** All applied and committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying and committing patches is not required.
5	At inactive unit, roll back the SIP Gateway application software. Complete procedures Upgrade/rollback/reinstall a Session Server application on page 156.
6	Restore the original security certificates from a backup directory using procedure Restore a previous version of security certificates on page 180. This procedure must be performed on both units.

Major release rollback activity

Step	Procedure or activity
7	From the active unit, use procedure Reboot a Session Server unit on page 98 to perform a **RebootMate** of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.
8	On the inactive unit, prepare to restore a backup copy of the SN07 SIP Gateway application database using procedure Prepare for a database restore on a Session Server unit on page 212. Attention: If an SN07 backup version of the database is not available, the unit must be recommissioned and the SIP Gateway application reprovisioned.
9	Perform a SwAct (Force) of the units by completing procedure Invoke a maintenance SwAct of the Session Server platform on page 170, to make the downgraded unit active.
10	On the active unit (the rolled back unit), install the backup copy of the SN07 SIP Gateway application database using procedure Perform a database restore to a Session Server unit on page 216.
11	Restart the SIP Gateway application by locking, suspending, unsuspending, and unlocking the application. Refer to the following for assistance: • Lock the SIP Gateway application on page 192 • Suspend the SIP Gateway application on page 195 • Unsuspend the SIP Gateway application on page 204 • Unlock the SIP Gateway application on page 208
12	As applicable to your site, test the software on the downgraded unit, now active. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* and to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.

Major release rollback activity

Step	Procedure or activity
13	Monitor the system for an appropriate period per your site guidelines. If all software tests are successful, continue with the next step in this activity. Otherwise, if the active unit (with rolled back load) experiences problems with call processing, STOP executing this activity and contact your next level of support or Nortel GNPS.
14	Use procedure Inhibit a system SwAct (Jam) on page 85 to jam the units.
15	Log onto the NCGL Platform Manager for the physical unit which is inactive and use procedure Rollback a Session Server NCGL platform software upgrade on page 183 to set the default NCGL bootfile to the SN07 load the unit was running prior to the major upgrade. ***Note:*** All applied and committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying and committing patches is not required.
16	From the active unit, use procedure Reboot a Session Server unit on page 98 to perform a **RebootMate** of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.
17	On the inactive unit, rollback the SIP Gateway application software using procedure Upgrade/rollback/reinstall a Session Server application on page 156.
18	From the active unit, use procedure Reboot a Session Server unit on page 98 to perform a **RebootMate** of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.

Major release rollback activity

Step	Procedure or activity
19	After the inactive unit reboots, go to the active unit. Verify that the SIP Gateway application databases are synchronizing using procedure Verify synchronization status of Session Server units on page 164. If they are synchronizing then go to step 20. If they are not synchronizing then go to the next step in this activity.
20	Use procedure View the operational status of a Session Server NCGL platform on page 119 to check the status of the inactive unit to determine why database synchronization is not taking place by reviewing existing faults and logs. Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
21	Once the databases are in sync, release the JAM on the units using procedure Enable a system SwAct (Unjam) on page 167.
22	Perform a SwAct of the units by completing procedure Invoke a maintenance SwAct of the Session Server platform on page 170, to make the downgraded unit active.
23	Monitor the system for an appropriate period per your site guidelines before declaring this major release rollback activity complete. If all software tests are successful, continue with the next step in this activity. Otherwise, if you continue to experience problems with call processing, contact your next level of support or Nortel GNPS.
24	You have completed this emergency rollback activity.

Applying a maintenance release upgrade

This section describes how to perform an in-service maintenance release (MR) upgrade of the Session Server units. It also describes how to perform a rollback of a partial or complete maintenance release upgrade in cases where a maintenance release fails or causes problems with the system.

Maintenance release upgrade strategy

Maintenance releases are generated for Session Server in two types: one MR type for the NCGL platform and another MR type for the SIP Gateway application.

- An NCGL platform MR consists of release notes, CS 2000 NCGL Platform Manager software, NCGL software and optional CS 2000 NCGL Platform Manager patches.

  Using the CS 2000 NCGL Platform Manager GUI you can select an MR image to upgrade from. You can upgrade the Session Server load from the local DVD-ROM drive, from an ISO image located on a remote system, or from a local file on the Session Server disk drive. Space is available on the local hard drive to maintain approximately 2 loads in case fallback to a previous load is necessary. Partial and complete rollbacks of a failed upgrade can be performed.

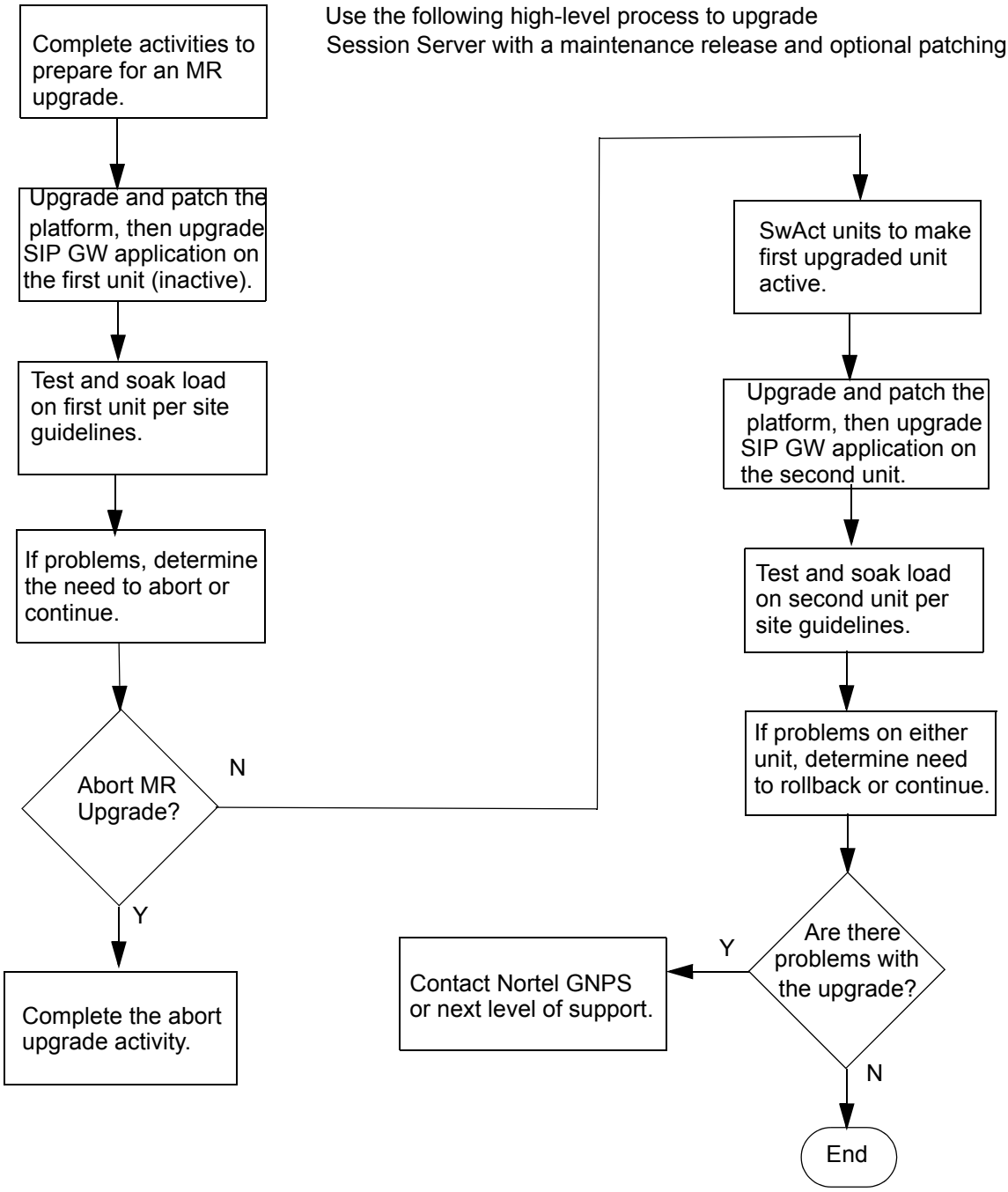
- A SIP Gateway application MR consists of release notes, CS 2000 Session Server Manager software, and SIP Gateway application software.

  Using both the Session Server command line interface (CLI), you can upgrade the SIP Gateway application.

Refer to the following activity diagram for a high-level view of the upgrade process for the Session Server units.

Maintenance release upgrade of Session Server with NCGL patching

Use the following high-level process to upgrade Session Server with a maintenance release and optional patching.



Maintenance release limitations and restrictions

The following general limitations apply when performing a maintenance release upgrade or rollback of an MR upgrade.

- While an MR upgrade is an in-service upgrade, performing a full rollback of an MR upgrade is an out-of-service activity. All call processing and billing information generation is terminated for part of the rollback activity.
- Patches can only be applied using the CLI (command line interface).

Software delivery methods for maintenance releases

MR software is delivered on a data DVD-ROM or using Electronic Software Delivery (ESD) where a compressed ISO image is delivered to an electronic drop-box on the customer network from Nortel Networks.

MR upgrades using ESD delivery require that the MR package be transferred onto both Session Server units and put in the /opt/swd directory using a secure file transfer program such as scp. After the MR upgrade of the NCGL platform the bootload file is stored in the /boot directory.

In order to receive maintenance releases from Nortel Networks using ESD the operating company must have an ESD agreement with Nortel Networks. When the agreement is established, the operating company furnishes Nortel Networks with the location of an electronic dropbox, an email address for notification and a username and password pair for delivering software loads. When Nortel Networks delivers a software load to the dropbox, an electronic mail notification is sent to the E-mail address specified by the operating company.

Software installation methods for maintenance releases

You can upgrade the Session Server NCGL platform load from the local DVD-ROM drive, or from an ISO image located on a remote system, or copied to a local directory. The following upgrade protocols (methods) are selectable from the Session Server Manager GUI:

- Local CDROM - the local DVD-ROM drive (labeled as the local CD-ROM).
- Local file - an iso image, or load.tgz file copied from the local DVD-ROM drive copied to the hard drive using the secure copy program, **scp**, to transfer the data.
- Remote file using FTP or anonymous FTP - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP service. If the

workstation or server is configured to allow anonymous FTP, use anonymous FTP to avoid sending username and password information in cleartext format across the network. This is not a recommended method.

- Remote file using HTTP or HTTPS - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP or HTTPS service. This is not a recommended method.

You can upgrade the Session Server SIP Gateway application from the local DVD-ROM drive, or from an ISO image copied to a local directory. Most of the time the software load for the SIP Gateway application is on the same DVD-ROM disk or copied ISO image as the NCGL platform load; however, some customers may receive a separate maintenance release load that contains an MR only for the SIP Gateway application. Consult your release notes for details.

Prepare for a maintenance release upgrade

Complete the steps for following activity, to prepare for a maintenance release upgrade:

Maintenance release upgrade preparation activity

Step	Procedure or activity
1	If you have purchased security certificates from a Certificate Authority or created self-signed certificates, use procedure Back up security certificates on page 58 to ensure that you have made a backup copy of the security certificate files on both Session Server units and to make a backup to a secure remote server location.
2	Backup the SIP Gateway application database on the active unit using procedure Perform a manual backup of the Session Server database on page 69.
3	Acquire the appropriate maintenance release software from Nortel either using ESD delivery to a customer dropbox/repository server or from a maintenance release DVD-ROM disk.
4	If performing a maintenance release upgrade using an ISO image acquired using ESD, complete procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 71 to copy ISO files to hard drive of each unit.

Maintenance release upgrade preparation activity

Step	Procedure or activity
5	Use procedure View release notes for a release on page 74 to check release notes for the applicability of the MR.
6	Locate and have available the original Session Server software DVD-ROM along with a copy of the existing version of the SIP Gateway application installed on your system. The existing version may be from the last maintenance release image installed from a DVD-ROM or an ESD downloaded image file.
7	Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
8	You have completed this high-level activity.

Perform a maintenance release upgrade

Complete the steps in the order listed, to perform an in-service maintenance release upgrade and optional patching of the NCGL platform and to perform a maintenance release upgrade of the SIP Gateway application.

Maintenance release upgrade activity

Step	Procedure or activity
Upgrade the NCGL platform load on first unit (inactive)	
1	Complete Section Prepare for a maintenance release upgrade on page 31.
2	Determine the version of the NCGL platform load that is currently installed on the Session Server node using procedure Determine the current version of the NCGL platform software load on page 77. Determine the version of the SIP Gateway application software (listed as Session Server load info) that is currently installed on the Session Server node using procedure Determine the current version of software loads on page 80.

Maintenance release upgrade activity

Step	Procedure or activity
3	Compare the current version of the NCGL Platform Load installed with the MR release notes to determine if you must upgrade the NCGL platform load with a newer maintenance release. Also use determine if you need to upgrade to a previously released MR first. If the MR contains a newer version of the NCGL platform load than what is currently installed, then proceed with this upgrade. If not, then you do not need to apply a maintenance release upgrade to this unit. Skip to step 9 to perform any necessary patching of this unit.
4	If applying an MR upgrade using a DVD-ROM, insert the disk into the disk drive of the inactive unit.
5	Log onto the active unit and use procedure Inhibit a system SwAct (Jam) on page 85 to jam the units.
6	Log into the NCGL Platform Manager for the physical unit which is inactive and upgrade the NCGL platform software using procedure Upgrade Session Server NCGL platform software on page 90. For instance, if unit 0 is the active unit, log into the NCGL Platform Manager GUI for unit 1.
7	From the active unit, use procedure Reboot a Session Server unit on page 98 to perform a RebootMate of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.
8	After the inactive unit completes rebooting, log into the inactive unit, use the CS 2000 NCGL Platform Manager and go to the **System Information** page to verify that the Current version of the NCGL software matches the expected new version. Use procedure Determine the current version of the NCGL platform software load on page 77 for assistance with this task.
Apply and commit NCGL patches to the first unit	
9	Use procedure View release notes for a release on page 74 to identify the required NCGL platform patches for the MR.

Maintenance release upgrade activity

Step	Procedure or activity
10	Log onto the active unit and use procedure Inhibit a system SwAct (Jam) on page 85 to verify that the units are jammed. If they are not, then jam the units.
11	Use procedure Acquire patch files on page 139 to copy all required patches from the DVD-ROM disk or the ESD delivered ISO image file to the patching holding directory on the unit.
12	Use procedure Apply and commit an NCGL patch on page 146 to apply and commit NCGL patches to the inactive unit.
Upgrade the SIP Gateway application software on the first unit	
13	If the inactive unit is not already Jammed, Jam it now. On the inactive unit, upgrade the SIP Gateway application software using procedure Upgrade/rollback/reinstall a Session Server application on page 156.
14	From the active unit, use procedure Reboot a Session Server unit on page 98 to perform a RebootMate of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.
15	After the inactive unit completes rebooting, log into the inactive unit's CLI and verify that the current version of the SIP Gateway application matches the expected new version by executing the following command: **cat /opt/apps/webint/version_info.txt**. ***Note:*** If upgrading the SIP Gateway application only, remember to Unjam the inactive unit before SwAct.
Activate and soak the new load on the first unit	
16	From the active unit, verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 164.
17	Use procedure Enable a system SwAct (Unjam) on page 167 to unjam the units.

Maintenance release upgrade activity

Step	Procedure or activity
18	As applicable to your site, test the new software on upgraded unit, still inactive. Testing may include: • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
19	From the active unit perform a SwAct of the units using procedure Invoke a maintenance SwAct of the Session Server platform on page 170.
20	Use procedure Inhibit a system SwAct (Jam) on page 85 to jam the units.
21	As applicable to your site, test new software on upgraded unit, now active. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
22	If all software tests are successful, continue with the next step in this procedure to upgrade the second (mate) Session Server unit (now inactive). Otherwise, if the active unit (with newly upgraded load) experiences problems with call processing, abort this upgrade procedure and complete activity Abort a maintenance release upgrade on page 40 and contact your next level of support or Nortel GNTS.

Maintenance release upgrade activity

Step	Procedure or activity
Upgrade the NCGL platform load on second unit	
23	Verify that all applicable activities in Section Prepare for a maintenance release upgrade on page 31 have been completed for the second unit.
24	Determine what version of the NCGL platform load is currently installed on the second unit using procedure by going to the **System Information** page of the CS 2000 NCGL Platform manager, using procedure Determine the current version of the NCGL platform software load on page 77. Determine what version of the SIP Gateway application software (listed as Session Server load info) is currently installed on the second unit using procedure Determine the current version of software loads on page 80.
25	Compare the current version of the NCGL Platform Load installed with the MR release notes to determine if you must upgrade the NCGL platform load on the second unit with a newer maintenance release. If the MR contains a newer version of the NCGL platform load than what is currently installed, then proceed with this upgrade. If not, then you do not need to apply a maintenance release upgrade to this unit. Skip to step 32 to perform any necessary patching of this unit.
26	If applying an MR upgrade using a DVD-ROM, insert the disk into the disk drive of the inactive unit.
27	Log onto the active unit and use procedure Inhibit a system SwAct (Jam) on page 85 to verify that the units are still jammed. If they are not, then jam the units.
28	Log into the NCGL Platform Manager for the physical unit which is inactive and upgrade the NCGL platform software using procedure Upgrade Session Server NCGL platform software on page 90. For instance, if unit 0 is the active unit, log into the NCGL Platform Manager GUI for unit 1.

Maintenance release upgrade activity

Step	Procedure or activity
29	From the active unit, use procedure Reboot a Session Server unit on page 98 to perform a RebootMate of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.
30	After the inactive unit completes rebooting, log into the inactive unit, use the CS 2000 NCGL Platform Manager and go to the **System Information** page to verify that the Current version of the NCGL software matches the expected new version. Use procedure View the operational status of a Session Server NCGL platform on page 119 for assistance with this task.
Apply and commit NCGL patches to the second unit	
31	Use procedure View release notes for a release on page 74 to identify the required NCGL platform patches for the MR.
32	Log onto the active unit and use procedure Inhibit a system SwAct (Jam) on page 85 to verify that the units are jammed. If they are not, then jam the units.
33	Use procedure Acquire patch files on page 139 to copy all required patches from the DVD-ROM disk or the ESD delivered ISO image file to the patching holding directory on the unit.
34	Use high-level procedure Patching the NCGL operating system on page 50 to apply and commit NCGL patches to the inactive unit.
Upgrade the SIP Gateway application software on the second unit	
35	If the inactive unit is not already Jammed, Jam it now. On the inactive unit, upgrade the SIP Gateway application software using procedure Upgrade/rollback/reinstall a Session Server application on page 156.
36	From the active unit, use procedure Reboot a Session Server unit on page 98 to perform a RebootMate of the inactive unit. Monitor the reboot progress from active unit CS 2000 NCGL Platform Manager.

Maintenance release upgrade activity

Step	Procedure or activity
37	After the inactive unit completes rebooting, log into the inactive unit's CLI and verify that the current version of the SIP Gateway application matches the expected new version by executing the following command: **cat /opt/apps/webint/version_info.txt**.
Activate and soak the new load on the second unit	
38	From the active unit, verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 164
39	Use procedure Enable a system SwAct (Unjam) on page 167 to unjam the units.
40	As applicable to your site, test the new software on the upgraded unit, still inactive. Testing may include: • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
41	From the active unit perform a SwAct of the units using procedure Invoke a maintenance SwAct of the Session Server platform on page 170.
42	As applicable to your site, test new software on the upgraded unit, now active. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.

Maintenance release upgrade activity

Step	Procedure or activity
43	If all software tests are successful, continue with the next step in this activity to upgrade. Otherwise, if the active unit (with newly upgraded load) experiences problems with call processing, abort this upgrade procedure. Go to and complete procedure Rollback a Session Server NCGL platform software upgrade on page 183 and contact your next level of support, Nortel GNPS or Nortel's emergency response team.
44	From the active unit, verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 164
45	Monitor the system for an appropriate period per your site guidelines before declaring this maintenance release complete.
46	You have completed the maintenance release upgrade activity.

Troubleshooting maintenance upgrades

If the system becomes unstable after an upgrade or after aborting an upgrade, contact GNPS for assistance.

Abort a maintenance release upgrade

Complete the steps for the following activity, in the order indicated, to abort a maintenance release upgrade activity in progress.

ATTENTION
This high-level activity assumes that you have not upgraded the second unit in the node with the maintenance release. If you have already upgraded both units with the maintenance release, then contact your next level of support or Nortel GNPS.

Abort maintenance release activity

Step	Procedure or activity
1	If necessary, use procedure Enable a system SwAct (Unjam) on page 167 to unjam the units.
2	If necessary, complete procedure Invoke a maintenance SwAct of the Session Server platform on page 170 to revert call processing to the un-upgraded unit (the unit that is operating with the pre-maintenance release load).
3	Use procedure Inhibit a system SwAct (Jam) on page 85 to jam the units.
4	Log onto the inactive unit and use procedure Rollback a Session Server NCGL platform software upgrade on page 183 to set the default NCGL bootfile to the pre-MR load (the load the unit operated on prior to the maintenance release upgrade).
5	Log into the active Session Server unit, use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a FORCED **RebootMate** of the inactive (mate) unit. Refer to procedure Reboot a Session Server unit on page 98 for assistance. ***Note:*** All committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying patches is not required.
6	On the inactive unit CLI use the pre-MR DVD-ROM or pre-MR SIP Gateway application ISO image to downgrade the SIP Gateway application software using procedure Upgrade/rollback/reinstall a Session Server application on page 156.

Abort maintenance release activity

Step	Procedure or activity
7	Log into the active Session Server unit, use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a reboot (RebootMate) of the inactive unit. Refer to procedure Reboot a Session Server unit on page 98 for assistance.
8	After the inactive unit reboots, go to the active unit and verify that the SIP Gateway application databases on both units have synchronized using procedure Verify synchronization status of Session Server units on page 164.
9	Once the databases are in sync, release the JAM on the units using procedure Enable a system SwAct (Unjam) on page 167.
10	Complete procedure Invoke a maintenance SwAct of the Session Server platform on page 170 to make the downgraded unit active.
11	As applicable to your site, test the software on the downgraded unit, now active. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.

Abort maintenance release activity

Step	Procedure or activity
12	Monitor the system for an appropriate period per your site guidelines before declaring this abort maintenance release activity complete. If all software tests are successful, continue with the next step in this activity. Otherwise, if the active unit (with downgraded load) experiences problems with call processing, perform the following tasks in order: • complete procedure Invoke a maintenance SwAct of the Session Server platform on page 170 • complete procedure Inhibit a system SwAct (Jam) on page 85 • contact your next level of support or Nortel GNPS.
13	You have completed this high-level abort activity.

Perform an emergency maintenance release rollback activity

Complete the steps for following activity, in the order indicated, to roll back a maintenance release upgrade activity that has been performed on both units in the node.

CAUTION

This is a service affecting activity. Performing this rollback activity causes approximately an hour long service interruption to all SIP-related call traffic and billing activity.

Emergency maintenance release rollback activity

Step	Procedure or activity
1	Locate and have available the previous Session Server software DVD-ROM or an ESD downloaded image file of the previous maintenance release. Ensure that you have available a recent backup copy of the SIP application database.
2	If performing a maintenance release rollback using an ISO image acquired using ESD, verify that the applicable ISO files are copied to the hard drive of each unit. If necessary, use procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 71.
3	Log onto the active unit CLI and complete procedure Drop database synchronization for the SIP Gateway application on page 187 executed from the current release of the Session Server software DVD-ROM or from the currently installed ISO image. ***Note:*** Once executed, this script drops call processing and application database synchronization between the active and inactive units. The SIP Gateway application maintains this non-synchronized state until a manual SwAct is performed, later in the procedure.

Emergency maintenance release rollback activity

Step	Procedure or activity
4	Log into the NCGL Platform Manager for the physical unit which is inactive and use procedure Rollback a Session Server NCGL platform software upgrade on page 183 to set the default NCGL bootfile to the pre-MR load (the load the unit operated on prior to the MR upgrade). ***Note:*** All committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying patches is not required.
5	On the inactive unit, rollback the SIP Gateway application software. Complete procedures Upgrade/rollback/reinstall a Session Server application on page 156.
6	Use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a reboot (RebootMate) of the inactive unit. Refer to procedure Reboot a Session Server unit on page 98 for assistance.
7	On the inactive unit, prepare to restore a backup copy of the SIP Gateway application database using procedure Prepare for a database restore on a Session Server unit on page 212. Attention: If an backup version of the database from the previous release is not available, the unit must be recommissioned and the SIP Gateway application reprovisioned.
8	Perform a SwAct (Force) of the units by completing procedure Invoke a maintenance SwAct of the Session Server platform on page 170 to make the downgraded unit active.
9	On the active unit (the rolled back unit), install the backup copy of the SIP Gateway application database using procedure Perform a database restore to a Session Server unit on page 216.

Emergency maintenance release rollback activity

Step	Procedure or activity
10	As applicable to your site, test the software on the downgraded unit, now active. Testing may include: • placing test calls per your site upgrade guidelines • applying a minimum live traffic soak time for the unit per your site upgrade guidelines • Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* and to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
11	Monitor the system for an appropriate period per your site guidelines. If all software tests are successful, continue with the next step in this activity. Otherwise, if the active unit (with rolled back load) experiences problems with call processing, STOP executing this activity and contact your next level of support or Nortel GNPS.
12	Use procedure Inhibit a system SwAct (Jam) on page 85 to jam the units.
13	Log into the NCGL Platform Manager for the physical unit which is inactive and use procedure Rollback a Session Server NCGL platform software upgrade on page 183 to set the default NCGL bootfile to the pre-MR load (the load the unit operated on prior to the MR upgrade). ***Note:*** All committed NCGL patches to the selected release are re-applied by the operating system when the unit is rebooted. Reapplying patches is not required.
14	Use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a reboot (RebootMate) of the inactive unit. Refer to procedure Reboot a Session Server unit on page 98 for assistance.
15	On the inactive unit, rollback the SIP Gateway application software using procedure Upgrade/rollback/reinstall a Session Server application on page 156.

Emergency maintenance release rollback activity

Step	Procedure or activity
16	Use the CS 2000 NCGL Platform Manager and go to the NCGL **Administration** page. Perform a reboot (RebootMate) of the inactive unit. Refer to procedure Reboot a Session Server unit on page 98 for assistance.
17	After the inactive unit reboots, go to the active unit. Verify that the SIP Gateway application databases are synchronizing using procedure Verify synchronization status of Session Server units on page 164. If they are synchronizing then skip to step 19. If they are not synchronizing then go to the next step in this activity.
18	Use procedure View the operational status of a Session Server NCGL platform on page 119 to check the status of the inactive unit to determine why database synchronization is not taking place by reviewing existing faults and logs. Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
19	Once the databases are in sync, release the JAM on the units using procedure Enable a system SwAct (Unjam) on page 167.
20	Perform a SwAct of the units by completing procedure Invoke a maintenance SwAct of the Session Server platform on page 170 to make the downgraded unit active.

Emergency maintenance release rollback activity

Step	Procedure or activity
21	Monitor the system for an appropriate period per your site guidelines before declaring this maintenance release rollback complete. If all software tests are successful, continue with the next step in this activity. Otherwise, if you continue to experience problems with call processing, contact your next level of support or Nortel GNPS.
22	You have completed this emergency rollback activity.

Patching the NCGL operating system

NCGL patching activities occur when new patches become available that must be installed. Any NCGL operating system software not delivered in a standard release or a maintenance release is delivered in a patch file. Patching can also occur when an older patch becomes obsolete and must be removed. Installing some patches may be optional.

A patch is a single file that contains the executables, libraries, data, scripts, dependency information and special instructions necessary to apply and remove the patch. Patching commands, run from the root account, are used to install and uninstall patches. Many patches can be applied without any impact to call processing, but some application patches must coordinate with call processing to be applied or removed successfully. Any patch can be applied on the inactive side of the Session Server without impact to active call processing. Consult the patch release notes or administrative file for details.

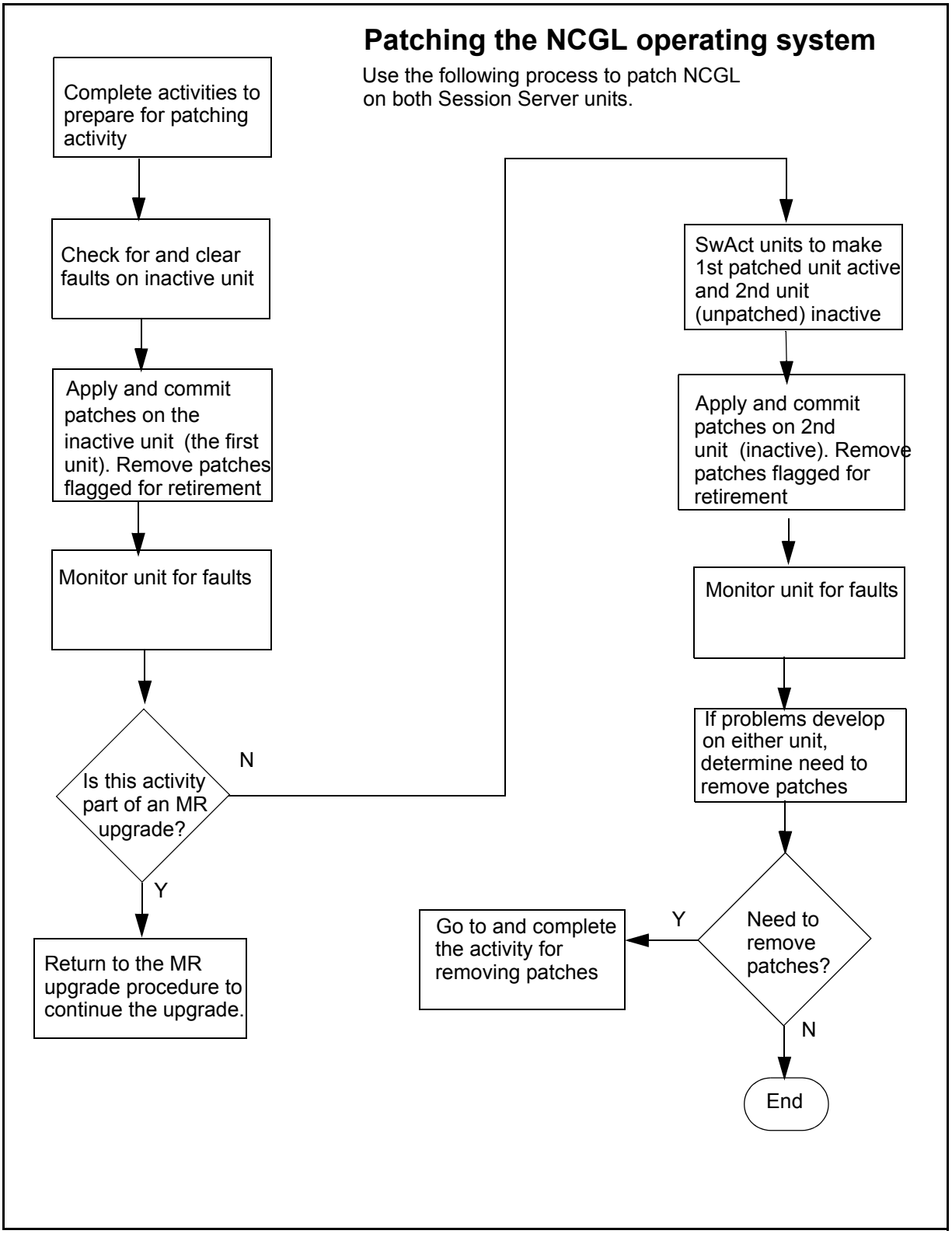
Patching strategy

Although most patch files apply to any Nortel customer site, some patch files are created for a particular customer's site-specific installation. Not all patches made available apply to all customer sites. Contact Nortel GNPS customer support if you are concerned about which patches are applicable to your site.

Both units in the Session Server node must be patched when applying patches. Each unit is usually patched separately while it is operating in standby mode. When patching the units, apply and commit the patch to the inactive unit first, then check logs and system status before SwActing the units. Check the logs and status for some period of time to ensure there are no patch-related events. After a time designated by your site guidelines, apply and commit the patch the newly inactive (unpatched) unit and check for logs and system status again. Refer to the following activity diagram for a high-level view of the patching process for the Session Server.

Patching the NCGL operating system

Use the following process to patch NCGL on both Session Server units.



Patching limitations

Patches can only be applied using the CLI (command line interface).

Delivery methods for patch files

Patch files may be released at any time. They may also be made available with a major upgrade or during a maintenance release. Patch files can be acquired in the following ways:

- the http://www.nortel.com website by accessing the Technical Support portal and selecting Software Downloads. Search under the Carrier VoIP product family for Next Generation Session Server.
- the DVD-ROM software disk, sent to the customer site, that has the installation software or maintenance release software.
- a patching CD-ROM sent to the customer site.
- a customer dropbox service where Nortel delivers patches to a customer-based interface server that is accessible from the internet. The patch files are transferred from the customer-based interface server to the Session Server units by the customer network administrator or other trained personnel.

Locating existing patch files on the Session Server units

NCGL patch files are stored in the /patching/patchholding directory on each unit that is to be patched.

Prepare for NCGL patching activities

Complete the steps for following activity, in the order indicated, to prepare for standalone NCGL patching activities, outside of any upgrade activity:

Patching preparation activity

Step	Procedure or activity
1	If you are applying NCGL patches while performing a maintenance release upgrade, then skip this step. If you have purchased security certificates from a Certificate Authority or created self-signed certificates, use procedure Back up security certificates on page 58 to ensure that you have made a backup copy of the security certificate files on both Session Server units and to make a backup to a secure remote server location.
2	Backup the SIP Gateway application database on active unit using procedure *Performing a backup of the Session Server database*, found in the Session Server Security and Administration NTP, NN10346-611.
3	Acquire patch files from Nortel either using ESD delivery or from a patch or maintenance release DVD-ROM disk.
4	Use procedure View release notes for a release on page 74 to check release notes to identify the required NCGL patches for your load. Also note any patches that are retired and must be removed. Verify if any previously installed patches must first be removed before installing new patches.
5	For NCGL patching only, use procedure Acquire patch files on page 139 to copy the NCGL patch files from a CD/DVD to the /patching/patchholding directory.
6	For NCGL patching, complete procedure Query status of NCGL patches on page 143 to ensure that the NCGL patch files being added or removed from the unit have been copied to the unit's hard drive.

Patching preparation activity

Step	Procedure or activity
7	Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
8	You have completed this high-level activity.

Apply and commit NCGL patches

Complete the steps for following activity, in the order indicated, to patch both of the Session Server units:

Note: This high-level activity may be part of a high-level maintenance release upgrade activity.

NCGL patch application activity

Step	Procedure or activity
1	Ensure that you have first completed section Prepare for NCGL patching activities on page 53.
2	Use procedure Inhibit a system SwAct (Jam) on page 85 to jam the units.
3	Complete procedure Apply and commit an NCGL patch on page 146 on the inactive unit.
4	Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
5	If you were directed to this patching activity from activity *Applying a maintenance release upgrade* in the Session Server Upgrades NTP, NN10349-461, return to that high level activity now. Otherwise continue with the next step in this activity.

NCGL patch application activity

Step	Procedure or activity
6	Release the JAM on the units using procedure Enable a system SwAct (Unjam) on page 167.
7	Complete procedure Invoke a maintenance SwAct of the Session Server platform on page 170.
8	Use procedure Inhibit a system SwAct (Jam) on page 85 to jam the units.
9	Repeat procedure Apply and commit an NCGL patch on page 146 for the second (mate) Session Server unit, now the new standby unit.
10	Release the JAM on the units using procedure Enable a system SwAct (Unjam) on page 167.
11	Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
12	You have completed this high-level activity.

Remove NCGL patches

Complete the steps for following activity, in the order indicated, to remove patches from one or both Session Server units:

ATTENTION

Under normal operating conditions patches must be removed from both units. Exceptions to this case may be when a patch is being tested on a single unit before being committed and installed on the second unit.

NCGL patch removal activity

Step	Procedure or activity
1	Use procedure Inhibit a system SwAct (Jam) on page 85 to jam the units.
2	Complete procedure Remove an NCGL patch on page 149 on the inactive unit.
3	Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
4	Use procedure Enable a system SwAct (Unjam) on page 167 to unjam the units.
5	Complete procedure Invoke a maintenance SwAct of the Session Server platform on page 170.
6	Repeat procedure Remove an NCGL patch on page 149 for the second (mate) Session Server unit, now the new standby unit.
7	Refer to the Session Server Fault Management NTP, NN10332-911, and use procedures *View Session Server alarms* and *View Session Server logs* to check the status of both units by reviewing existing faults and logs. Clear all alarms and verify normal functioning of both units before continuing.
8	You have completed this high-level activity.

1 Individual procedures

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

Back up security certificates

Purpose of this procedure

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

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

Limitations and Restrictions

There are no limitations on performing this procedure.

Prerequisites

There are no prerequisites for this procedure.

Action

Perform the following steps to complete this procedure.

At the Session Server CLI or Integrated EMS client

1 Log on to the Session Server unit that has the security certificates you need to back up, and change to the root user.

If you are performing this procedure outside of a high-level task, back up the security certificates on both units. Otherwise, back up the security certificates on the unit indicated in the high-level task that directed you to this procedure.

2 Change directories to the /opt/base/share/ssl directory. Type

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

and press the Enter key.

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

```
$ mkdir <SNxx_ddmmyyyy>
```

and pressing the Enter key.

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 by typing

```
# cp * <SNxx_ddmmyyyy>
```

and press the Enter key.

where

SNxx_ddmmyyyy
is the name of the new backup directory

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

5 Use the following table to determine your next step:

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

6 Secure copy the server.key file to the remote server by typing

```
$ scp server.key <user>@<remote_server>:</path>
```

and pressing the Enter key.

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 server.key file is copied to the remote server.

7 Secure copy the certificate.keystore file to the remote server by typing

```
$ scp certificate.keystore
<user>@<remote_server>:</path>
```

and pressing the Enter key.

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 certificate.keystore file is copied to the remote server.

8 Secure copy the server.crt file to the remote server by typing

```
$ scp server.crt <user>@<remote_server>:</path>
```

and pressing the Enter key.

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 server.crt file is copied to the remote server.

9 If you have a CA-signed certificate, secure copy the trusted.crt file to the remote server by typing

```
$ scp trusted.crt
<user>@<remote_server>:/<path>
```

and pressing the Enter key.

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 trusted.crt file is copied to the remote server.

10 You have completed this procedure.

Prepare to validate a certificate chain

Purpose of this procedure

Use the following procedure to migrate certificate authority (CA)-signed security certificates during an upgrade from SN07. If not upgrading from SN07, do not use this procedure.

This procedure cannot be performed on self-signed certificates. Migrating self-signed certificates is not supported. If your site uses self-signed certificates, you must create new ones during the upgrade activity.

Limitations and Restrictions

The following restrictions apply to migrating CA-signed certificates:

- Only PEM formatted, CA-signed certificates are supported on Session Server.
- A CA-chain is required in PEM format in a trusted.crt file, top down, with the root CA at the top. Refer to section Additional information about trusted certificates on page 63 for more information.

Prerequisites

Existing CA-signed security certificates must be prepared per section Additional information about trusted certificates on page 63.

Action

Perform the following steps to complete this procedure.

At the Session Server CLI or Integrated EMS client

1. Log onto the inactive Session Server unit and change to the root user.
2. Ensure that the local server CA-signed certificate that was obtained from the certificate authority is in the file /opt/base/share/ssl/server.crt.
3. Ensure that the private key corresponding to the local server CA-signed certificate is in the file /opt/base/share/ssl/server.key.

ATTENTION

There can only be one certificate in the server.crt file and that certificate must be in PEM format.

Note: Refer to section Additional information about trusted certificates on page 63 for assistance with this task.

4 From the certificate authority, obtain the CA certificate chain, with the root CA-certificate, in top down format, in the file /opt/base/share/ssl/trusted.crt file. This chain can be obtained from the certificate authority directly.

ATTENTION
The trusted.crt certificate must be in PEM format.

5 Verify successful preparation of the certificate files by typing

```
openssl verify /opt/base/share/ssl/trusted.crt
/opt/base/share/ssl/server.crt
```

and press the Enter key.

6 If the result from step 5 is “OK”, you are ready to proceed with the upgrade preparation. If the result from step 5 is not “OK”, then there was problem with the security certificates and you must contact Nortel GNPS.

7 The procedure is complete.

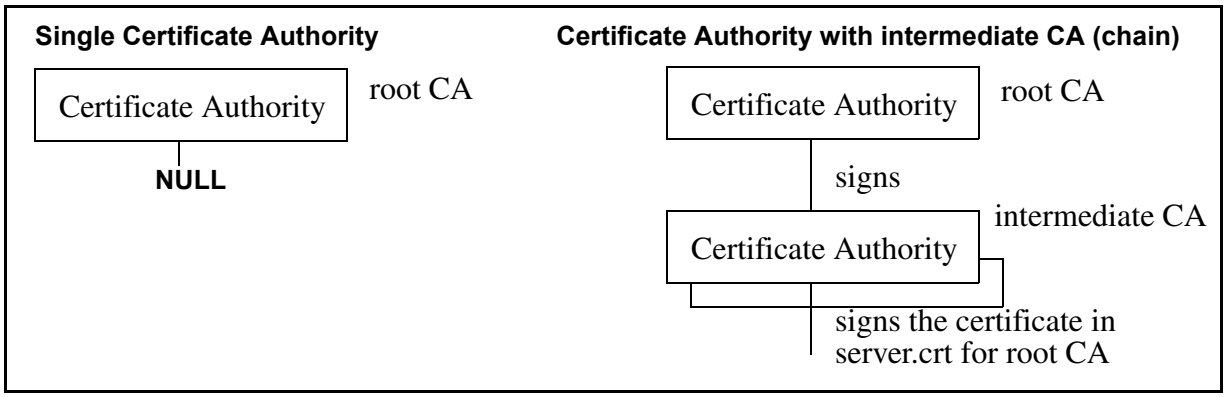
Additional information about trusted certificates

The following section provides additional information about trusted certificates and root CAs.

Root CAs that do not correspond to the local server certificate are not placed in the trusted.crt file. They are added using the CS 2000 Session Server Manger GUI using procedure *Manage Trusted Certificates*, found in the Session Server Security and Administration NTP, NN10346-611. Only the Root CA corresponding to the local certificate is placed in the trusted. crt file, followed by the CA chain. For example, if the local certificate is signed by one of the global public root certificate authorities, then that root CA certificate is placed in this file.

The following figure shows an example of the structure of a trusted.crt file. The trusted.crt on the left shows a single CA signing the root certificate. The trusted.crt on the right shows the certificate of the Certificate Authority (CA), followed by each intermediate chain CA, followed by the CA which ultimately signed the local certificate.

Structure of a trusted.crt file



The following is an example of a CA-signed trusted.crt file. In this case, it is a chain composed of a root CA, followed by 3 (three) intermediate chain CAs. At the top of the file is certificate of the root Certificate Authority (CA), followed by each intermediate chain CA, followed by that last CA which ultimately signed the local certificate.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Timbuktu, O=Nortel Networks,
OU=Certificate Authority
        Validity
            Not Before: Oct  8 01:14:48 2004 GMT
            Not After : Oct  8 01:14:48 2005 GMT
        Subject: C=CA, ST=Ontario, L=Timbuktu, O=Nortel Networks,
OU=Certificate Authority
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                00:bc:53:2a:bd:bf:36:87:36:5b:12:93:a7:55:84:
                 1d:3b:75:0f:d9:de:d6:34:d3:51:8d:96:c6:41:c6:
                      80:b3:08:18:e7:b1:e5:af:0a:00:1d:65:82:77:0a:
                ca:7d:74:00:79:85:d6:80:07:79:8d:ec:b0:e3:6e:
                8c:d0:a7:20:6f:c7:3b:df:09:83:93:36:9f:eb:67:
                  c1:e2:ab:a5:ed:ab:3a:d8:97:ad:83:bf:8c:11:02:
                     12:3b:dc:a9:82:0d:f3:45:d7:8a:ae:96:eb:17:26:
                  3c:de:7a:cd:91:71:b9:56:c7:e7:0c:7a:5e:57:62:
                9c:d7:3e:41:82:c9:f3:34:1d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:

90:20:BC:77:DD:64:50:D7:50:56:5D:C7:3F:EC:7A:32:21:0F:AE:F4
            X509v3 Authority Key Identifier:

keyid:90:20:BC:77:DD:64:50:D7:50:56:5D:C7:3F:EC:7A:32:21:0F:AE:F4
                DirName:/C=CA/ST=Ontario/L=Timbuktu/O=Nortel
Networks/OU=Certificate Authority
                serial:00

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: md5WithRSAEncryption
```

```
        33:65:6c:d0:0d:b8:7f:58:1c:33:1c:d2:4e:e3:19:2d:36:c3:
        15:7f:b3:80:cb:22:2a:dc:eb:ba:84:50:24:7c:cc:07:49:62:
        f5:2c:f9:bc:47:04:56:ea:bd:78:de:44:43:22:e2:1c:5f:fc:
        17:91:80:70:f3:29:e2:74:46:8d:3d:ac:fa:63:f2:b4:ba:79:
        d2:22:76:6c:2e:fb:e6:55:16:6f:db:27:5f:e3:ff:32:84:5a:
        b7:a3:9c:c4:73:f9:72:c2:8b:6e:8d:4f:bf:d2:3f:b1:51:48:
        b5:4e:27:b4:bb:80:4b:87:f9:e7:18:ba:63:20:ac:6d:25:c2:
        74:1b

-----BEGIN CERTIFICATE-----
MIIDGDCCAoGgAwIBAgIBADANBgkqhkiG9w0BAQQFADBsMQswCQYDVQQGEwJDQTEQ
MA4GA1UECBMHT250YXJpbzERMA8GA1UEBxMIVGltYnVrdHUxGDAWBgNVBAoTD05v
cnRlbCBOZXR3b3JrczEeMBwGA1UECxMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTA0MTAwODAxMTQ0OFoXDTA1MTAwODAxMTQ0OFowbDELMAkGA1UEBhMCQ0ExEDAO
BgNVBAgTB09udGFyaW8xETAPBgNVBAcTCFRpbWJ1a3R1MRgwFgYDVQQKEw9Ob3J0
ZWwgTmV0d29ya3MxHjAcBgNVBAsTFUNlcnRpZmljYXRlIEF1dGhvcml0eTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAvFMqvb82hzZbEpOnVYQdO3UP2d7WNNNR
jZbGQcaAswgY57HlrwoAHWWCdwrKfXQAeYXWgAd5jeyw426M0Kcgb8c73wmDkzaf
62fB4qul7as62Jetg7+MEQISO9ypgg3zRdeKrpbrFyY83nrNkXG5VsfnDHpeV2Kc
1z5BgsnzNB0CAwEAAaOByTCBxjAdBgNVHQ4EFgQUkCC8d91kUNdQVl3HP+x6MiEP
rvQwgZYGA1UdIwSBjjCBi4AUkCC8d91kUNdQVl3HP+x6MiEPrvShcKRuMGwxCzAJ
BgNVBAYTAkNBMRAwDgYDVQQIEwdPbnRhcmlvMREwDwYDVQQHEwhUaW1idWt0dTEY
MBYGA1UEChMPTm9ydGVsIE5ldHdvcmtzMR4wHAYDVQQLExVDZXJ0aWZpY2F0ZSBB
dXRob3JpdHmCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQQFAAOBgQAzZWzQ
Dbh/WBwzHNJO4xktNsMVf7OAyyIq3Ou6hFAkfMwHSWL1LPm8RwRW6r143kRDIuIc
X/wXkYBw8ynidEaNPaz6Y/K0unnSInZsLvvmVRZv2ydf4/8yhFq3o5zEc/lywotu
jU+/0j+xUUi1Tie0u4BLh/nnGLpjIKxtJcJ0Gw==
-----END CERTIFICATE-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Timbuktu, O=Nortel Networks,
OU=Certificate Authority
        Validity
            Not Before: Oct  8 01:19:20 2004 GMT
            Not After : Oct  8 01:19:20 2005 GMT
        Subject: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
OU=Chain1, CN=Chain1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c5:d9:e9:4d:aa:87:56:ce:b0:ba:17:fb:fd:78:
                    89:85:54:21:5b:2e:e8:71:e8:14:64:00:dd:b5:2e:
                    0b:2a:e5:75:71:c2:42:17:29:e7:44:79:b0:2a:82:
                    05:5b:92:c1:f3:5a:72:90:72:ee:ec:b1:77:39:cf:
                    3c:c3:92:6a:6d:49:41:43:96:4c:e9:f6:3f:c3:3a:
                    d9:79:11:ff:aa:74:ba:31:71:b3:0e:f0:f8:20:21:
                    3c:76:5b:ad:6b:b6:27:2a:27:86:99:06:3a:1c:81:
                    a5:ca:7c:68:36:cd:45:bd:2f:48:b0:5e:03:75:6e:
                    35:95:42:60:3e:6e:f5:bc:35
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        99:56:1b:2f:2f:b0:5f:4f:a5:7b:70:ce:6c:41:d3:36:20:2c:
        31:fb:61:df:81:58:81:4c:7f:30:a8:e1:d8:c7:97:0b:ad:19:
        21:19:79:ba:90:9f:3d:38:a0:66:6d:0a:6e:47:16:7f:4c:5b:
        7d:5b:bd:21:23:bc:15:27:e9:e5:f5:ec:6b:38:67:69:4e:86:
        82:a9:c0:f5:8a:c4:39:f7:98:89:ac:45:3f:a1:c9:47:26:9b:
        54:d2:d4:9d:d2:dd:c8:4f:58:cf:7c:57:d8:10:6d:d4:3e:3e:
        0a:12:1f:54:d7:f5:38:43:3d:f7:09:8e:33:b5:a1:80:00:14:
        50:f0

-----BEGIN CERTIFICATE-----
```

```
MIICXjCCAcegAwIBAgIBATANBgkqhkiG9w0BAQUFADBsMQswCQYDVQQGEwJDQTEQ
MA4GA1UECBMHT250YXJpbzERMA8GA1UEBxMIVGltYnVrdHUxGDAWBgNVBAoTD05v
cnRlbCBOZXR3b3JrczEeMBwGA1UECxMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTA0MTAwODAxMTkyMFoXDTA1MTAwODAxMTkyMFowbDELMAkGA1UEBhMCQ0ExEDAO
BgNVBAgTB09udGFyaW8xDzANBgNVBAcTBk90dGF3YTEYMBYGA1UEChMPTm9ydGVs
IE5ldHdvcmtzMQ8wDQYDVQQLEwZDaGFpbjExDzANBgNVBAMTBkNoYWluMTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxdnpTaqHVs6wuhf7/XiJhVQhWy7ocegU
ZADdtS4LKuV1ccJCFynnRHmwKoIFW5LB81pykHLu7LF3Oc88w5JqbUlBQ5ZM6fY/
wzrZeRH/qnS6MXGzDvD4ICE8dluta7YnKieGmQY6HIGlynxoNs1FvS9IsF4DdW41
lUJgPm71vDUCAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
gQCZVhsvL7BfT6V7cM5sQdM2ICwx+2HfgViBTH8wqOHYx5cLrRkhGXm6kJ89OKBm
bQpuRxZ/TFt9W70hI7wVJ+nl9exrOGdpToaCqcD1isQ595iJrEU/oclHJptU0tSd
0t3IT1jPfFfYEG3UPj4KEh9U1/U4Qz33CY4ztaGAABRQ8A==
-----END CERTIFICATE-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
OU=Chain1, CN=Chain1
        Validity
            Not Before: Oct  8 01:22:23 2004 GMT
            Not After : Oct  8 01:22:23 2005 GMT
        Subject: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
OU=Chain2, CN=Chain2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:bf:8a:b7:44:9c:92:b5:fd:f0:e7:d3:1c:9d:65:
                    c4:e3:8c:cb:d3:60:a0:9d:bc:d7:87:15:d1:f0:68:
                    3c:71:be:2e:8d:2f:d0:7e:f6:95:2f:f3:89:b4:9b:
                    b6:c9:bd:52:62:8d:05:e3:71:3e:d5:c1:50:27:67:
                    01:f4:8b:7e:c9:6d:4e:a5:24:ff:d7:80:37:86:09:
                    8c:0a:8d:79:cc:b2:e6:9e:d8:7d:71:db:12:e6:84:
                    7e:2f:90:17:ca:84:87:9b:63:72:4a:28:d7:75:91:
                    f1:4f:c2:6b:5e:a7:d2:2b:01:60:f7:5f:35:dd:8e:
                    92:d7:b7:f5:a4:66:f6:af:21
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        3c:0c:fa:58:1f:14:d3:3f:f1:cb:80:7b:8f:bb:f7:17:e5:18:
        21:bd:a2:77:3e:ce:5d:4c:80:a8:3e:7e:a1:9c:fe:c8:6a:d0:
        7d:67:45:b9:5a:a6:89:3a:2f:de:25:20:2f:ed:62:b5:06:8f:
        dd:a1:85:aa:a2:a3:8d:a3:6d:4c:5e:ed:e8:35:f3:50:98:26:
        99:38:1c:33:a3:99:0a:50:11:f8:0e:21:9d:fe:56:fb:ec:b9:
        55:ed:83:a7:b0:a4:26:82:7f:12:3b:35:9c:03:b9:40:02:3d:
        5c:d5:34:e2:ee:ff:91:58:9f:9d:cf:2e:91:35:9d:c8:5a:f1:
        19:59

-----BEGIN CERTIFICATE-----
MIICXjCCAcegAwIBAgIBAjANBgkqhkiG9w0BAQUFADBsMQswCQYDVQQGEwJDQTEQ
MA4GA1UECBMHT250YXJpbzEPMA0GA1UEBxMGT3R0YXdhMRgwFgYDVQQKEw9Ob3J0
ZWwgTmV0d29ya3MxDzANBgNVBAsTBkNoYWluMTEPMA0GA1UEAxMGQ2hhaW4xMB4X
DTA0MTAwODAxMjIyM1oXDTA1MTAwODAxMjIyM1owbDELMAkGA1UEBhMCQ0ExEDAO
BgNVBAgTB09udGFyaW8xDzANBgNVBAcTBk90dGF3YTEYMBYGA1UEChMPTm9ydGVs
IE5ldHdvcmtzMQ8wDQYDVQQLEwZDaGFpbjIxDzANBgNVBAMTBkNoYWluMjCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAv4q3RJyStf3w59McnWXE44zL02CgnbzX
hxXR8Gg8cb4ujS/QfvaVL/OJtJu2yb1SYo0F43E+1cFQJ2cB9It+yW1OpST/14A3
hgmMCo15zLLmnth9cdsS5oR+L5AXyoSHm2NySijXdZHxT8JrXqfSKwFg91813Y6S
17f1pGb2ryECAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
gQA8DPpYHxTTP/HLgHuPu/cX5RghvaJ3Ps5dTICoPn6hnP7IatB9Z0W5WqaJOi/e
JSAv7WK1Bo/doYWqoqONo21MXu3oNfNQmCaZOBwzo5kKUBH4DiGd/lb77LlV7YOn
sKQmgn8SOzWcA7lAAj1c1TTi7v+RWJ+dzy6RNZ3IWvEZWQ==
-----END CERTIFICATE-----
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
OU=Chain2, CN=Chain2
        Validity
            Not Before: Oct  8 01:24:40 2004 GMT
            Not After : Oct  8 01:24:40 2005 GMT
        Subject: C=CA, ST=Ontario, L=Ottawa, O=Nortel Networks,
OU=Chain3, CN=Chain3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:9e:10:4a:52:3a:e3:27:cc:0f:bb:70:a0:dc:66:
                    df:27:47:17:54:4c:56:1e:f1:7c:6e:71:e6:b0:f1:
                    7e:2d:a3:32:e0:c1:a4:50:5e:3a:cf:eb:09:ac:f5:
                    00:f4:25:a5:ae:59:3d:b0:e5:02:af:ec:d8:b2:e5:
                    c3:31:35:d0:d0:14:35:7d:c9:85:ef:fc:b3:c4:05:
                    0b:06:b4:b9:67:53:4d:0b:e9:c8:f1:a0:44:ac:6f:
                    27:4c:71:6f:be:31:63:12:21:4d:4b:a8:58:97:67:
                    c0:e4:1f:bb:d2:fe:4d:d6:48:3c:19:c6:fb:db:2a:
                    4e:1d:bf:f4:b4:41:23:69:c5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        bd:1b:08:a2:9f:af:f4:3e:3e:b6:72:e4:ca:ec:89:c5:fe:e4:
        fd:99:b9:a4:31:b9:58:64:83:df:b5:8e:d3:97:89:c3:e8:0c:
        96:0b:9d:c2:cc:81:b1:cd:78:17:13:ad:28:e8:ae:4d:2b:0e:
        1b:b7:96:e2:74:65:23:02:5a:b1:e6:90:89:cf:9b:3c:c1:b5:
        44:6f:ac:05:0d:d7:86:cc:eb:ce:ea:36:12:5a:3b:44:ac:f9:
        0e:44:f5:c0:23:ff:55:1f:ef:1d:64:04:82:f2:7b:cc:22:25:
        49:e4:a5:74:8c:9a:1d:22:5c:a7:7e:04:12:90:c9:88:d6:f4:
        a2:b0
-----BEGIN CERTIFICATE-----
MIICXjCCAcegAwIBAgIBAzANBgkqhkiG9w0BAQUFADBsMQswCQYDVQQGEwJDQTEQ
MA4GA1UECBMHT250YXJpbzEPMA0GA1UEBxMGT3R0YXdhMRgwFgYDVQQKEw9Ob3J0
ZWwgTmV0d29ya3MxDzANBgNVBAsTBkNoYWluMjEPMA0GA1UEAxMGQ2hhaW4yMB4X
DTA0MTAwODAxMjQ0MFoXDTA1MTAwODAxMjQ0MFowbDELMAkGA1UEBhMCQ0ExEDAO
BgNVBAgTB09udGFyaW8xDzANBgNVBAcTBk90dGF3YTEYMBYGA1UEChMPTm9ydGVs
IE5ldHdvcmtzMQ8wDQYDVQQLEwZDaGFpbjMxDzANBgNVBAMTBkNoYWluMzCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAnhBKUjrjJ8wPu3Cg3GbfJ0cXVExWHvF8
bnHmsPF+LaMy4MGkUF46z+sJrPUA9CWlrlk9sOUCr+zYsuXDMTXQ0BQ1fcmF7/yz
xAULBrS5Z1NNC+nI8aBErG8nTHFvvjFjEiFNS6hYl2fA5B+70v5N1kg8Gcb72ypO
Hb/0tEEjacUCAwEAAaMQMA4wDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
gQC9Gwiin6/0Pj62cuTK7InF/uT9mbmkMblYZIPftY7Tl4nD6AyWC53CzIGxzXgX
E60o6K5NKw4bt5bidGUjAlqx5pCJz5s8wbVEb6wFDdeGzOvO6jYSWjtErPkORPXA
I/9VH+8dZASC8nvMIiVJ5KV0jJodIlynfgQSkMmI1vSisA==
-----END CERTIFICATE-----
```

Perform a manual backup of the Session Server database

Purpose of this procedure

Use this procedure to perform a backup of the active Session Server unit SIP Gateway application database. Use this procedure to make regular backup copies of the database or as a precautionary activity before starting any type of upgrade to the SIP Gateway application. This procedure may be used as a standalone task or as part of a higher level upgrade activity.

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.

Prerequisites

ATTENTION

The SIP Gateway application database must be in sync with the CS 2000 to ensure an accurate copy of the active unit database is created. Verify this condition using procedure Verify synchronization status of Session Server units on page 164.

Action

At the Session Server CLI or Integrated EMS client

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

2 Change directory to the database directory by typing

```
# cd /opt/apps/database/solid/dbfiles
```

and pressing the Enter key.

3 Put a copy of the database for the active unit in the backup directory by typing

```
# cp solid.db  /opt/apps/database/solid/backup
```

and pressing the Enter key.

Note: If other backup copies of the database exist with the same filename, you have the option of deleting those files or putting the backup copy into the backup directory under a new file name.

Example

```
# cp solid.db
/opt/apps/database/solid/backup/solid.db.backup1
```

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

Use the unix **scp** command to make a secure copy of the backup database file to a secure, remote server on your network. This server should be continuously available for cases where a restoration of the SIP Gateway application database become necessary, such as during an upgrade rollback. A root password for the remote server may be required.

5 You have completed this procedure.

Extract an ISO image from an Electronic Software Delivery (ESD)

Purpose of this procedure

Use this procedure to extract an ISO image, patch files and release notes for a major upgrade or maintenance release archive file retrieved from an electronic software delivery dropbox. This procedure can be used as a standalone task or as part of higher level activity.

Prerequisites

Ensure that the ESD software archive file has been transferred from the dropbox on the repository server. The repository server is the machine owned by the operating company that was selected to be the destination for the ESD software files.

Your existing Regional Customer Service Team has knowledge of your ESD implementation methodology. You can also contact the technical assistance support (TAS) hotline after hours for any urgent issues related to ESD.

For more information about how your site's ESD is implemented, contact your site network administrator. Also, refer to the Carrier Voice over IP Network Upgrade Overview NTP, NN10440-450 and the document Electronic Software Delivery Customer Implementation Guide, found on your solution CD.

Restrictions and Limitations

This procedure must be completed on both the active and inactive units.

Action

At the Session Server CLI or Integrated EMS client

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

2 Change directory to the location of the ESD software archive file by typing

```
$ cd /opt/swd
```

and pressing the Enter key.

3 Ensure that enough disk space is available for the extracted ISO image by typing

```
$ df -h /opt/swd
```

and pressing the Enter key.

Ensure that the value in field Avail is at least 350. This ensures that at least 350 Megabytes are available. In the example that follows, 1013 Megabytes are available.

```
[root@hostname swd]# df -h /opt/swd
Filesystem            Size  Used Avail Use% Mounted on
/dev/ntvg/_opt_swd   1014M  364k 1013M   1% /opt/swd
[root@hostname swd]#
```

4 Uncompress the ESD software load from the ESD archive file by typing

`$ tar xvzf <ESD_ISOfilename>.tar.gz`

and pressing the Enter key.

where

`<ESD_ISOfilename>`
is the file name of the ESD delivered upgrade file

Example
$ tar xvzf NGSS0080.80.P.NCL.NAP.VAULT.6.D.tar.gz

The ESD software load is unarchived, and a new directory named after the ESD software filename is created. The directory name is the name of the ESD filename without the .tar.gz suffix. The contents of the ESD software load are placed in this new directory.

5 Change directory to the newly created directory by typing

`$ cd <ESD_ISO_directory>`

and pressing the Enter key.

where

`<ESD_ISO_directory>`
is the file name of the ESD delivered upgrade file

Example
$ cd NGSS0070.70.P.NCL.NAP.VAULT.6.D

6 Verify that the image file exists in the directory by typing

`$ ls -l`

and pressing the Enter key.

The system responds with a long listing of files in the directory including the ISO image file, any applicable patch files and the release notes file.

7 Mount the image file to mount point `/cdrom` by typing

`mount -t iso9660 -o loop <image>.iso.tape /cdrom`

Example
mount -t iso9660 -o loop NGSS08_NCL.iso.tape /cdrom

The command prompt returns upon success and the contents of the image are available from the /cdrom mount point.

8 List the contents of the ISO by typing

`cd /cdrom`
`ls -l`

The system responds with a list of files in the ISO image including any applicable patch files and the release notes file.

```
[root@hostname cdrom]# ls -l
total 19361
-r-xr-xr-x    1 208126   4848         5005 Mar 22 17:36 InstallApps
drwxrwxrwx    2 208126   4848         6144 Mar 22 17:36 Tools
-r-xr-xr-x    1 208126   4848           33 Feb 23 18:09 buildversion
drwxrwxrwx    2 208126   4848         2048 Feb 23 18:09 isolinux
-r-xr-xr-x    1 208126   4848     19810925 Feb 23 18:09 load.tgz
```

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

The NCGL software is available for install by selecting Local CDROM from the Software Upgrade area of the Services web page.

The SIP Gateway application software is available for install by logging in to the unit and running the InstallApps script from the `/cdrom` directory.

Note: Repeat this procedure on the second unit before beginning the software upgrade.

View release notes for a release

Purpose of this procedure

Use this procedure to view the release notes for a major upgrade, maintenance release or patching release. This procedure can be used as a standalone task or as part of a higher level activity.

Limitations and Restrictions

There are no restrictions for performing this procedure.

Prerequisites

If reading release notes from a CD/DVD disk, ensure that the maintenance release or major release CD/DVD-ROM disk is inserted into the inactive unit DVD-ROM drive.

If reading release notes from an ESD delivered ISO archive file, ensure the software archive file, which includes the release notes, has been extracted and put in the /opt/swd directory on the inactive unit, and that the image file has been mounted to mount point /cdrom. If required, refer to procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 71.

Action

At the Session Server CLI or Integrated EMS client

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

2 Use the following table to determine your first step.

If media is delivered by	Do
ESD	step 3.
CD/DVD disk	step 4.

3 Ensure the software archive file, which includes the release notes, has been extracted and put in the /opt/swd directory on the inactive unit, and that the image file has been mounted to mount point /cdrom. If required, refer to procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 71.

When complete, return to this procedure, and proceed to step 7.

4 Insert the CD/DVD-ROM disk into the DVD-ROM disk drive of the inactive unit.

5 At the prompt, type

```
$ cd /
```

and press Enter.

6 Mount the DVD-ROM drive by typing

```
$ mount /cdrom
```

and pressing the Enter key.

7 Change directories to the mounted filesystem by typing

```
$ cd /cdrom
```

and pressing the Enter key.

8 Locate the release notes file by typing

```
$ ls
```

and pressing the Enter key.

If release notes are available, they are listed as a .pdf file with the rest of the files.

9 Transfer the release notes file from the unit and then open the file with a viewer that reads .pdf format files.

Note: It may be necessary to transfer the release notes .pdf file (/cdrom/pdf) using FTP to an OAMP node in the network, and then transfer the pdf file to a PC with Adobe Acrobat Reader.

10 When you have finished reviewing the release notes file, change directories out of the mounted DVD-ROM filesystem by typing

```
$ cd /
```

and pressing the Enter key.

11 Unmount the DVD-ROM drive by typing

```
$ umount /cdrom
```

and pressing the Enter key.

12 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.

Determine the current version of the NCGL platform software load

Purpose of this procedure

Use this procedure to determine the version of the NCGL platform software load for a Session Server unit, regardless of installed application software. This procedure can be used as a standalone task or as part of a higher level activity.

Limitations and Restrictions

There are no restrictions to performing this procedure

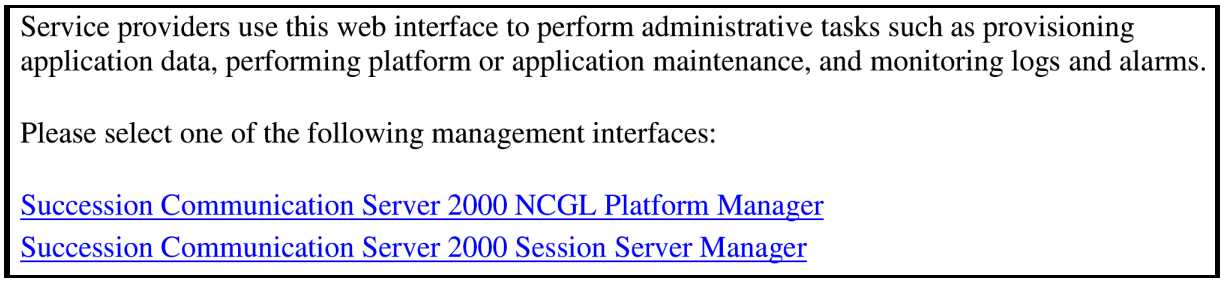
Prerequisites

This procedure has no prerequisites.

Action

At the Session Server GUI or Integrated EMS client

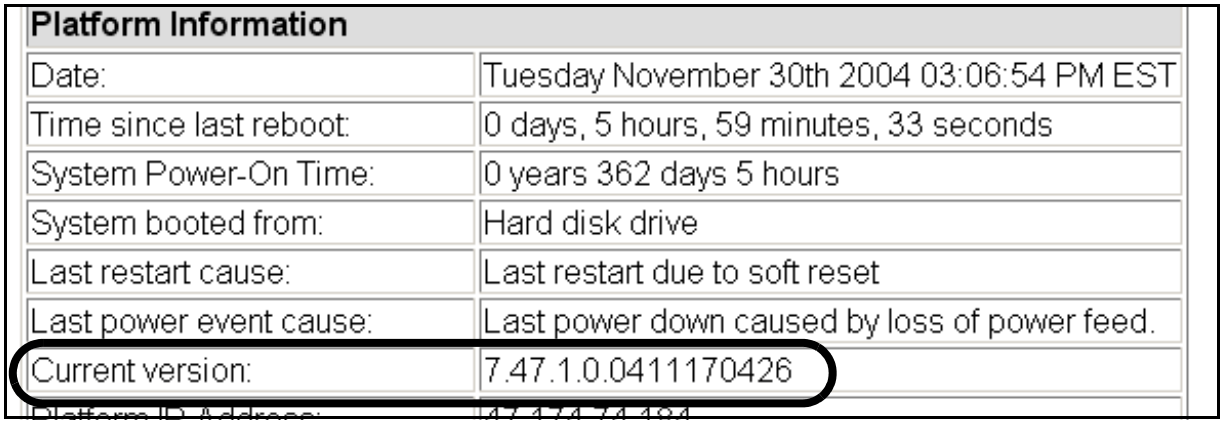
1 Select ***Succession Communication Server 2000 NCGL Platform Manager*** from the launch point menu.


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

Please select one of the following management interfaces:

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

2 Review the **System/Platform Information** page for the NCGL platform version information.



Platform Information	
Date:	Tuesday November 30th 2004 03:06:54 PM EST
Time since last reboot:	0 days, 5 hours, 59 minutes, 33 seconds
System Power-On Time:	0 years 362 days 5 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:	7.47.1.0.0411170426

3 You have completed this procedure.

Alternate command line interface method- (existing SN08 platforms)

At the Session Server console interface

1 Log onto the Session Server unit using a secure shell (ssh) and change to root user.

2 Verify the installed software versions for this unit by typing

`# cat /opt/apps/webint/version_info.txt`

and pressing the **Enter** key.

The system responds:

```
=======================================================
Session Server Load Info
=======================================================
Release  = NGSS_08_Bld_int
Version  = NGSS_08_Bld_49_b
Build Date = Mon Nov 29 14:47:17 EST 2004
=======================================================
=======================================================
NCGL Platform Load Info
=======================================================
BUILDVERSION=7.47.1.0.0411170426
=======================================================
```

3 You have completed this procedure.

Alternate command line interface method- (existing SN07 platforms)

At the Session Server console interface

1 Log onto the Session Server unit using a secure shell (ssh) and change to root user.

2 Verify the installed software versions for this unit by typing

`# cat /opt/apps/webint/jakarta-tomcat-4.1.30/webapps/prov/html/version_info.txt`

and pressing the **Enter** key.

The system responds:

```
=======================================================
Session Server Load Info
=======================================================
Release  = NGSS_08_Bld_int
Version  = NGSS_08_Bld_49_b
Build Date = Mon Nov 29 14:47:17 EST 2004
=======================================================
=======================================================
NCGL Platform Load Info
=======================================================
BUILDVERSION=7.47.1.0.0411170426
=======================================================
```

3 You have completed this procedure.

Determine the current version of software loads

Purpose of this procedure

Use this procedure to determine the version of the software loads for the SIP Gateway application on the active unit. This procedure can be used as a standalone task or as part of a higher level activity.

Limitations and Restrictions

The version information for the NCGL platform load is only accurate if a maintenance release has not been applied to the load. If a maintenance release has been applied to the NCGL platform load, its version information is not accurately shown on this page. To accurately determine the NCGL platform load version that the unit is operating on, use procedure View the operational status of a Session Server NCGL platform on page 119 and go to the ***System Info*** page. As an alternative, you can use the procedure Use the procedure Alternate command line interface method- (existing SN08 platforms) on page 82 or Alternate command line interface method- (existing SN07 platforms) on page 82 to determine the correct NCGL platform load version.

The version information for the SIP Gateway application is accurately shown even if a maintenance release is applied to the application.

Prerequisites

This procedure has no prerequisites.

Action

At the Session Server GUI or Integrated EMS client

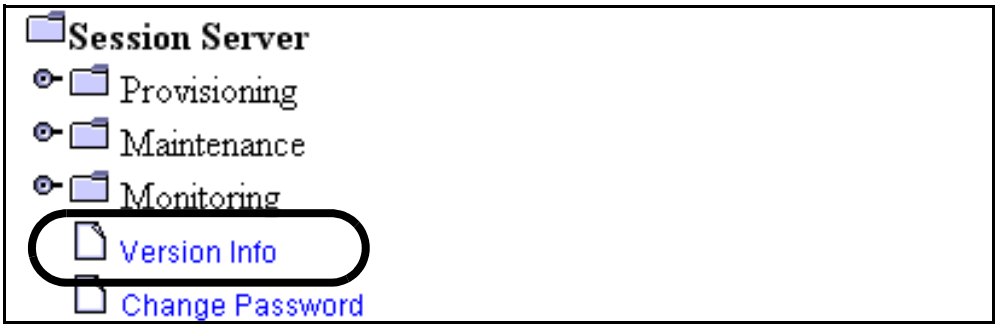
1 Select ***Succession Communication Server 2000 Session Server Manager*** from the launch point menu.

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

Please select one of the following management interfaces:

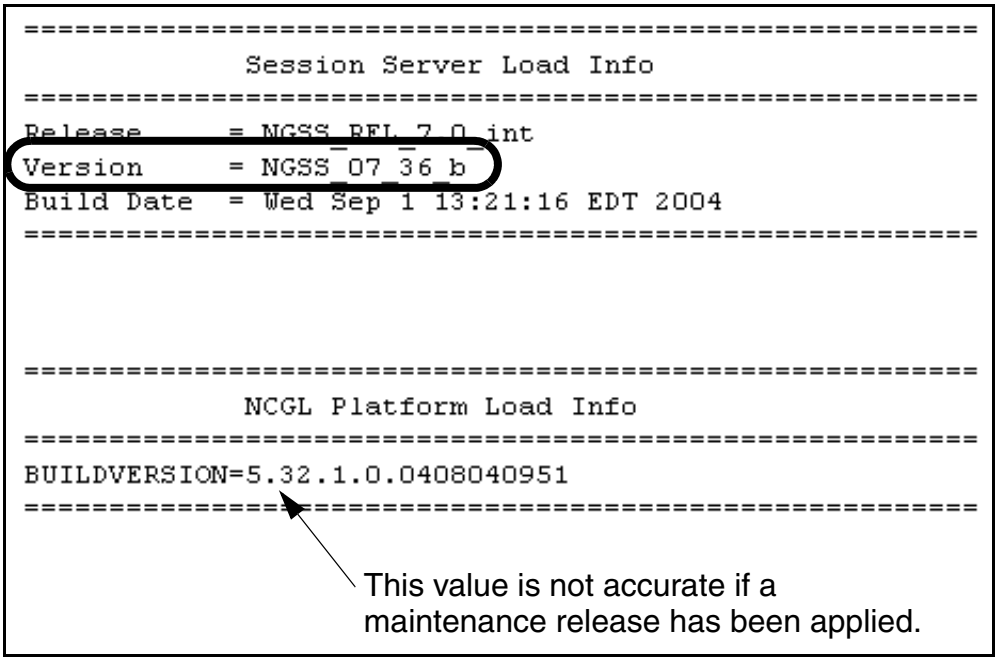
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 At the Session Server folder, click the **Version Info** link.



3 Review and record the software load version information for the SIP Gateway application (top).

Note: The version information for the NCGL platform load is only accurate if a maintenance release has not been applied to the load. However, if a major upgrade is applied, the version info will be accurately reflected in the view. If a maintenance release is applied behind a major upgrade to the NCGL platform load, then the version information is not accurately reflected on this page. Use the procedure Alternate command line interface method- (existing SN08 platforms) on page 82 or Alternate command line interface method- (existing SN07 platforms) on page 82 to determine the correct NCGL platform load version.



4 You have completed this procedure.

Alternate command line interface method- (existing SN08 platforms)

At the Session Server console interface

1 Log onto the Session Server unit using a secure shell (ssh) and change to root user.

2 Verify the installed software versions for this unit by typing

`# cat /opt/apps/webint/version_info.txt`

and pressing the **Enter** key.

The system responds:

```
=========================================================
Session Server Load Info
=========================================================
Release  = NGSS_08_Bld_int
Version  = NGSS_08_Bld_49_b
Build Date = Mon Nov 29 14:47:17 EST 2004
=========================================================
=========================================================
NCGL Platform Load Info
=========================================================
BUILDVERSION=7.47.1.0.0411170426
=========================================================
```

3 You have completed this procedure.

Alternate command line interface method- (existing SN07 platforms)

At the Session Server console interface

1 Log onto the Session Server unit using a secure shell (ssh) and change to root user.

2 Verify the installed software versions for this unit by typing

`# cat /opt/apps/webint/jakarta-tomcat-4.1.30/webapps/prov/html/version_info.txt`

and pressing the **Enter** key.

The system responds:

```
=========================================================
Session Server Load Info
=========================================================
Release  = NGSS_08_Bld_int
Version  = NGSS_08_Bld_49_b
Build Date = Mon Nov 29 14:47:17 EST 2004
=========================================================
=========================================================
NCGL Platform Load Info
=========================================================
BUILDVERSION=7.47.1.0.0411170426
=========================================================
```

3 You have completed this procedure.

Inhibit a system SwAct (Jam)

Purpose of this procedure

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

Limits and Restrictions

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

ATTENTION

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

CAUTION

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

Prerequisites

There are no prerequisites for performing this procedure.

Action

At the Session Server GUI or IEMS client for the active unit

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

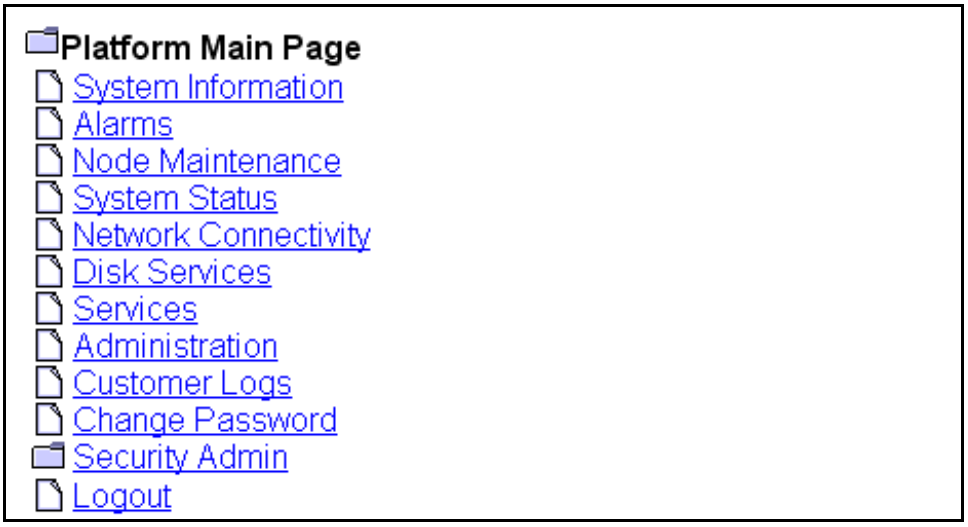
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

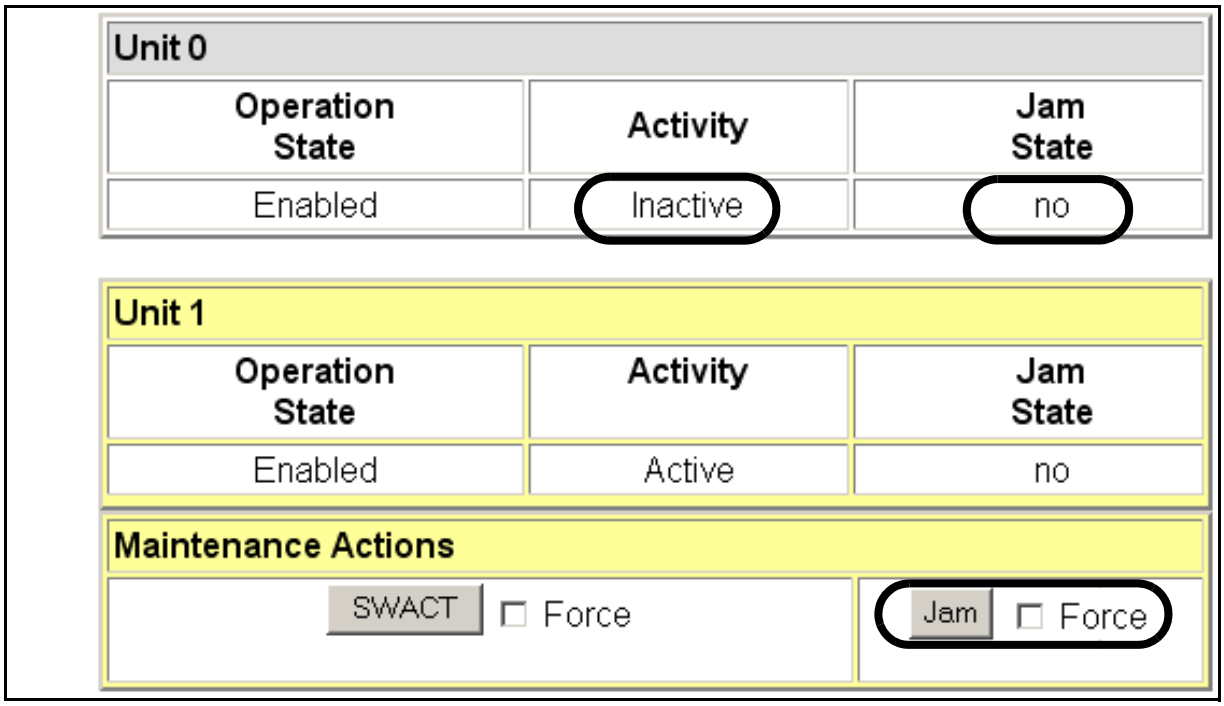
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Node Maintenance** link.

The Node Maintenance page is displayed.



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.



Note: Refer to procedure Enable a system SwAct (Unjam) on page 167 to unjam a standby Session Server unit.

4 Click the **Jam** button.

or

If you want to override any pre-Jam queries, first click the **Force** check box, then click the **Jam** button.

The system responds

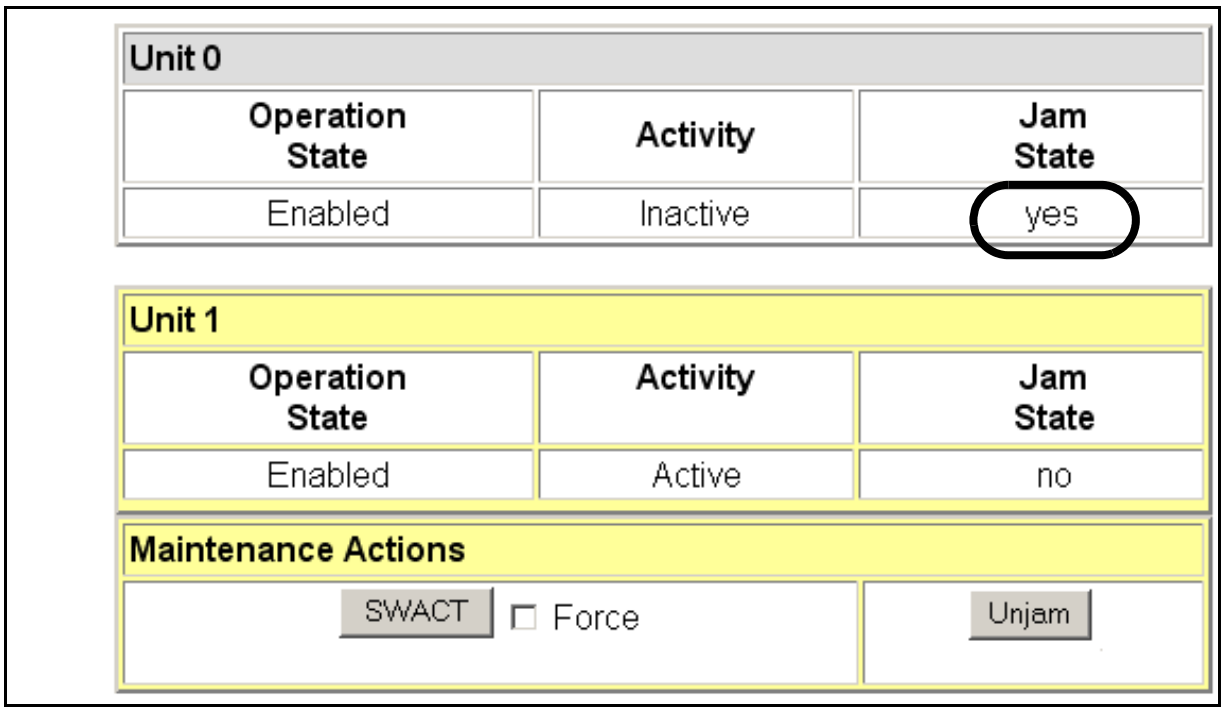
```
Are you sure you wish to perform jam action?

This will prevent the switch of activity to the
inactive node.
Click OK to confirm node jam or cancel to abort.
```

5 Click **OK** to proceed with the jam activity.

The system responds:

```
Info: Jam - Command passed.
```

6 Observe the Jam state for the standby Session Server unit transitions from No to Yes.



7 This procedure is complete.

To Jam or Force Jam?

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 could occur on the Session Server node if the active unit fails.

Upgrade Session Server NCGL platform software

Purpose of this procedure

This procedure describes how to use the CS 2000 NCGL Platform Manager GUI to apply a maintenance release or major release upgrade to an NCGL platform load.

ATTENTION

This procedure should only be used as part of the high level activity *Upgrading from a previous major release* or *Applying a maintenance release upgrade* in the Session Server Upgrades NTP, NN10349-461.

Limitations and Restrictions

You can upgrade the NCGL platform load from the local DVD-ROM drive, from an ISO image located on the system disk drive, or from a Session Server CD/DVD disk mounted elsewhere in the network (via FTP). The following upgrade protocols (methods) are selectable from the CS 2000 NCGL Platform Manager GUI:

- Local CDROM - the local DVD-ROM drive (labeled in the software as the local CD-ROM)
- Local file - an iso image, or load.tgz file copied from the local CD/DVD disk to the hard drive using the secure copy program, **scp**, to transfer the data
- Remote file using FTP or anonymous FTP - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the FTP service. If the workstation or server is configured to allow anonymous FTP, use anonymous FTP to avoid sending username and password information in cleartext format across the network.
- Remote file using HTTP or HTTPS - an iso image, or load.tgz file copied from a remotely mounted DVD-ROM drive on a workstation or server that provides the HTTP or HTTPS service.

Prerequisites

For the prerequisites of performing any upgrade, refer to section *Prepare for a maintenance release upgrade* or section *Prepare for a maintenance release upgrade* in the Session Server Upgrades NTP, NN10349-461.

Action

At the Session Server GUI or Integrated EMS client

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

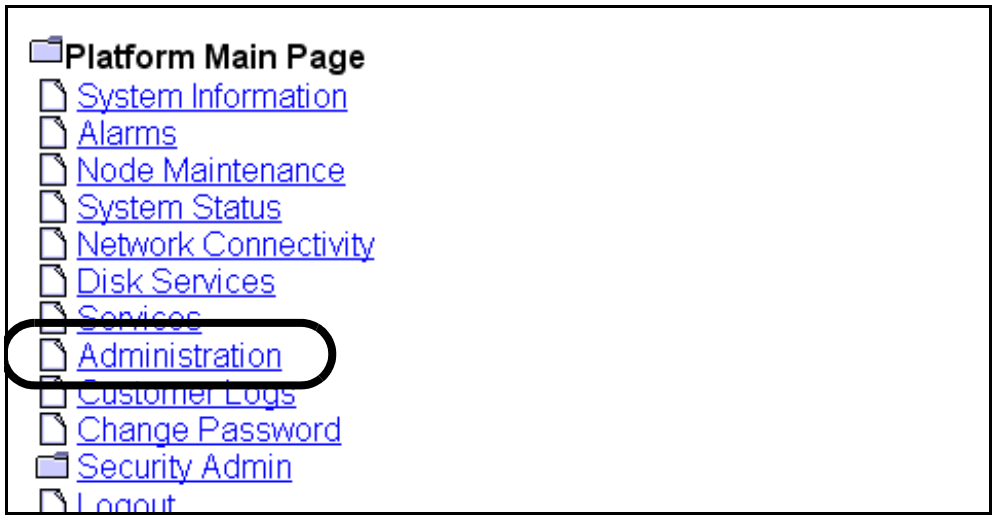
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

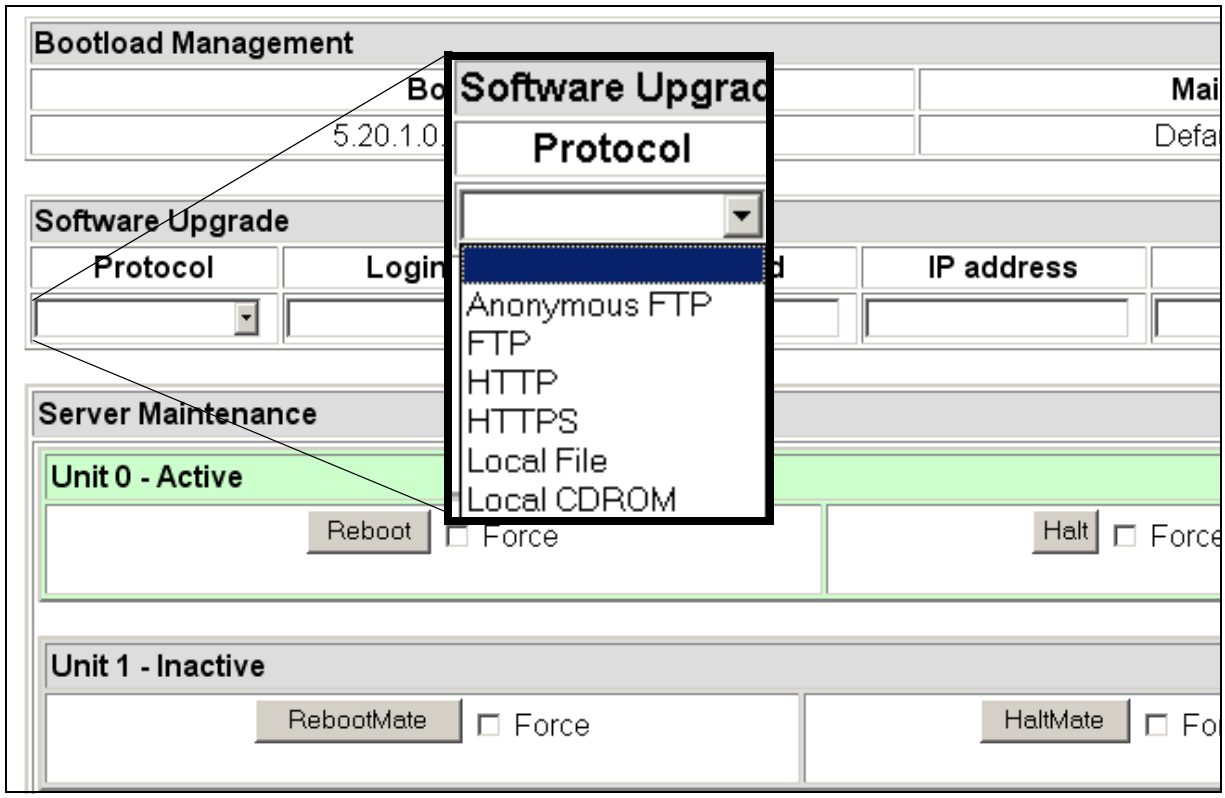
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

The Platform Main Page menu is displayed.

2 Click the **Administration** link.



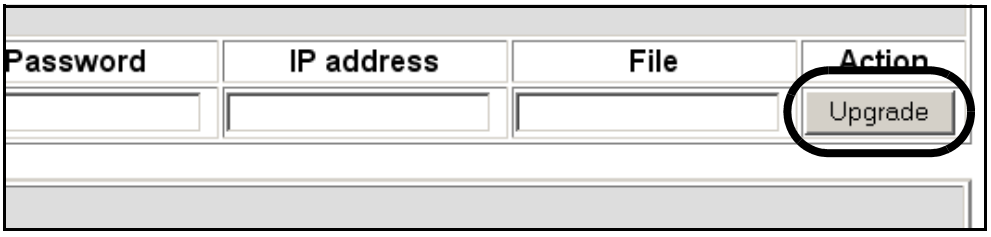
3 Click the **Protocol** drop down menu and select an upgrade protocol. Refer to the following table to help you determine the appropriate protocol:



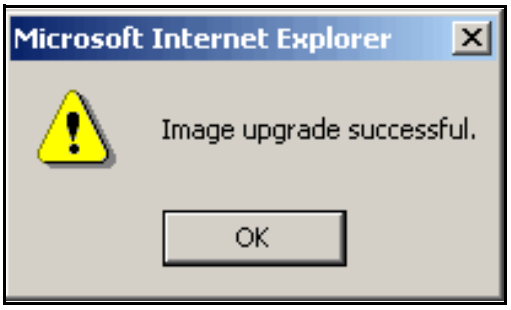
If the Protocol selection is	Do
Anonymous FTP	Enter the IP address of the remote server which has the bootload image in the IP address text box. Enter the location (as a relative path on the remote server) of the bootload image file `load.tgz` in the File text box. For example, `/opt/swd/load.tgz`. then continue with step 4

If the Protocol selection is	Do
FTP	Enter your username in the Login ID text box. Enter your password in the Password text box. Enter the IP address of the remote server which has the bootload image in the IP address text box. Enter the location (as a relative path) of the bootload image file `load.tgz` in the File text box. For example, `/opt/swd/load.tgz`. then continue with step 4
HTTP or HTTPS	Enter the IP address of the remote server which has the bootload image in the IP address text box. Enter the location (as a relative path on the remote server) of the bootload image file `load.tgz` in the File text box. For example, `/opt/swd/load.tgz`. then continue with step 4
Local File	Enter the location (as a relative path of the Session Server unit) of the bootload image file `load.tgz` in the File text box. For example, `/opt/swd/load.tgz`. then continue with step 4
Local CDROM	Ensure that the CD/DVD disk is inserted into the drive then continue with step 4

4 Click the **Upgrade** button.



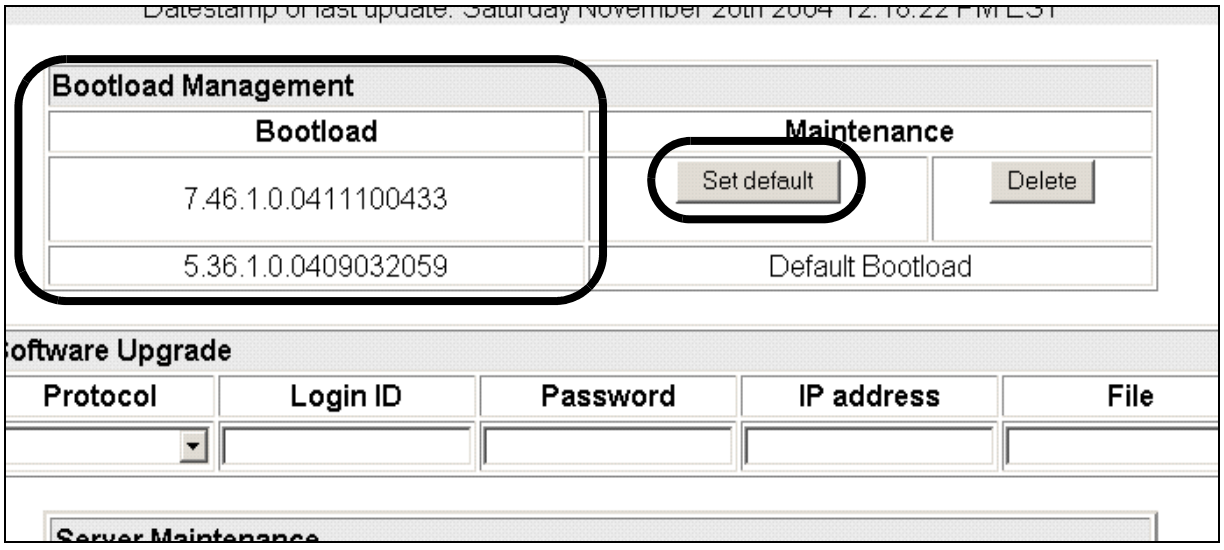
5 Verify that the load files were successfully copied by clicking **OK** on the popup window.



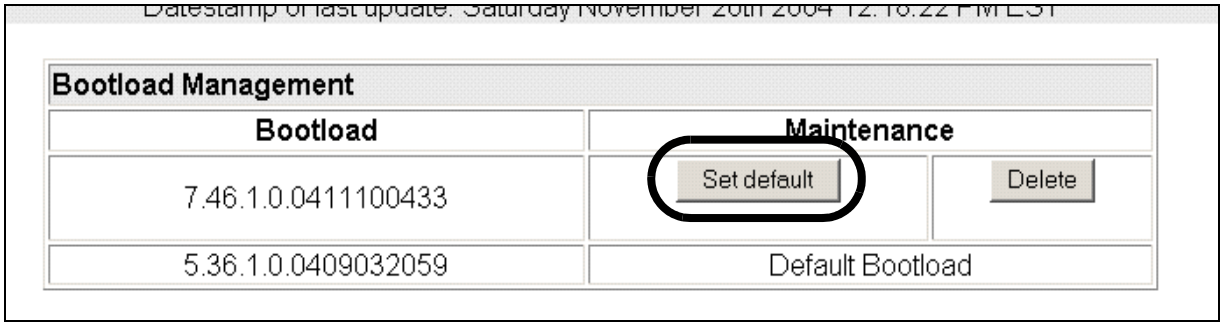
ATTENTION

Refer to the Troubleshooting Upgrades on page 95 section if the popup window does not indicate a successful image upgrade.

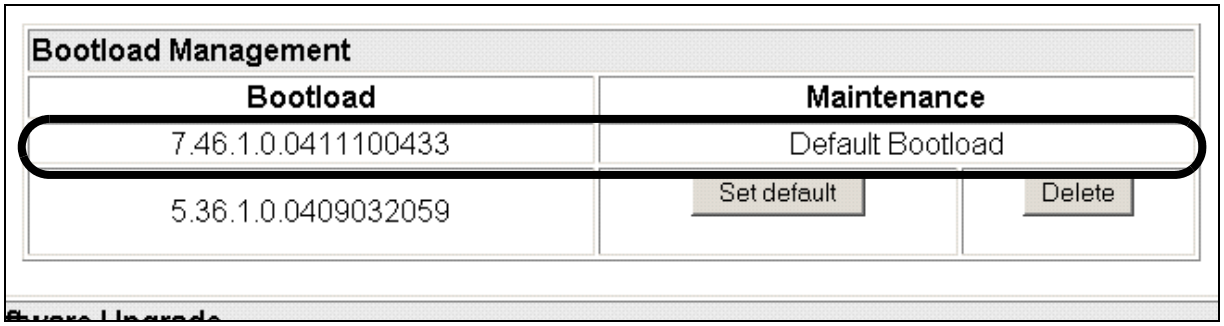
6 Once the selected NCGL load has been successfully copied to the unit, look for the load number to appear in the Bootload Management panel.



7 Click the **Set Default** button to the right of the new (upgraded) bootload.



The system responds by setting the newly installed load as the default load, as shown below.



8 Verify that you have set the correct bootload to be the default.

9 If you upgraded using the Local CD-ROM protocol, remove the CD/DVD disk from the drive.

10 You have completed this procedure. Return to the high-level activity *Prepare for a maintenance release upgrade* or section *Prepare for a maintenance release upgrade* in the Session Server Upgrades NTP, NN10349-461.

Troubleshooting Upgrades

For step 5 of this procedure, review the message in the popup window. The following possible error messages and their meaning are described:

- Error: Failed to update image /usr/bin/copy_boot_image -f /opt/swd/load.tgz Invalid load file content. Exiting

  Indication: If the bootload file is corrupt, the system software indicates that the bootload contains invalid content.

- Error: Failed to update image /usr/bin/copy_boot_image -u https://10.40.5.62//tmp/load.tgz: Failed to retrieve file from the network.

Indication: The user has attempted to perform a software upgrade where the file path or the IP address used is not correct. You need to validate that the IP address is correct, also, make sure the file path is correct.

- Error: Failed to update image /usr/bin/copy_boot_image -u ftp://mtc:mtc@10.40.5.59//usr/load.tgz: Failed to retrieve file from the network.

  Indication: The user has attempted to perform a software upgrade where the file path or the user ID or password used is not correct. You need to validate that the file path is correct and make sure to check the user ID and password.

- Error: Failed to update image /usr/bin/copy_boot_image -u ftp://mtc:mtc@10.40.5.59//usr/load.tgz: 10.40.5.59 IP address is not responding.

  Indication: The user has attempted to perform a software upgrade from a host that is not responding. You need to check that the host IP address is available and try again.

- Error: Failed to update image /usr/bin/copy_boot_image -f load.tgz: Could not find load.tgz

  Indication: The user has attempted to perform a software upgrade where the file path is not correct. Validate that the file path is correct.

- Error: Failed to update image /usr/bin/copy_boot_image -c : Failed to mount the cdrom RC=32

  Indication: If the CDROM is not placed in the CDROM drive and an attempt is made to upgrade software with the “Local CDROM” option, the above message appears. Verify that the CDROM is in the drive. If the CDROM is inserted, verify that the drive is functioning properly.

  or

  The user has attempted to perform a software upgrade where there is a problem with mounting the CD-ROM drive. Mount or remount the CD-ROM drive before attempting another software upgrade process.

- Error: Failed to update image /usr/bin/copy_boot_image -u https://10.40.5.62/load.tgz : Unable to decompress /opt/base/upgrade/29335/load.tgz Exiting

  Indication: The user has attempted to perform a software upgrade, which uses filesystem (/opt/base) that is full. You need to remove unwanted files and make sure there is enough space in the targeted filesystem.

Reboot a Session Server unit

Purpose of this procedure

Use this procedure to perform a graceful shutdown and reboot of the NCGL operating system running on a Session Server 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 3-4 minute service interruption of the affected unit and should only be used when recommended by Nortel support personnel.

Limitations and Restrictions

ATTENTION

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

CAUTION

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

Prerequisites

Use procedure View the operational status of a Session Server NCGL platform on page 119 to check for any disk array rebuilds in progress. Wait for the rebuild to complete before executing this procedure.

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

Action

At the Session Server GUI or IEMS client for the active unit

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

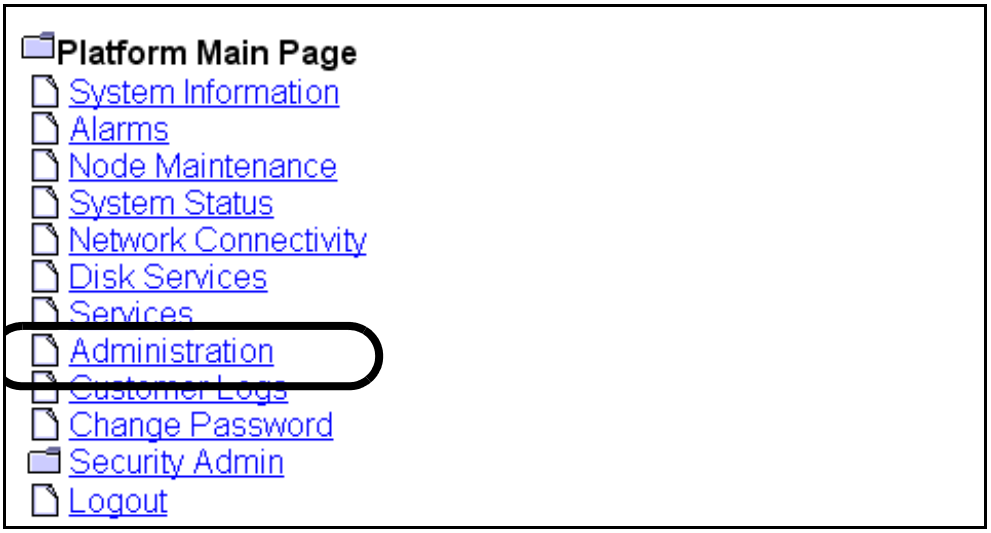
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

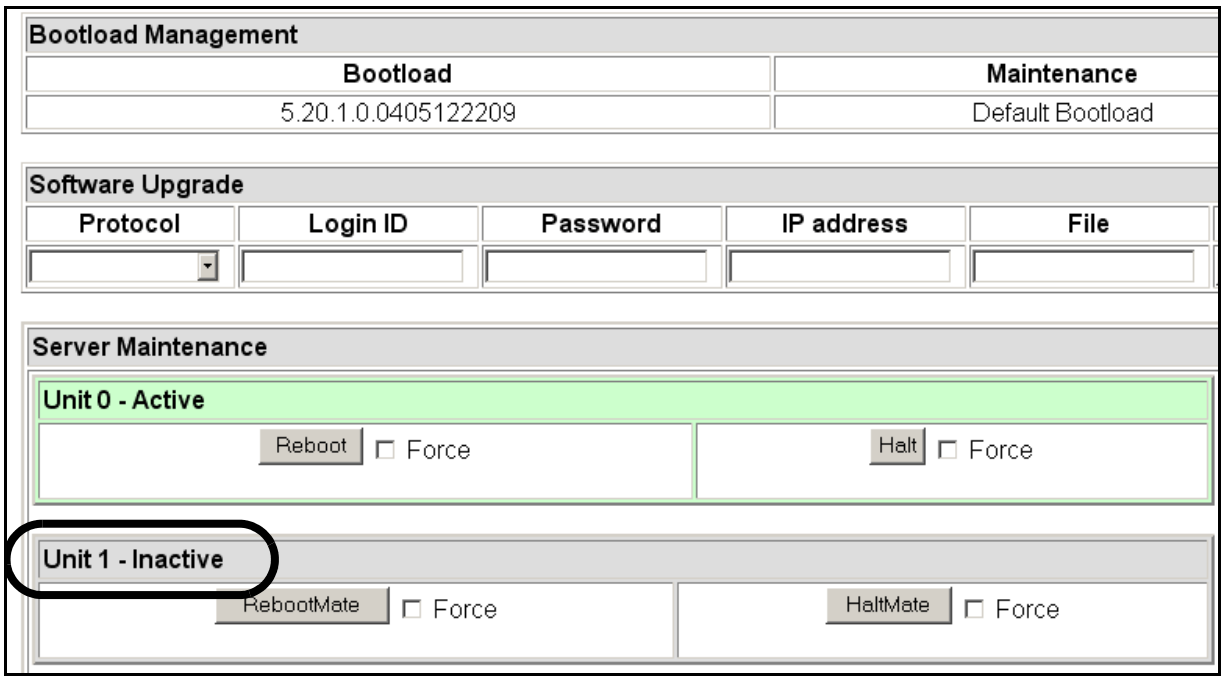
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Administration** link.

The Administration page is displayed.



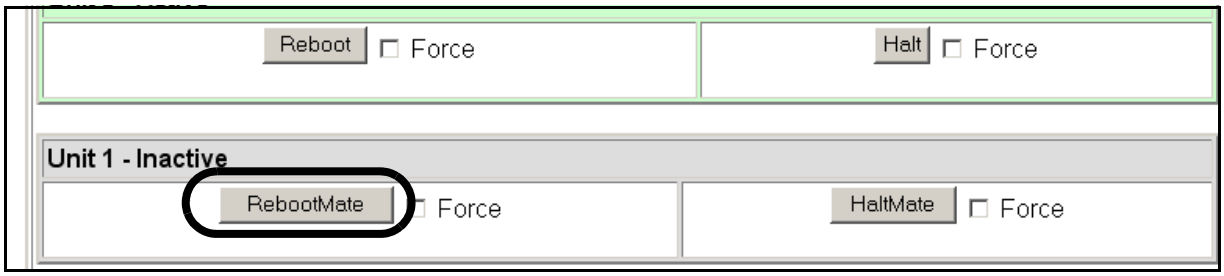
3 Review the status of the unit you want to reboot. If it is available, the **Reboot** or **RebootMate** buttons are accessible.



4 Click the **Reboot** button (for the active unit) or **RebootMate** button (for the inactive unit) for the Session Server unit you want to reboot.

Note 1: If you want to override any pre-reboot queries including a pre-check by applications running on the unit, click the **Force** check box before clicking the **Reboot** or **RebootMate** button.

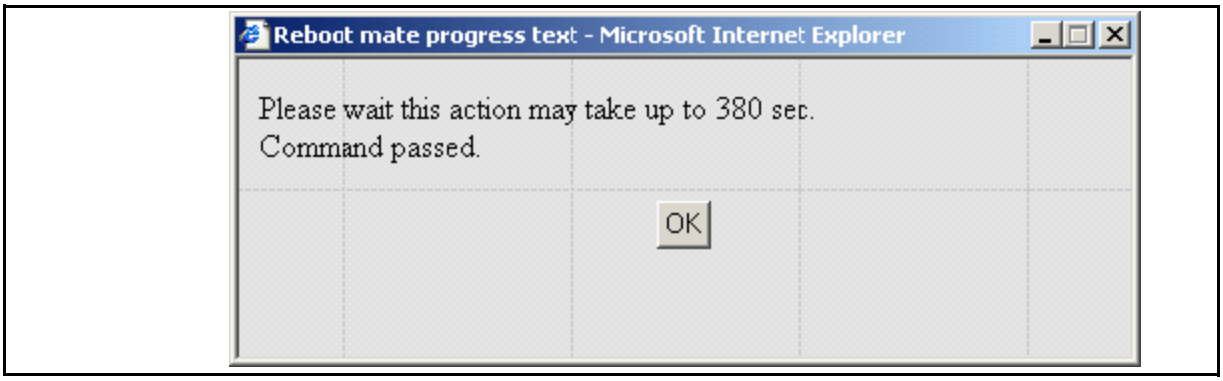
Note 2: In a system operating in fault-tolerant (duplex) mode, only the inactive unit can be rebooted using RebootMate or a Forced RebootMate. A Reboot or Forced Reboot can only be performed if the system is operating in simplex mode.



The system responds with the following message box:

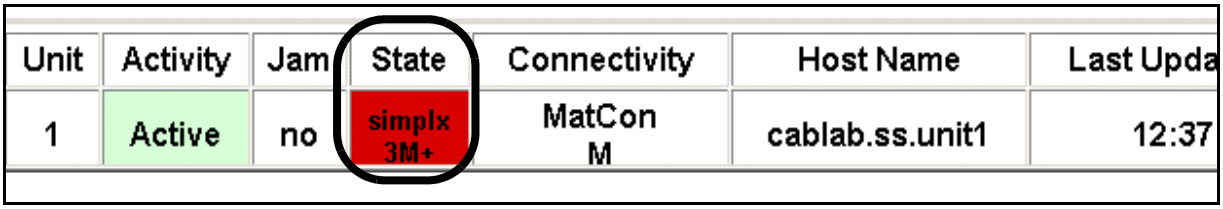
5 Click **OK** to confirm the reboot operation.

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



6 Click **OK** to close the dialog box.

7 Monitor the recovery of the rebooting unit using procedure View the operational status of a Session Server NCGL platform on page 119 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 Upda
1	Active	no	simplx 3M+	MatCon M	cablab.ss.unit1	12:37

8 This procedure is complete.

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 Session Server node from operating in a fault-tolerant mode.

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

ATTENTION

All prerequisites and restrictions shown on page 98 apply when using this procedure.

At Session Server CLI or Integrated EMS client

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

2 Reboot the selected Session Server unit by typing

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

or

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

and pressing the **Enter** key.

3 Use procedure View the operational status of a Session Server NCGL platform on page 119 to confirm the recovery of the unit after reboot.

4 You have completed this procedure.

Troubleshooting reboots

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

Error: Command failed. Reason: Mate not available.
You must reboot the unit using the Alternate command line interface (CLI) method on page 102.

Error: Reboot - Command rejected. Reason: Mate is available.
You have attempted to reboot the active server when the inactive server is available.

Error: Halt - Command rejected. Reason: Mate is available.
You have 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. The user should 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.

Validate a certificate chain

Purpose of this procedure

This procedure uses the certificate management tool to validate a certificate chain. It is part of the process for provisioning a CA-signed certificates. This procedure should only be used as part of a high level task for creating or updating security certificates.

Limitations and restrictions

The private key that was generated by the certificate signing request must be the same private key currently stored in /opt/base/share/ssl. The certificate management tool will verify that the certificate provided as the user certificate matches the private key file server.key located in /opt/base/share/ssl.

Prerequisites

You must first complete procedure Prepare to validate a certificate chain on page 62.

The following certificate files are required from a signing authority and must be located in the /opt/base/share/ssl directory to complete this procedure:

- Server.crt - contains the local certificate
- Trusted.crt - contains the CA chain in top down with the root CA at the top

The following restrictions apply to migrating CA-signed certificates:

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

Action

At the Session Server CLI or Integrated EMS client

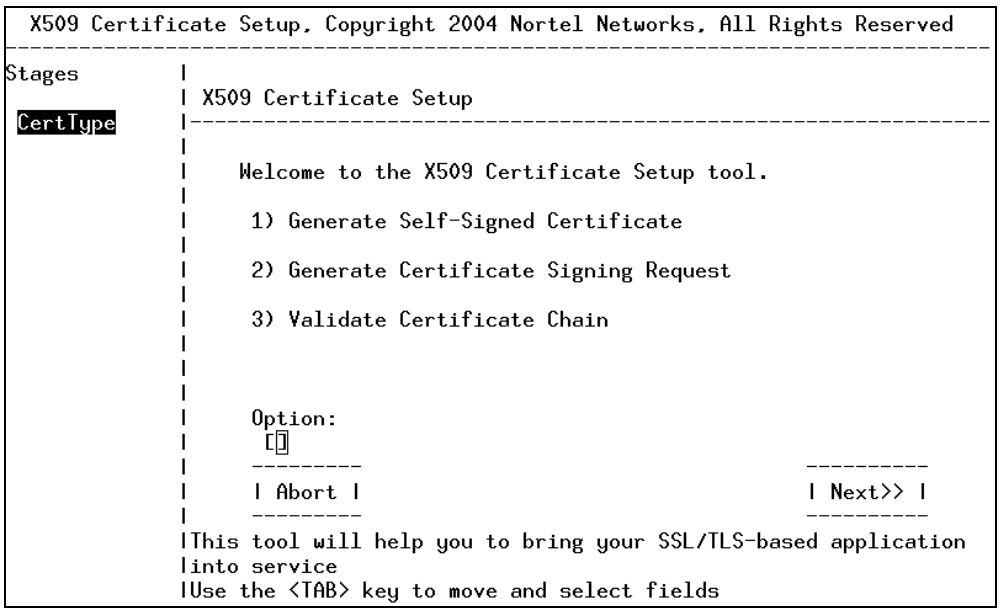
1 Complete procedure Prepare to validate a certificate chain on page 62.

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

3 Start the certificate management tool by typing

cert_mgnt

After a few seconds the Introduction screen is displayed.



4 Press **3** for the option to validate a certificate chain, position the cursor on the **Next** button and press **Enter**.

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

The configure CA-signed certificate screen appears.

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

5 Enter the full path and filename where the CA certificate can be found by typing

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

position the cursor on the **Next** button and press **Enter**.

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

The configure server certificate screen appears.

```
 X509 Certificate Setup, Copyright 2004 Nortel Networks, All Rights Reserved
-------------------------------------------------------------------------------
Stages          |
                | Configure the CA-signed certificate filename
 CertType       |-----------------------------------------------------------------
 CAFile         |
 CertFile       |    Please enter the user certificate filename
 Summary        |
                |     []
                |
                |
                |
                |
```

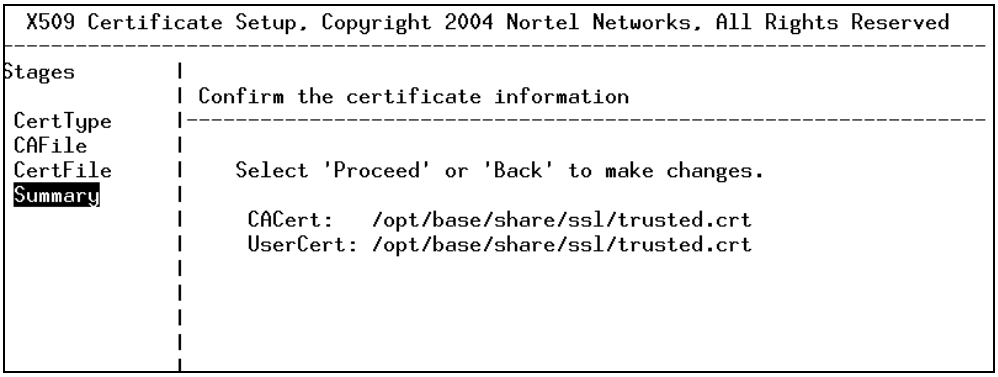
6 Enter the full path and filename where the server.crt certificate can be found by typing

`/opt/base/share/ssl/server.crt`

position the cursor on the **Next** button and press **Enter**.

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

The summary screen appears.



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

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

```
Provisioning CA Certificate
Verifying certificate/key pair
spawn openssl verify -CAfile /opt/base/share/ssl/trusted.crt
/opt/base/share/ssl/server.crt
/opt/base/share/ssl/server.crt: OK
server.crt: OK
Certificate validation succeeded
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
```

8 The procedure is complete.

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.

Generate self-signed security certificates

Purpose of this procedure

This procedure uses the certificate management tool to generate self-signed security certificates used for both Session Server units. 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 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. These file permissions should not be changed.

Prerequisites

Please read the complete disclaimer, found in section Self-signed certificate security disclaimer on page 116.

Action

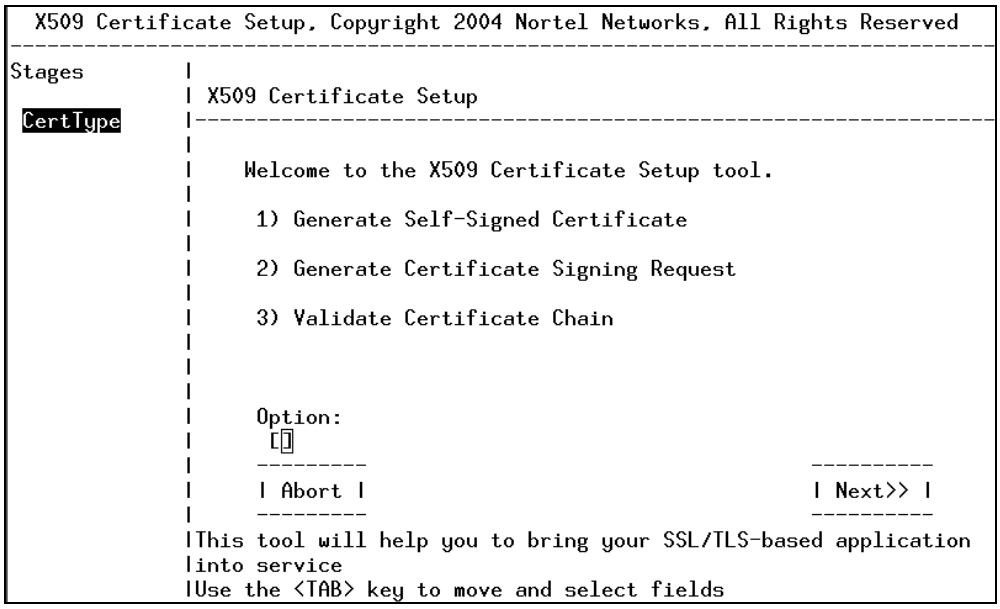
At the Session Server CLI or Integrated EMS client

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

2 Start the certificate management tool by typing

`cert_mgnt`

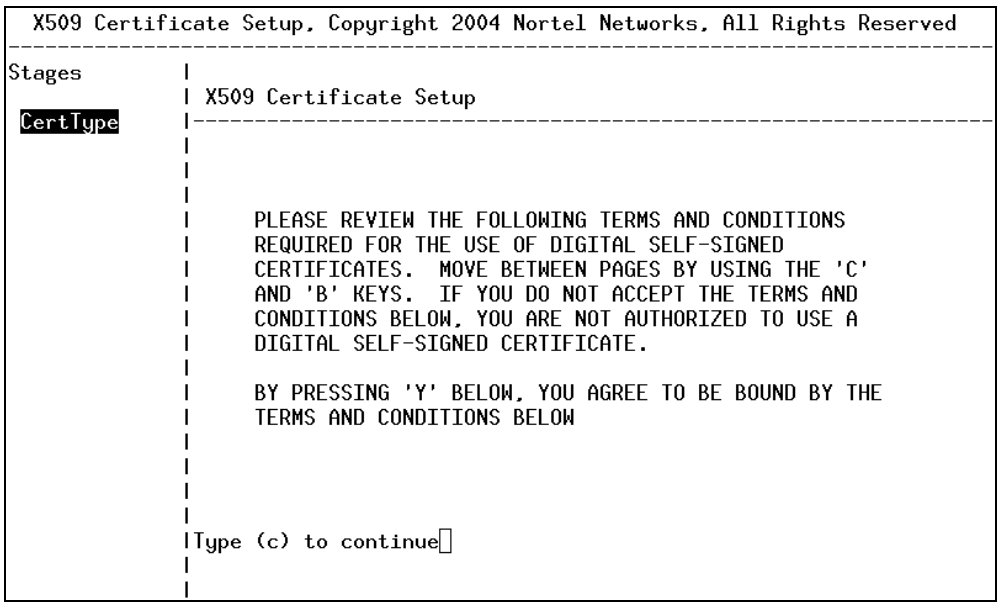
After a few seconds the Introduction screen is displayed.



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

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

A security disclaimer screen appears.

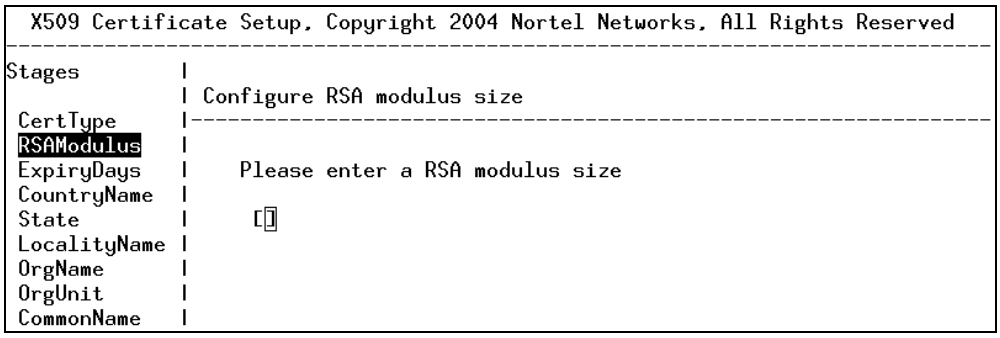


4 Carefully read the series of screens displaying the terms and conditions of the security certificate tool. Press **c** to continue to the next disclaimer page or press **b** to go back to the previous disclaimer page.

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)

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

7 Use the following table to determine your next step:

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

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

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

9 Use the following table to determine your next step:

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

10 Press any key and return to step 6.

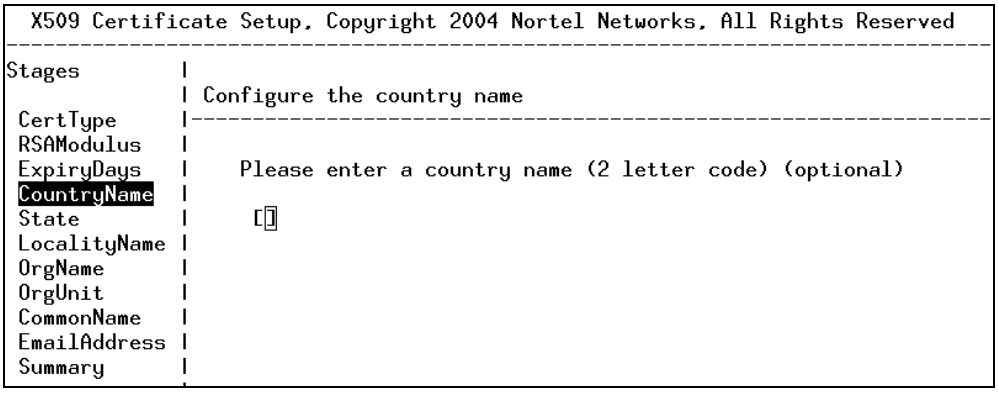
11 If you want to delete the existing RSA key, press **y**.

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

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

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

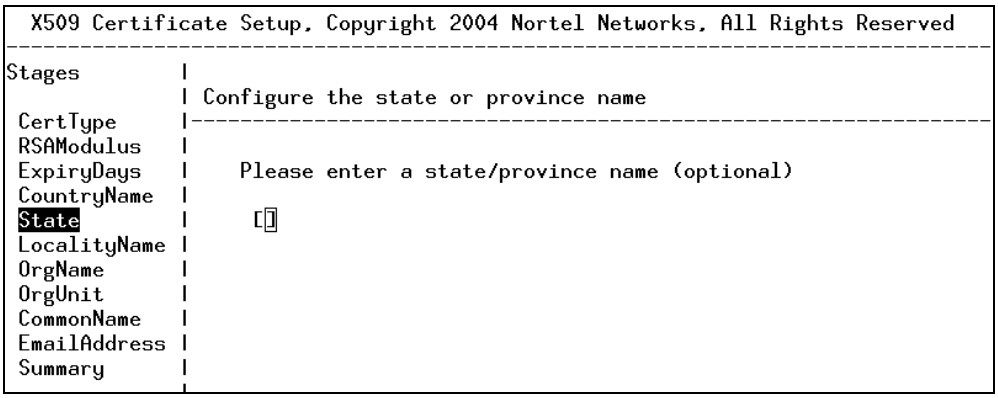
The country name configuration screen appears.



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

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

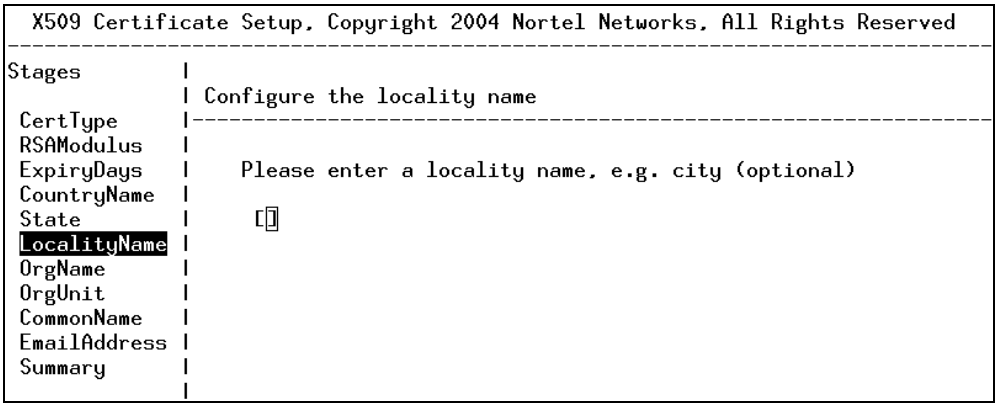
The state/province configuration screen appears.



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

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

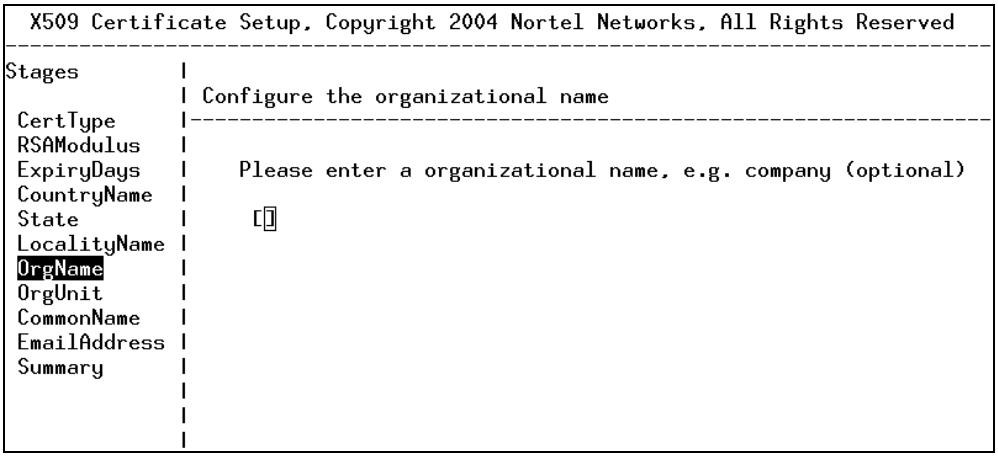
The locality configuration screen appears.



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

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

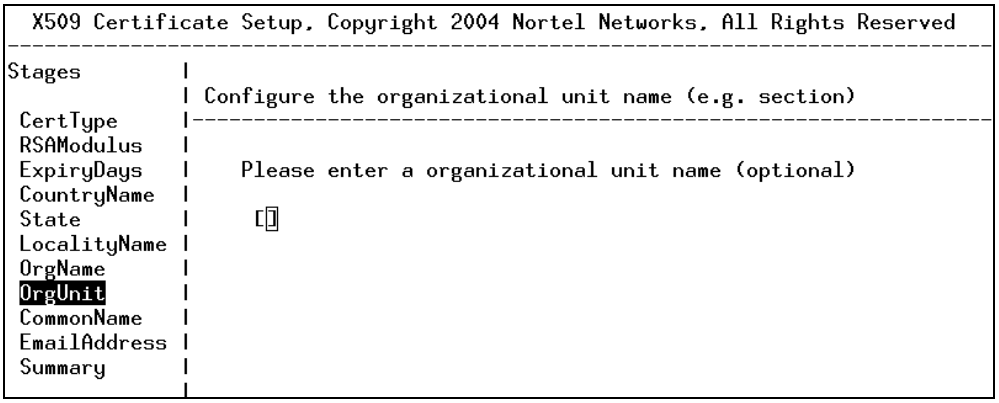
The organizational configuration screen appears.



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

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

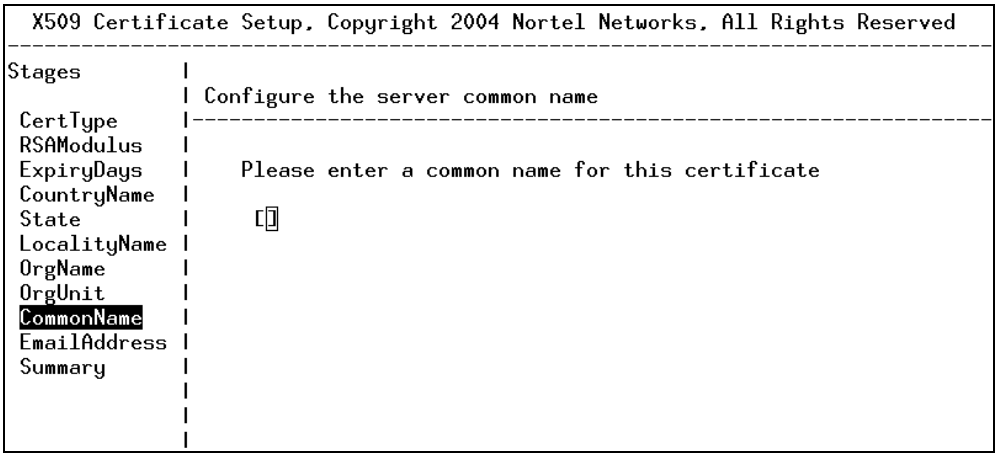
The organizational unit configuration screen appears.



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

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

The server common name configuration screen appears.



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

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

Gateway application parameters, in NTP Session Server Configuration Management, NN10338-511.

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

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

An email configuration screen appears.

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

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

Note: This entry helps identify the Session Server 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 The procedure is complete.

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.”;

View the operational status of a Session Server NCGL platform

Purpose of this procedure

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

Limitations and restrictions

This procedure provides instructions for determining the service status of the Session Server NCGL platform only. For instructions on determining the status of the SIP Gateway application, refer to procedure *View the operational status of the SIP Gateway application* in the Session Server Configuration Management NTP, NN10338-511.

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

This procedure does not describe how to change platform or NCGL settings such as changing BIOS settings or platform provisioning. Refer to the appropriate procedures in the Session Server Configuration Management NTP, NN10338-511, for changing these settings.

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

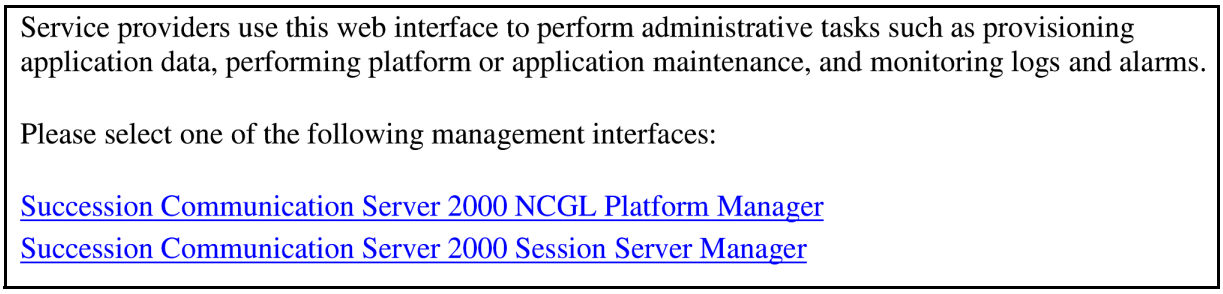
Prerequisites

There are no prerequisites for using this procedure.

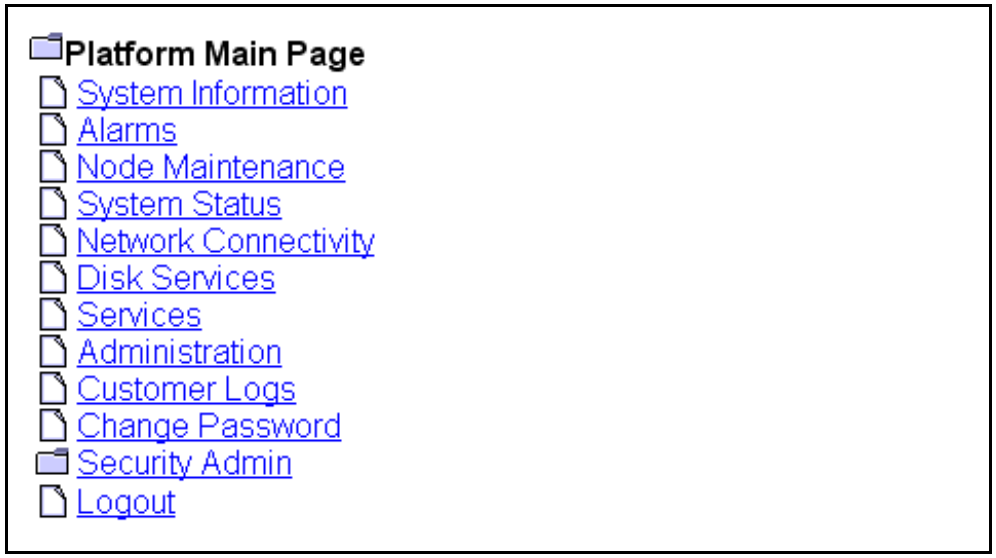
Action

At the Session Server GUI or Integrated EMS client

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



The Platform Main Page menu is displayed.



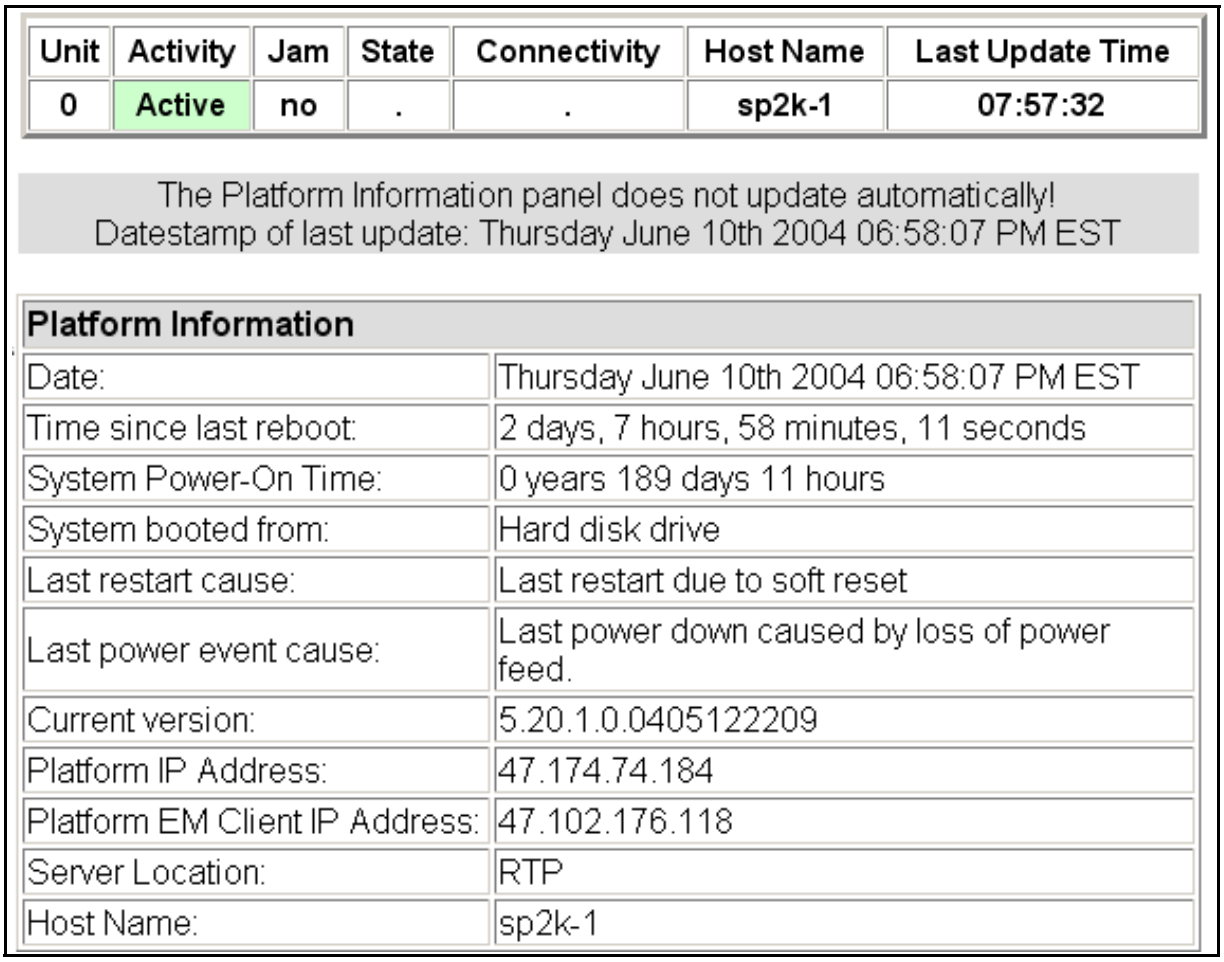
2 Use the following table to determine your next step:

If	Do
you want to review the version of the platform software load, boot statistics and platform IP address	Click the **System Information** link and go to step 3.
you want to review existing platform alarms	Skip to step 17 and go to procedure *View Session Server alarms* in the Session Server Fault Management NTP, NN10332-911.
you want to review node maintenance status	Click the **Node Maintenance** link and go to step 5.

If	Do
you want to review the status of system processes, CPU load and memory or related alarm thresholds	Click the **System Status** link and go to step 7.
you want to review the connectivity status of the network links. To perform link management activities, refer to the Session Server Security and Administration NTP, NN10346-611	Click the **Network Connectivity** link and go to step 9.
you want to review storage related information including array status, disk capacity and disk alarm thresholds	Click the **Disk Services** link and go to step 10.
you want to review details about platform services including the network time protocol servers	Click the **Services** link and go to step 12.
you want to review platform version information only	Click the **Administration** link and go to step 14.
you want to review customer logs	Skip to step 17 and go to procedure *View Session Server logs* in the Session Server Fault Management NTP, NN10332-911.
you want to change root passwords	Skip to step 17 and go to procedure *Manage user passwords with the Session Server GUI* in the Session Server Security and Administration NTP, NN10346-611.
you want to view TLS security information or manage security certificates	Skip to step 17 and refer to the Session Server Security and Administration NTP, NN10346-611 to manage security certificates. Refer to the Session Server Configuration Management NTP, NN10338-511 to review TLS security settings.
you are finished reviewing information and want to logout from the GUI	step 16.

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

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



Unit	Activity	Jam	State	Connectivity	Host Name	Last Update Time
0	Active	no	.	.	sp2k-1	07:57:32

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

Platform Information	
Date:	Thursday June 10th 2004 06:58:07 PM EST
Time since last reboot:	2 days, 7 hours, 58 minutes, 11 seconds
System Power-On Time:	0 years 189 days 11 hours
System booted from:	Hard disk drive
Last restart cause:	Last restart due to soft reset
Last power event cause:	Last power down caused by loss of power feed.
Current version:	5.20.1.0.0405122209
Platform IP Address:	47.174.74.184
Platform EM Client IP Address:	47.102.176.118
Server Location:	RTP
Host Name:	sp2k-1

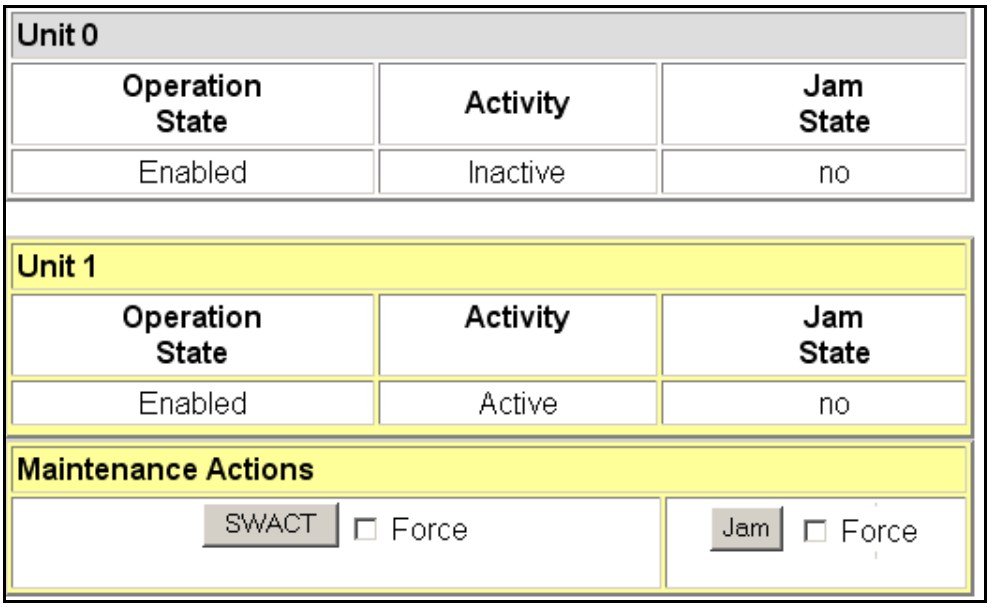
Field	Description
Unit	The unit number in the node that you are logged into.
Activity	Indicates the activity of the unit (either active or standby).
Jam	Indicates if an activity Jam has occurred on the active Session Server unit. This prevents the standby unit from becoming active, regardless of any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

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

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

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

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



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

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

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

Note: The Chassis Information panel is not automatically refreshed.

Chassis Information

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

CPU Load

1 min. load average	5 mins. load average	15 mins. load average	Minor alarm threshold 1 min.	Major alarm threshold 1 min.	Critical alarm threshold 1 min.
0.02	0.01	0.00	10.00	20.00	40.00

CPU Utilization

5 mins. Utilization average	20 mins. Utilization average	30 mins. Utilization average	Minor alarm threshold 5 min.	Major alarm threshold 20 min.	Critical alarm threshold 30 min.
0.77	0.62	0.62	95.00%	99.00%	99.00%

Process Information

Number of processes	Number of zombie process(es)	Zombie		
		Minor alarm threshold value	Major alarm threshold value	Critical alarm threshold value
165	0	5	10	15

Memory Information

Total memory (MB)	Free memory (MB)	Available memory (MB)	Minor alarm threshold value (MB)	Major alarm threshold value (MB)	Critical alarm threshold value (MB)
3,787.31	2,951.86	3,539.29	500.00	250.00	100.00

Field	Description
Chassis information: Self Test	Indicates the status of the self test performed on the platform at boot up.
Chassis information: Chassis Subsystems	Indicates the status of the platform hardware subsystems including the memory, CPU, all drives, network connection, power supplies, cooling and other I/O connections.
CPU Information: load average	Indicates the 1, 5 and 15 minute load averages for the CPU utilization.
CPU information: load average threshold values	Indicates the 1 minute CPU load average utilization threshold value. When the set threshold value is exceeded, the appropriate minor, major or critical alarm is raised.
Chassis Utilization: Utilization average	Indicates the 5, 20 and 30 minute CPU utilization average. When the threshold value is exceeded, an alarm is raised.
Chassis Utilization: alarm threshold values	Indicates the 5, 20 and 30 minute CPU utilization average threshold value. When the set threshold value is exceeded, an alarm is raised.
Process Information: Number of Processes	Indicates the total number of processes (non-threaded) that are running on the Session Server Platform.
Process Information: Number of zombie processes	Indicates the number of defunct or terminated NCGL zombie processes. ***Note:*** A zombie process is a process that has terminated either because it has been killed by a signal or because it has called an exit() and whose parent process has not yet received notification of its termination. A zombie process exists solely as a process table entry and consumes no other resources.
Process Information-zombie: minor alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a minor alarm is raised indicating that the set threshold has been exceeded.

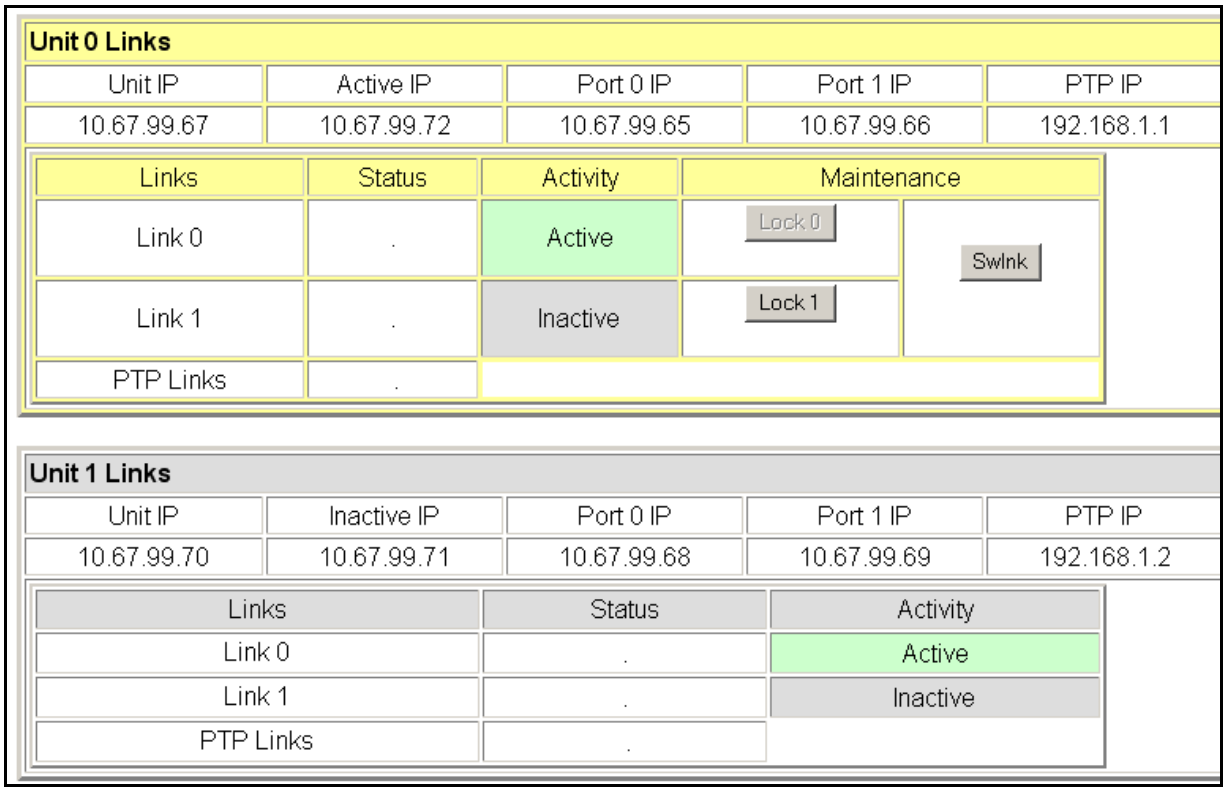
Field	Description
Process Information-zombie: major alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a major alarm is raised indicating that the set threshold has been exceeded.
Process Information-zombie: critical alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a critical alarm is raised indicating that the set threshold has been exceeded.
Memory Information: Total Memory (MB)	The total amount of RAM installed on the motherboard of each Session Server unit. Both units must have the same amount.
Memory Information: Free Memory (MB)	The amount of memory available unallocated for use.
Memory Information: Available memory (MB)	The amount of memory available for programs.
Memory Information: minor alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a minor alarm is raised.
Memory Information: major alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a major alarm is raised.
Memory Information: critical alarm threshold value	Indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a critical alarm is raised.

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

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

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

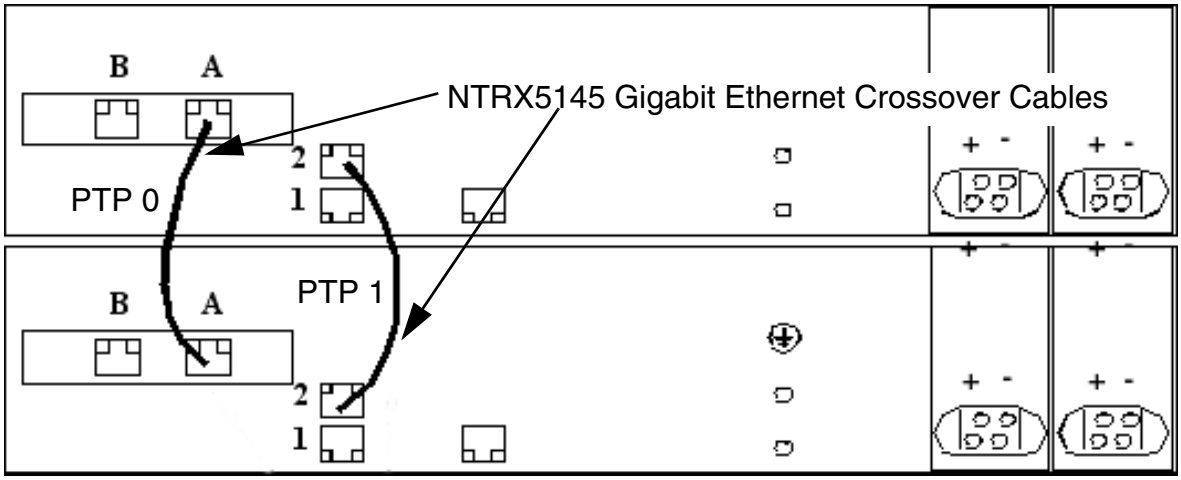
Note: The Network Connectivity panel is refreshed every 45 seconds.



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

Field	Description
Unit 0,1 Activity	Indicates the activity status of the ethernet links; either active or inactive.
Unit 0,1 Maintenance	Indicates the maintenance actions that can be performed on the ethernet links; either Lock, Unlock or Swlink. Refer to the Session Server Security and Administration NTP, NN10346-611, to perform link management.
Unit 0,1 PTP Links status	Indicates the status of the PTP links between both units in the node.
Unit IP	The network IP address of the Session Server unit.
Active IP	The IP address of the local (active) Session Server unit.
Inactive IP	The IP address of the mate (inactive) Session Server unit.
Port 0 IP	The IP address of the active or inactive ethernet port 0.
Port 1 IP	The IP address of the active or inactive ethernet port 1.
PTP IP	The IP address of the active or inactive PTP link.

Crossover and LAN ethernet cable connections for Session Server units



Ethernet Ports:

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

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

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

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

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

RAID Array Status

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

Disk Maintenance

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

Filesystem Information

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

Create/Remove Filesystem

Create New Filesystem | Remove Filesystem

Volume Group Information

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

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

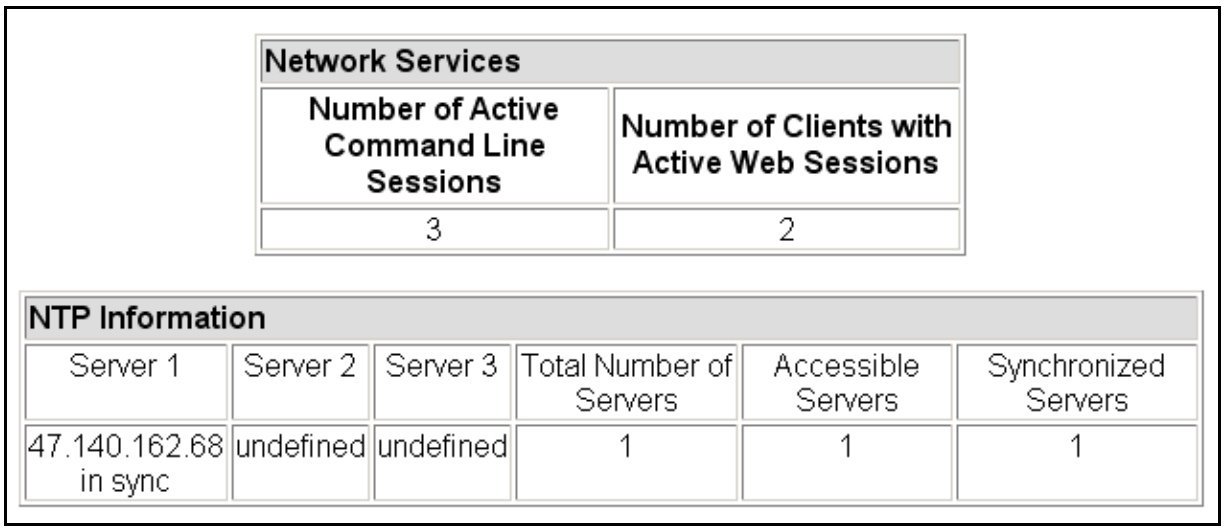
Field	Description
RAID Array Status: State	Indicates a high level state for the array: - ".": indicates the array is functioning normally. - Missing: a disk was removed from the array. - Failed: a disk in the array has failed and needs to be replaced. - Rebuilding: the array is in the process of rebuilding to a fault-tolerant mode.
RAID Array Status: Disk 0	Indicates the service status of disk 0.
RAID Array Status: Disk 1	Indicates the service status of disk 1.
RAID Array Status: Status	Indicates the status of the array. Values are: - The array is operating normally - Missing - Failed - Rebuild.
Disk Maintenance: Disk Number	Indicates the disk number in the array; 0 or 1.
Disk Maintenance: Disk Size (GB)	Indicates the total capacity of the disk drive in gigabytes.
Disk Maintenance: Disk State	Indicates the installation state of the disk.
Disk Maintenance: Disk Action	Indicates whether a hard disk can be inserted into the operating system. For more information about the **Remove** and **Insert** commands, refer to the Session Server Upgrades NTP, NN10349-461.
Filesystem Information: Monitor	Indicates the status of individual filesystems on the disk array. For more information about the **Monitor** command, refer to procedures in the Configuration Management NTP, NN10338-511.
Filesystem Information: Filesystem Name	Indicates the name of the filesystem on the disk array. Some filesystem names are reserved.
Filesystem Information: Test Results	Indicates the results of any tests run on the filesystems. Tests are run approximately every 10 minutes to verify that all of the basic filesystem operations are working on each of the filesystems.
Filesystem Information: Total Space (MB)	Indicates the total amount of disk space (in MB) allocated for this filesystem.

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

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

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

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



Network Services	
Number of Active Command Line Sessions	Number of Clients with Active Web Sessions
3	2

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

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

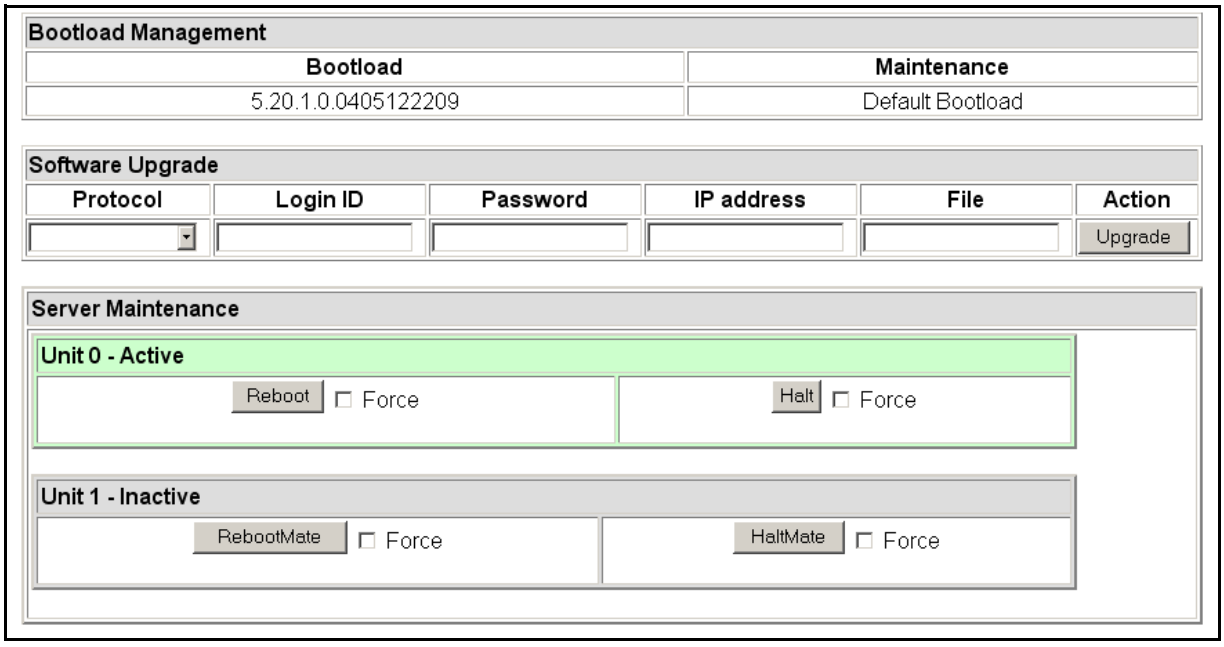
13 When you have completed reviewing Platform Services status, return to step 2.

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

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

ATTENTION

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



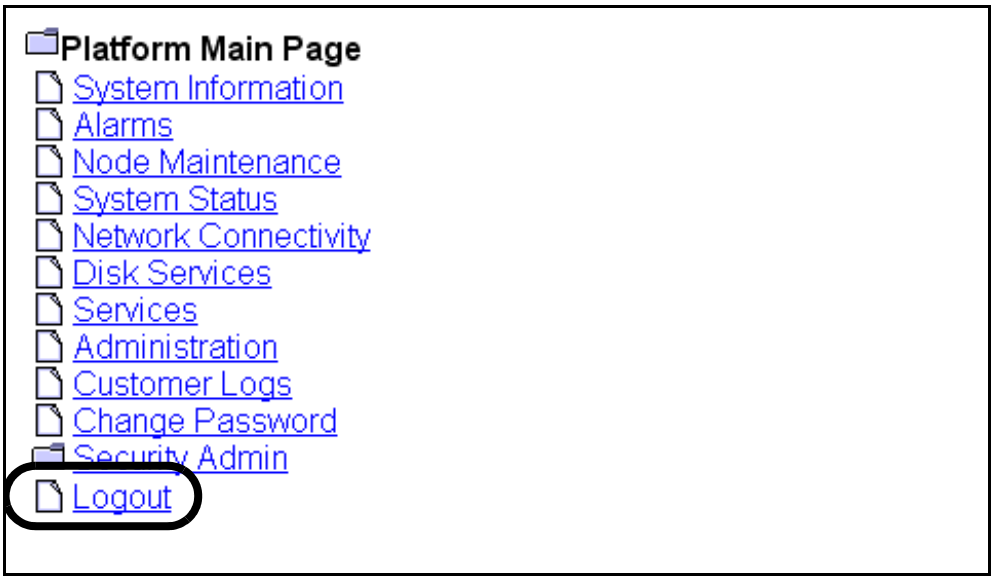
Field	Description
Bootload Management: Bootload	Indicates the load ID for the NCGL platform software load.
Bootload Management: Maintenance	Indicates whether the Bootload is the default. May also allow choosing a new default bootload if there is more than one load available. Additional loads can come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

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

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

16 If you want to logout from platform GUI, click the **Logout** button.

You are returned to the login page



17 The procedure is complete.

Acquire patch files

Purpose of this procedure

Use this procedure to identify NCGL patch files from a CD/DVD disk or ESD archive file and copy them to an appropriate patch holding directory on each Session Server unit. This procedure may be used as a standalone task or as part of a higher level activity found in activities *Patching the NCGL operating system and installed applications* or *Applying a maintenance release upgrade*, both found in the Session Server Upgrades NTP, NN10349-461, or Upgrading from a previous major release - SN07 to SN08 on page 4.

Limitations and Restrictions

As this is not a service impacting procedure, it can be performed on either the active or inactive units.

Prerequisites

If locating patch files from a CD/DVD disk, ensure that the upgrade, maintenance release or patching CD/DVD disk is inserted into the unit DVD-ROM drive.

If locating patch files from an ESD delivered ISO archive file, ensure that the software archive file has been extracted and put into the /opt/swd directory on both units using procedure Extract an ISO image from an Electronic Software Delivery (ESD) on page 71.

Action

If locating patch files from a CD/DVD disk, proceed with procedure Procedure: Acquire patch files from a CD/DVD disk.

If locating patch files from an ESD delivered ISO maintenance release image file, then go to Procedure: Acquire patch files from an ESD delivered ISO image on page 141.

Procedure: Acquire patch files from a CD/DVD disk

At the Session Server CLI or Integrated EMS client

1. Log onto either Session Server unit and change to the root user.
2. Insert the CD/DVD disk into the disk drive.
3. At the prompt, type

   ```
   $ cd /
   ```

   and press Enter.

4 Mount the DVD-ROM drive by typing

```
$ mount /cdrom
```

and pressing the Enter key.

5 Change directories to the mounted DVD-ROM filesystem by typing

```
$ cd /cdrom
```

and pressing the Enter key.

6 Locate the patch files by typing

```
$ ls
```

and pressing the Enter key.

The system responds by displaying a list of files. Locate the patch files with the following filename format:

ncgl_samxts_patch_<rel#>.<wk#>.<major#>.<minor#>

Example
ncgl_samxts_patch_5.31.1.1

ncgl_samxts_patch_5.31.1.2

7 For NCGL patches, copy the patch files from the CD/DVD disk to the patch holding directory on the Session Server unit by typing

```
$ cp <patchfilename> /patch/patchholding
```

and pressing the Enter key.

where

patchfilename
is the file name for the patch file

8 Change directories to root by typing

```
$ cd /
```

and pressing the Enter key.

9 Unmount the DVD-ROM drive by typing

```
$ umount /cdrom
```

and pressing the Enter key.

10 Repeat this procedure on the mate Session Server unit.

11 You have completed this procedure.

Procedure: Acquire patch files from an ESD delivered ISO image

At the Session Server CLI or Integrated EMS client

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

2 Change directories to the directory where the maintenance or upgrade release ISO image (and associated patch files) is located by typing

```
$ cd /opt/swd/<ESD_ISO_directory>
```

and pressing the Enter key.

where

<ESD_ISO_directory>
is the directory containing the version of the ISO image and associated patch files.

Note: There may be multiple directories containing different versions of ISO images.

3 Locate the patch files by typing

```
$ ls
```

and pressing the Enter key.

The system responds by displaying a list of files. Locate patch files with the following filename format:

ncgl_samxts_patch_<rel#>.<wk#>.<major#>.<minor#>

Example
ncgl_samxts_patch_5.31.1.1

ncgl_samxts_patch_5.31.1.2

4 For NCGL patches, copy the patch files from the CD/DVD disk to the patch holding directory on the Session Server unit by typing

```
$ cp <patchfilename> /patch/patchholding
```

and pressing the Enter key.

where

patchfilename
list the file name for the patch file

5 Repeat the previous step for additional patch files you need to install.

6 Repeat this procedure on the mate Session Server unit.

7 You have completed this procedure.

Query status of NCGL patches

Purpose of this procedure

Use this procedure to review the status of patch files on a Session Server unit and to ensure that a patching file has been installed on both units in the node. This procedure may be used as a standalone task or as part of a higher level activity.

Two patch query methods are available:

- Displaying patch status information for all NCGL patches on page 143
- Displaying detailed information for a specific NCGL patch on page 143

Restrictions and Limitations

There are no restrictions for performing this procedure.

Prerequisites

Patch files must first be copied to the Session Server unit.

Action

Displaying patch status information for all NCGL patches

At the Session Server CLI or Integrated EMS client

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

2 To display patch status information for all NCGL patches type:

 # patch_ha -o QueryAll

and press the Enter key.

3 To compare this patch information to that on the mate unit, repeat this procedure for the second (mate) Session Server unit.

4 You have completed this procedure.

Displaying detailed information for a specific NCGL patch

At the Session Server CLI or Integrated EMS client

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

2 To display detailed patch status information for a specific patch on a unit, at the prompt type:

```
# patch_ha -v <patch_version> -o QueryPatch
```

and press the Enter key.

where

patch_version
is the name of the patch file to be queried in the format: <NCGL_release_number>.<week_number>.<major_version_number>.<minor_version_number>

3 To compare this patch information to that on the mate unit, repeat this procedure for the second (mate) Session Server unit.

4 You have completed this procedure.

Apply and commit an NCGL patch

Purpose of this procedure

Use this procedure to apply patch files to the inactive Session Server unit. This procedure should only be used as part of the high level activity *Patching the NCGL operating system and installed applications* in the Session Server Upgrades NTP, NN10349-461.

Restrictions and Limitations

ATTENTION
NCGL patch files should only be applied the inactive unit.

Patching activities must be completed on both units in the node.

Prerequisites

The patch files must have already been put into the **/patching/patchholding** directory on the Session Server hard drive. Contact your network administrator to determine if this has already been done. Refer to section *Patching the NCGL operating system and installed applications* in the Session Server Upgrades NTP, NN10349-461, to copy patch files to the hard drives.

Use the patching or upgrade release notes to verify if any NCGL patches must first be removed before applying new patches.

Action

At the Session Server CLI or Integrated EMS client

1. Log onto the inactive Session Server unit and change to the root user.
2. Change directory to the patchholding directory by typing

   `$ cd /patching/patchholding`

   and pressing the Enter key.
3. Retrieve and untar the patch files from the patch archive to the /patching/<patch_version>/ directory, and fill the patching subsystem's database with the patch information. At the prompt, type:

   # patch_ha -f <patch_file_name> -o Fetch

   and press the Enter key.

where

patch_file_name
is the name of the patch archive you want to extract patch files from.

4 Validate the patch file to verify that the patch file is sane, and the patch is ready to be applied. At the prompt type:

 # patch_ha -v <patch_version> -o Validate

and press the Enter key.

where

patch_version
is the name of the patch file to be applied

5 Apply the patch file. Type:

 # patch_ha -v <patch_version> -o Apply

and press the Enter key.

where

patch_version
is the name of the patch file to be applied

ATTENTION
NCGL patches are not automatically committed when applied. In order for a patch to reapply the next time the unit is rebooted, it must first be committed.

6 Commit the patch so it is auto-applied at each reboot of the unit. Type:

patch_ha -v <patch_version> -o Commit

and press the Enter key.

where

patch_version
is the name of the patch file to be committed

7 If necessary, allow the unit to reboot or if requested, perform a reboot using procedure Reboot a Session Server unit on page 98. Otherwise go to the next step.

8 Perform a status check of the unit including checking for newly generated logs and alarms, to ensure the inactive unit is operating without error. Refer to the Session Server Fault Management NTP, NN10332-911, for applicable procedures. If

errors occur that are related to the patching activity, contact your next level of support.

Note: Checking unit status may entail different activities depending on the what type of software item has been patched and any special patch application requirements. For example, some software subsystem processes may require a reboot before a patch can become active, whereas other subsystem processes restart with the new patched version once patch application is complete.

9 You have completed this procedure. If you were patching files as part of an upgrade activity, then return to the high-level activity.

Remove an NCGL patch

Purpose of this procedure

Use this procedure to remove patches from the inactive Session Server unit. This procedure should only be used as part of the high level task Patching the NCGL operating system on page 50.

Restrictions and Limitations

ATTENTION
NCGL patch files should only be removed from the inactive unit.

Patching activities must be completed on both units in the node.

Prerequisites

Verify which patches should be removed by referring to the patching or maintenance release notes.

Action

At the Session Server CLI or Integrated EMS client

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

2 Uncommit the patch by typing:

patch_ha -v <patch_version> -o Uncommit

and pressing the Enter key.

where

patch_version
is the name of the patch file to be uncommitted

3 Remove the patch files and replace them with the files that existed prior to the patch. At the prompt type:

 # patch_ha -v <patch_version> -o Remove

and press the Enter key.

where

patch_version
is the name of the patch file to be removed

4 Delete the patch file. Type:

 # patch_ha -v <patch_version> -o Delete

and press the Enter key.

where

patch_version
is the name of the patch file to be deleted

5 If necessary, allow the unit to reboot or if requested, perform a reboot using procedure Reboot a Session Server unit on page 98. Otherwise go to the next step.

6 Perform a status check of the unit including checking for newly generated logs and alarms, to ensure the inactive unit is operating without error. Refer to the Session Server Fault Management NTP, NN10332-911, for applicable procedures. If errors occur that are related to the patch removal activity, contact your next level of support.

Note: Checking unit status may entail different activities depending on the what type of software item has been patched and any special patch application requirements. For example, some software subsystem processes may require a reboot before a pre-patched version can become active, whereas other subsystem processes restart once patch removal is complete.

7 Complete procedure Invoke a maintenance SwAct of the Session Server platform on page 170.

8 Repeat this procedure for the second (mate) Session Server unit, now the new standby unit.

9 You have completed this procedure. If you were patching files as part of an upgrade activity, then return to the high-level activity.

View web proxy settings in SSPFS for Session Server

Purpose of this procedure

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

Limitations and restrictions

If the web proxy entry for a particular Session Server node requires changing, you must configure a new proxy entry with the modified values, then remove the obsolete proxy entry. Do not use this procedure to add a new Session Server node to the proxy service configuration. To perform this activity, refer to procedure *Add a Session Server node to the SSPFS server web proxy*, found in the Session Server Configuration NTP, NN10338-511.

Prerequisites

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

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

Refer to section *Understanding Session Server IP addressing*, found in the Session Server Configuration NTP, NN10338-511, for more information about Session Server IP addressing and naming schemes needed to complete this activity. The following IP addresses are referenced in this activity:

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

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

Action

At the Session Server CLI or Integrated EMS client

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

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

3 Change to the root user by typing

`su - root`

and pressing the Enter key.

4 Enter the root password and press Enter.

5 Start the command line interface application by typing

`cli`

and pressing the Enter key.

The system responds:

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

6 Access the Configuration level by typing

2

and pressing the Enter key.

The system responds:

```
Configuration

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

7 Access the Apache Proxy Configuration level by typing

2

and pressing the Enter key.

The system responds:

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

 X - exit

select -
```

8 List the current Apache Proxy Configuration entries by typing

3

and pressing the Enter key.

The system responds:

```
=== Executing "list_proxy_conf"
```

```
#Begin Proxy Config
<IfModule mod_proxy.c>
  ProxyRequests On
  # Add Proxy Entries Here
  ProxyPass /47.174.74.184/ https://47.174.74.184:443/
  ProxyPassReverse /47.174.74.184/ https://47.174.74.184:443/
  ProxyPass /47.142.209.118/ https://47.142.209.118:443/
 ProxyPassReverse /47.142.209.118/ https://47.142.209.118:443/
  ProxyPass /47.142.209.116/ https://47.142.209.116:443/
 ProxyPassReverse /47.142.209.116/ https://47.142.209.116:443/
  ProxyPass /prov/ https://47.174.74.184:8443/prov/
  ProxyPassReverse /prov/ https://47.174.74.184:8443/prov/
  AllowCONNECT 433
  <Proxy *>
    Order deny,allow
    Allow from all
  </Proxy>

      </IfModule>
      #End Proxy Config
      === "list_proxy_conf" completed successfully
```

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

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

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

ATTENTION

If necessary, please refer to section Selecting and using tag names in SN08 and beyond on page 155 for more information about using remote tag names. The tag name shown must match the tag name used by the SIP Gateway application for the same Session Server node when you installed or upgrading it.

11 Exit the Apache Proxy Configuration level by typing

x

and pressing the Enter key.

You are returned to the SSPFS operating system.

12 Exit the Configuration level by typing

```
x
```

and pressing the Enter key.

You are returned to the SSPFS operating system.

13 Exit the CLI by typing

```
x
```

and pressing the Enter key.

You are returned to the SSPFS operating system.

14 If applicable, logout from the workstation.

Selecting and using tag names in SN08 and beyond

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

ATTENTION

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

If the remote tag name for a Session Server node does not match that used during installation or upgrade of the SIP Gateway application, you must configure a new proxy entry using the correct remote tag name, then remove the obsolete proxy entry. To perform this activity, refer to procedure *Add a Session Server node to the SSPFS server web proxy*, found in the Session Server Configuration NTP, NN10338-511.

Upgrade/rollback/reinstall a Session Server application

Purpose of this procedure

Use the following procedure to install any version of a Session Server application onto a Session Server unit including:

- reinstalling a current version of the SIP Gateway Application
- upgrading to a newer version of the SIP Gateway Application
- rolling back to a previous version of the SIP Gateway Application

ATTENTION

It is recommended that this procedure only be used as part of the high level activity Upgrading from a previous major release - SN07 to SN08 on page 4 or *Applying a maintenance release upgrade*, found in the Session Server Upgrades NTP, NN10349-461.

Limitations and restrictions

If the Session Server node is in operation and performing call processing activities, only perform this procedure on the standby unit.

This procedure must be performed on both Session Server units based on the upgrade or rollback activity being performed.

Prerequisites

CAUTION

Use care when using this procedure. This procedure may cause the loss of customer data. Ensure that you have backed up the SIP Gateway application database before executing this procedure.

Action

If you are reinstalling, upgrading or rolling back the SIP Gateway application from a CD/DVD disk, proceed with procedure Procedure: Reinstall, upgrade or rollback the SIP Gateway application from a CD/DVD disk.

If reinstalling, upgrading or rolling back the SIP Gateway application from an ESD delivered ISO image file, then go to Procedure: Reinstall, upgrade or rollback the SIP Gateway application from an ISO image file on page 160.

Procedure: Reinstall, upgrade or rollback the SIP Gateway application from a CD/DVD disk

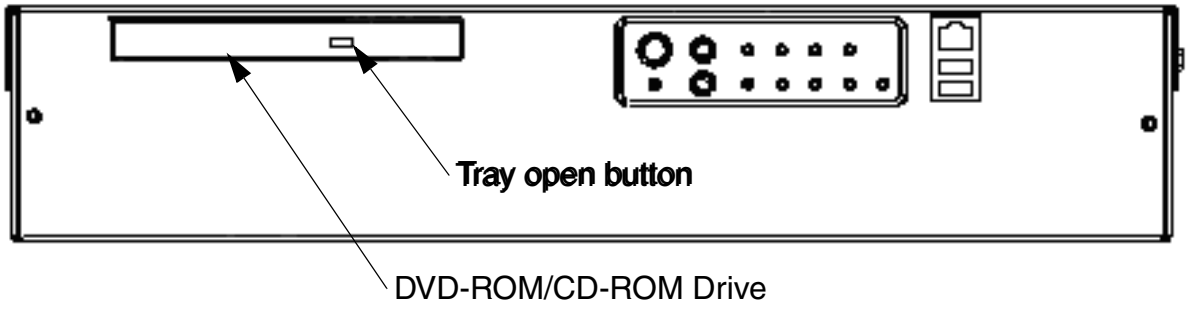
At the Session Server CLI or Integrated EMS client

1 Log onto the Session Server unit using a secure shell (ssh) and change to root user.

2 Ensure that the CD/DVD disk containing the SIP Gateway Application is inserted before continuing.

Note: In some cases the SIP Gateway Application may be on its own disk or it may be on the NCGL CD/DVD disk.

Session Server Front Panel



3 At the prompt, type

cd /

and press Enter.

4 At the prompt, type

mount /cdrom

and press Enter.

The operating system may respond with the following warning:

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

5 From the root level, at the prompt, type

/cdrom/InstallApps APP_NAME

and press Enter.

where

APP_NAME
is SIPGW, for the SIP Gateway application

The operating system responds:

```
The NGSS Application layer is currently
installed. Do you wish to uninstall the previous
application and install the newer version? (yes,
no)
```

6 Type

yes

and press Enter.

The inactive unit begins installing the application. You will see messages scrolling on the screen. No action is needed. Ignore any “No such file or directory" messages.

7 For upgrading to SN08 only, when prompted, enter a remote tag name for this unit, of up to 64 alphanumeric characters, including period, hyphen and underscore and press Enter. For the Session Server node you are upgrading from SN07, you must reuse the existing SN07 tag names “prov” or “/prov”.

ATTENTION
The tag name you select must match the tag name used by the SSPFS web proxy server.

ATTENTION
If you are rolling back to SN07 from SN08, the SSPFS web proxy server must be using the “prov” tag name. Use procedure *View web proxy settings in SSPFS for Session Server*, in the Session Server Configuration Management NTP, NN10338-511, to verify the tag name currently in use.

Note 1: If you are performing an SN08 or greater maintenance release and changing the remote tag name, the following labels cannot be used for a remote tag name:

- spc
- ROOT
- webdav
- admin.xml
- manager.xml

Note 2: Starting in SN08, multiple Session Server nodes, made up of two units per node, can be installed in the CS-LAN network. Therefore, each node installed on the CS-LAN must have its own unique remote tag name (used on both units in the node). Failure to follow this rule will prevent you from accessing a node's GUIs properly. Refer to section "Using multiple tag names for multiple Session Server nodes", part of procedure *Add a Session Server node to the SSPFS server web proxy*, in the Session Server Configuration Management NTP, NN10338-511, for more information about using multiple remote tag names.

8 After the SIP application has completed installation, at the prompt, type

cd /

and press Enter.

9 Unmount the disk drive by typing

umount /cdrom

and pressing the Enter key.

10 Press the tray open button and remove the CD/DVD disk from the drive.

11 You have completed this procedure. If applicable, return to the high-level activity.

Procedure: Reinstall, upgrade or rollback the SIP Gateway application from an ISO image file

At the Session Server CLI or Integrated EMS client

1 Log onto the inactive Session Server unit using a secure shell by typing

> **ssh -l <userid> <inactive_SS_IP_address>**

and pressing the Enter key.

where

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

inactive_SS_IP_address
is the IP address or host name of the Session Server unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

$ **su - root**

and pressing the Enter key.

4 When prompted, enter the root password.

5 Verify that the DVD-ROM drive is not currently mounted to the /cdrom directory by typing

umount /cdrom

and pressing the Enter key.

6 At the prompt, type

mount -o loop /opt/swd/<ESD_ISO_directory>/<ESD_file_ISO> /cdrom

and press **Enter**.

where

ESD_file_ISO
is the name of the maintenance release or upgrade ISO file

Example
mount -o loop /opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_MNCL.ISO. /cdrom

The operating system responds with the following warning:

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

7 From the root level, at the prompt, type

/cdrom/InstallApps APP_NAME

and press Enter.

where

APP_NAME
is SIPGW, for the SIP Gateway application

The operating system responds:

```
The NGSS Application layer is currently
installed. Do you wish to uninstall the previous
application and install the newer version? (yes,
no)
```

8 Type

yes

and press Enter.

The inactive unit begins installing the application. You will see messages scrolling on the screen. No action is needed. Ignore any “No such file or directory" messages.

9 For upgrading to SN08 only, when prompted, enter a remote tag name for this unit, of up to 64 alphanumeric characters, including period, hyphen and underscore and press Enter. For the Session Server node you are upgrading from SN07, you must reuse the existing SN07 tag names “prov” or “/prov”.

ATTENTION
The tag name you select must match the tag name used by the SSPFS web proxy server.

ATTENTION
If you are rolling back to SN07 from SN08, the SSPFS web proxy server must be using the “prov” tag name. Use procedure *View web proxy settings in SSPFS for Session Server*, in the Session Server Configuration Management NTP, NN10338-511, to verify the tag name currently in use.

Note 1: If you are performing an SN08 or greater maintenance release and changing the remote tag name, the following labels cannot be used for a remote tag name:

- spc
- ROOT
- webdav
- admin.xml
- manager.xml

Note 2: Starting in SN08, multiple Session Server nodes, made up of two units per node, can be installed in the CS-LAN network. Therefore, each node installed on the CS-LAN must have its own unique remote tag name (used on both units in the node). Failure to follow this rule will prevent you from accessing a node's GUIs properly. Refer to section "Using multiple tag names for multiple Session Server nodes", part of procedure *Add a Session Server node to the SSPFS server web proxy*, in the Session Server Configuration Management NTP, NN10338-511, for more information about using multiple remote tag names.

10 After the application has completed installation, at the prompt, type

cd /

and press Enter.

11 Unmount the ISO image by typing

umount -f /opt/swd/<ESD_ISO_directory>/<ESD_file_ISO>

and pressing Enter.

Example
umount -f
/opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_MNCL.ISO

12 You have completed this procedure. If applicable, return to the high-level activity.

Verify synchronization status of Session Server units

Purpose of this procedure

Use this procedure to determine the synchronization status of the Session Server units. This procedure may be used as a standalone task or as part of a higher level activity.

Limitations and restrictions

There are no restrictions for performing this procedure.

Prerequisites

There are no prerequisites for performing this procedure.

Action

At the Session Server GUI or Integrated EMS client

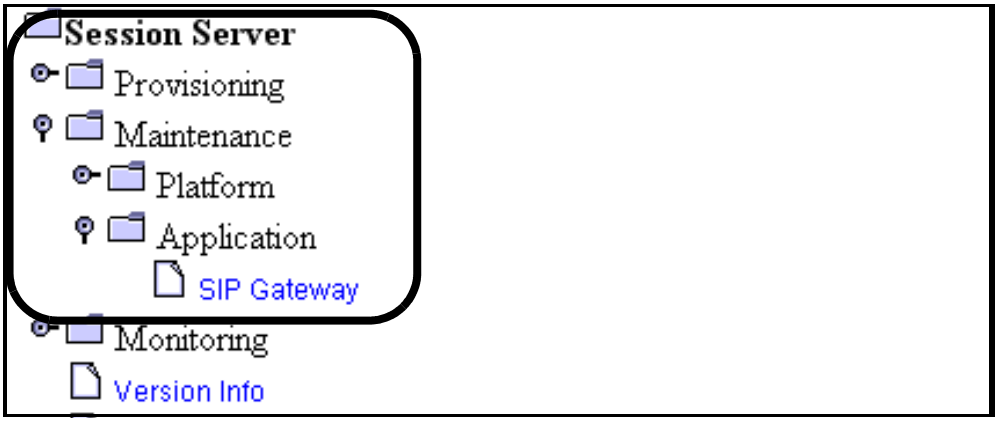
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

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

Please select one of the following management interfaces:

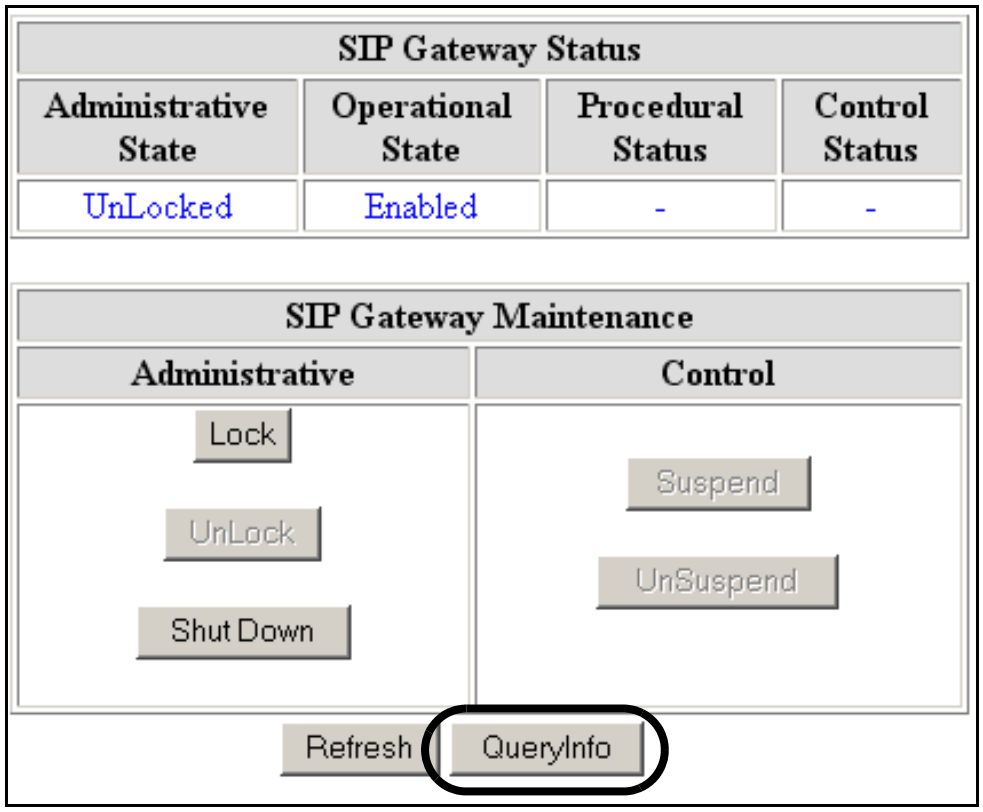
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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



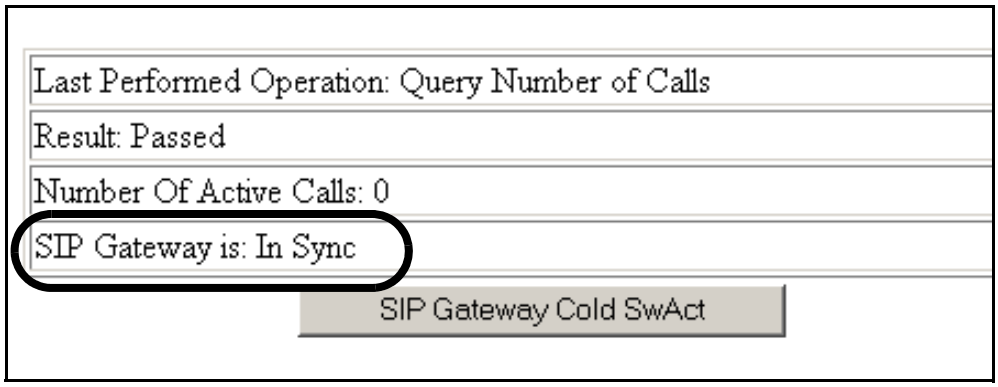
3 Click on the **SIP Gateway** folder to open it.

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



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

If the units are not in sync, execute procedure *View Session Server alarms*, found in the Session Server Fault Management NTP, NN10332-911, and check for alarm conditions.



6 The procedure is complete.

Enable a system SwAct (Unjam)

Purpose of this procedure

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

Limits and Restrictions

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

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

Prerequisites

There are no prerequisites for performing this procedure.

Action

At the Session Server GUI or Integrated EMS client

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

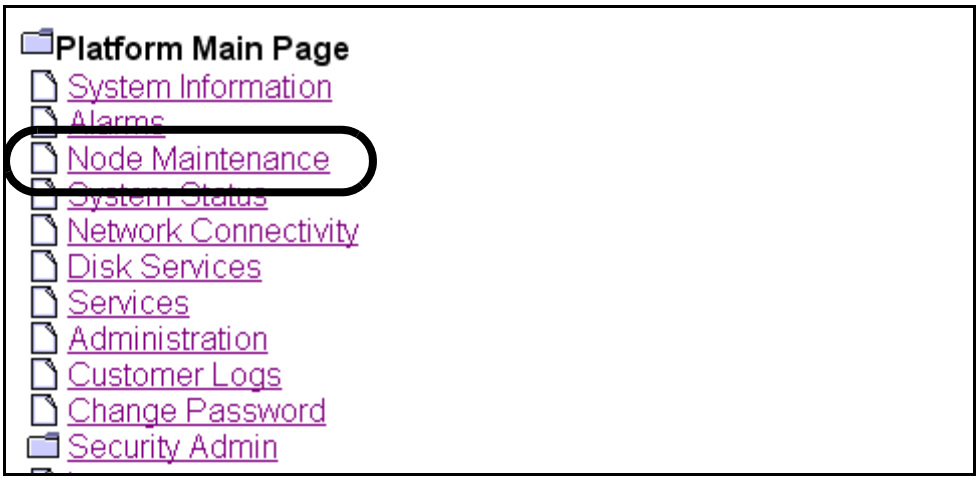
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

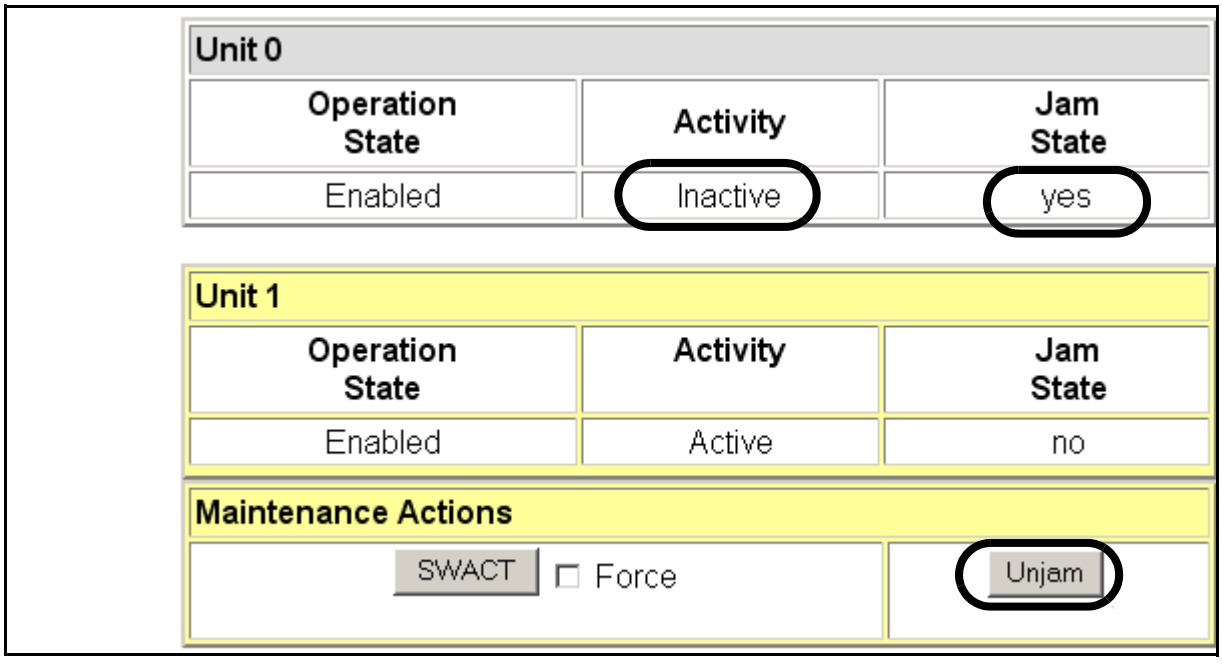
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Node Maintenance** link.

The Node Maintenance page is displayed.



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

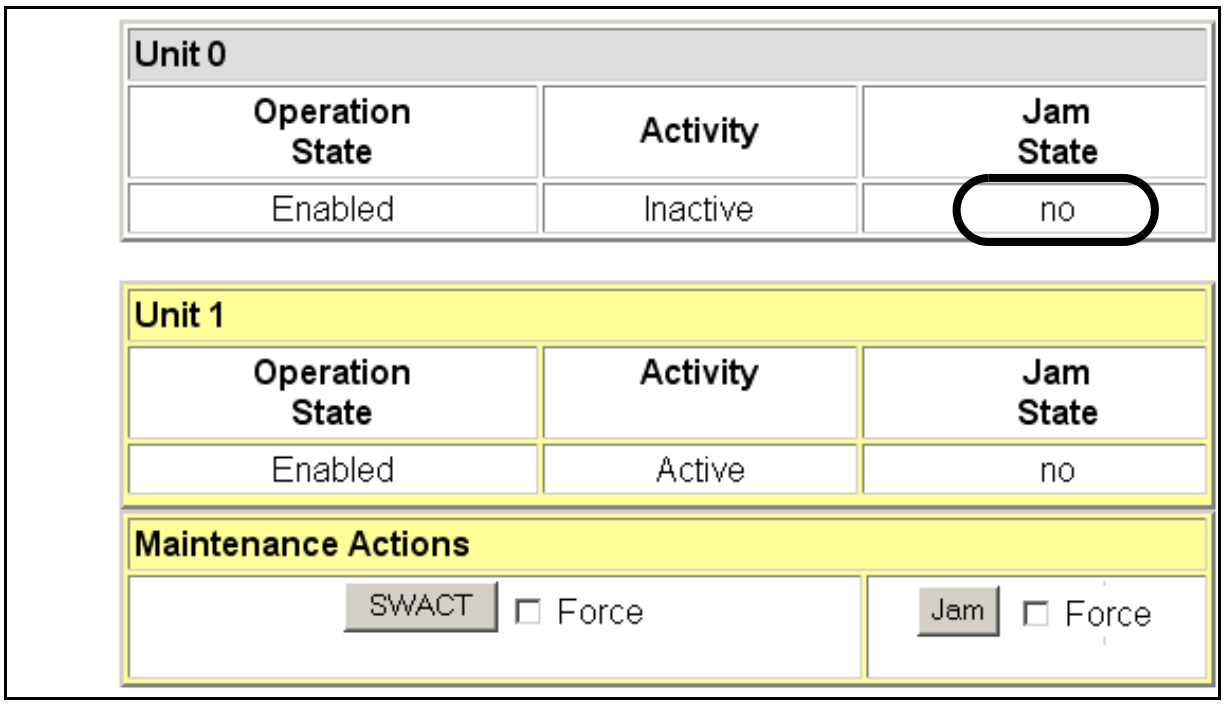


4 Click the **UnJam** button.

The system responds:

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

5 Observe the Jam state for the standby session server unit transitions from Yes to No.



6 This procedure is complete.

Invoke a maintenance SwAct of the Session Server platform

Purpose of this procedure

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

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

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

Limits and Restrictions

ATTENTION
A maintenance SwAct should only be performed when both the active and standby units are operationally enabled and their databases are synchronized.

You cannot SwAct Session Server units if the active unit Jam state is *jammed*. If the unit Jam state is jammed, refer to procedure Enable a system SwAct (Unjam) on page 167 to unjam the unit.

ATTENTION
Logins to the Session Server do not survive a platform SwAct.

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

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

Prerequisites

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

Action

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

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

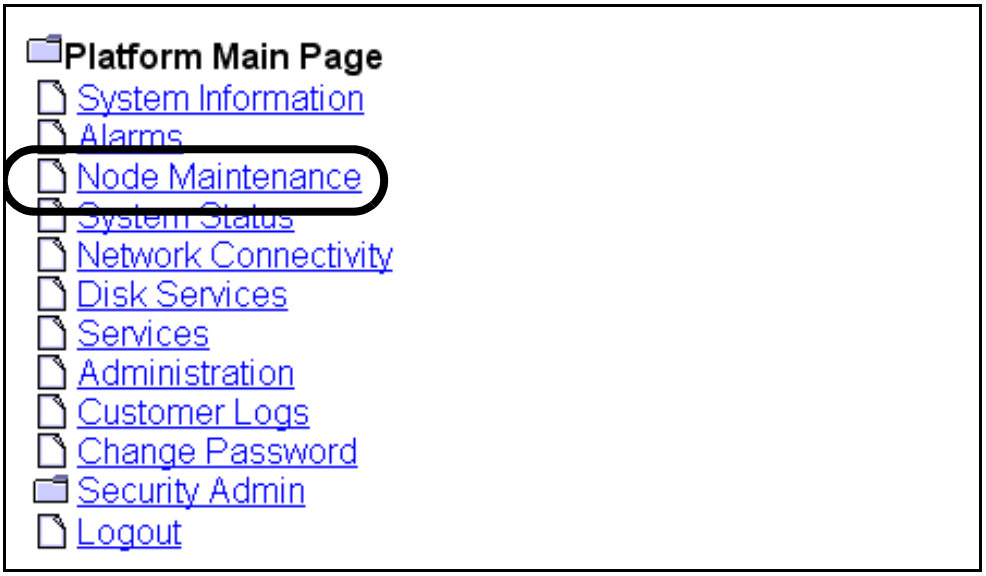
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

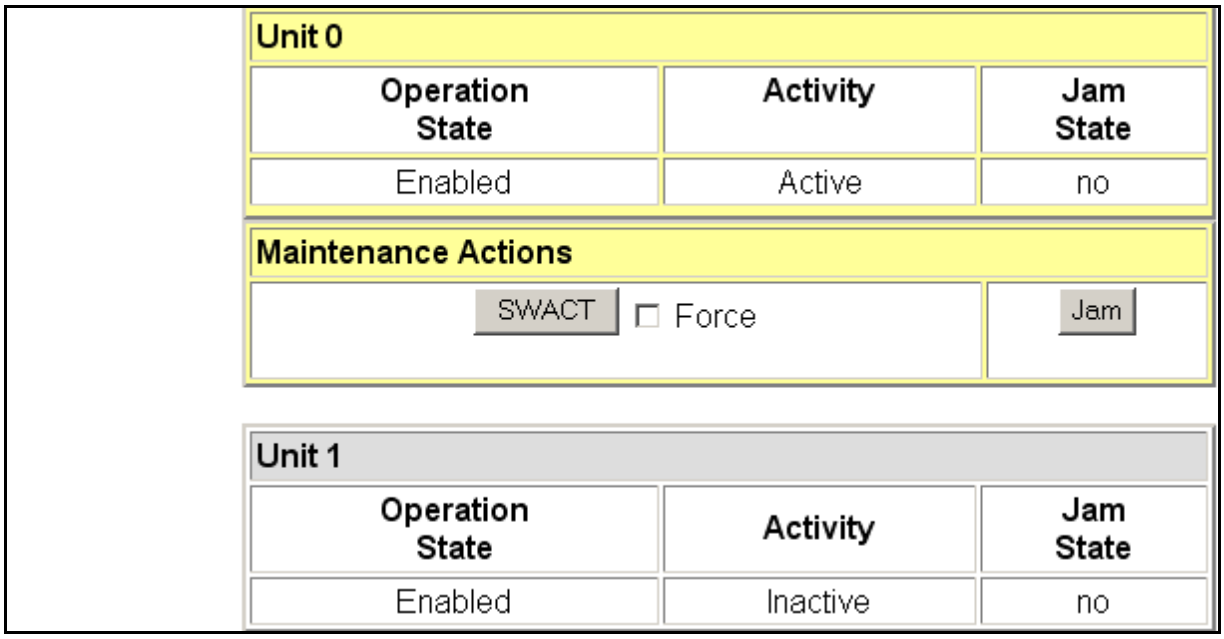
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

2 Click the **Node Maintenance** link.

The Node Maintenance page is displayed.



3 Refer to the table in section Additional status information on page 173 to review the description of the various fields of the Node Maintenance page.



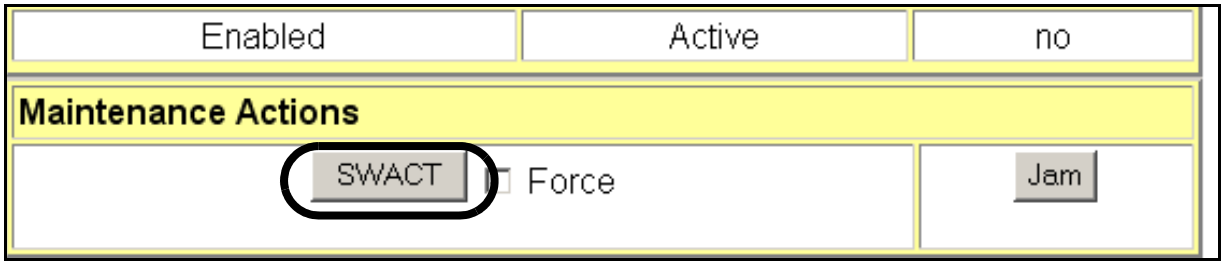
4 To SwAct the Session Server units, click the **SWACT** button.

or

To override any pre-SwAct queries, first click the **Force** check box, then click the **SWACT** button. Refer to section To SWACT or Force a SWACT? on page 174 for details regarding which type of SWACT to chose.

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.



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.

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

7 The procedure is complete.

Additional status information

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

Field	Description
Operation State (unit 0 or 1)	The operational state of the platform software, either enabled or disabled.
Activity (unit 0 or 1)	The 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.

To SWACT or Force a SWACT?

A forced SWACT overrides any SWACT pre-checks and is not recommended. SWACT pre-checks monitor the inactive unit for critical faults on the platform that should prevent a SWACT. In addition, the pre-check ensures that the SIP Gateway application is in-sync. A SWACT force may result in a full service outage on the Session Server 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.

Copy security certificates to the mate unit

Purpose of this procedure

The following procedure is used to copy security certificates from one Session Server unit to another.

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. This procedure may also be used as part of a major release upgrade activity.

Limitations and Restrictions

There are no restrictions for performing this procedure.

Prerequisites

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

Action

Perform the following steps to complete this procedure.

At the Session Server CLI or Integrated EMS client

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

2 Change directories to the security certificates level by typing

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

and pressing the Enter key.

3 Secure copy the server.key file to the mate Session Server unit by typing

```
$ scp server.key
mtc@<mate_SS_IP_address>:/users/mtc
```

and pressing the Enter key.

where

mate_SS_IP_address
is the IP address of the mate Session Server unit

Note: For initial connections to the mate unit, confirm that you want to continue connecting by entering “yes.”

The mate unit responds by prompting for the password for the mtc user.

4 Enter the password for the mtc user at the password prompt.

The server.key file is copied to the /users/mtc directory on the mate Session Server unit. This is the only Session Server directory that files can be copied into from an external server.

5 Secure copy the certificate.keystore file to the mate Session Server unit by typing

```
$ scp certificate.keystore
mtc@<mate_SS_IP_address>:/users/mtc
```

and pressing the Enter key.

where

mate_SS_IP_address
is the IP address of the mate Session Server unit

The mate unit responds by prompting for the password for the mtc user.

6 Enter the password for the mtc user at the password prompt.

The certificate.keystore file is copied to the /users/mtc directory on the mate Session Server unit. This is the only Session Server directory that files can be copied into from an external server.

7 Secure copy the server.crt file to the mate Session Server unit by typing

```
$ scp server.crt
mtc@<mate_SS_IP_address>:/users/mtc
```

and pressing the Enter key.

where

mate_SS_IP_address
is the IP address of the mate Session Server unit

The mate unit responds by prompting for the password for the mtc user.

8 Enter the password for the mtc user at the password prompt.

The server.crt file is copied to the /users/mtc directory on the mate Session Server unit. This is the only Session Server directory that files can be copied into from an external server.

9 If you have a CA-signed certificate, secure copy the trusted.crt file to the mate Session Server unit by typing

```
$ scp trusted.crt
mtc@<mate_SS_IP_address>:/users/mtc
```

and pressing the Enter key.

where

mate_SS_IP_address
is the IP address of the mate Session Server unit

The mate unit responds by prompting for the password for the mtc user.

10 If applicable, enter the password for the mtc user at the password prompt. Otherwise, skip to the next step.

The trusted.crt file is copied to the /users/mtc directory on the mate Session Server unit. This is the only Session Server directory that files can be copied into from an external server.

At your workstation CLI or Integrated EMS client

11 Log into to the mate Session Server and change to the root user.

12 Change directories to the /users/mtc level by typing

```
cd /users/mtc
```

and pressing the Enter key.

13 Move the server.key file from the /users/mtc directory to the /opt/base/share/ssl directory by typing

```
$ mv server.key /opt/base/share/ssl
```

and pressing the Enter key.

14 If necessary, confirm overwriting any existing server.key file by typing **y** and pressing Enter.

15 Move the certificate.keystore file from the /users/mtc directory to the /opt/base/share/ssl directory by typing

```
$ mv certificate.keystore /opt/base/share/ssl
```

and pressing the Enter key.

16 If necessary, confirm overwriting any existing certificate.keystore file by typing **y** and pressing Enter.

17 Move the server.crt file from the /users/mtc directory to the /opt/base/share/ssl directory by typing

```
$ mv server.crt /opt/base/share/ssl
```

and pressing the Enter key.

18 If necessary, confirm overwriting any existing server.crt file by typing **y** and pressing Enter.

19 If you have a CA-signed certificate, move the trusted.crt file from the /users/mtc directory to the /opt/base/share/ssl directory by typing

```
$ mv trusted.crt /opt/base/share/ssl
```

and pressing the Enter key.

20 If necessary, confirm overwriting any existing trusted.crt file by typing **y** and pressing Enter.

21 Change directories to the security certificates level by typing

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

and pressing the Enter key.

22 Change the key file's owner and group to *root* by typing

```
# chown root:root server.key
```

and pressing the Enter key.

23 Change the keystore file's owner and group to *root* by typing

```
# chown root:root certificate.keystore
```

and pressing the Enter key.

24 Change the certificate's owner and group to *root* by typing

```
# chown root:root server.crt
```

and pressing the Enter key.

25 If you have a CA-signed certificate, change the trusted certificate file's owner and group to *root* by typing

```
# chown root:root trusted.crt
```

and pressing the Enter key.

26 Set the key file permissions by typing

```
# chmod 600 server.key
```

and pressing the Enter key.

27 Set the keystore file permissions by typing

```
# chmod 600 certificate.keystore
```

and pressing the Enter key.

28 Set the certificate permissions by typing

```
# chmod 644 server.crt
```

and pressing the Enter key.

29 If you have a CA-signed certificate, set the keystore file permissions by typing

```
# chmod 644 trusted.crt
```

and pressing the Enter key.

30 You have completed this procedure. If you completed this procedure as part of an upgrade activity, return to the high level activity.

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

Restore a previous version of security certificates

Purpose of this procedure

The following procedure is restore backup copies of security certificates on the Session Server unit from a previous release.

This procedure should only be used as part of a major release abort or rollback activity.

Limitations and Restrictions

There are no limitations on performing this procedure.

Prerequisites

This procedure assumes that you have previously made backup copies of the CA-signed or self-signed security certificates from the previous release using procedure Back up security certificates on page 58.

Action

Perform the following steps to complete this procedure.

At the Session Server CLI or Integrated EMS client

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

2 Ensure that you have made a backup copy of your current security certificates to an SN08 (backup) using procedure Back up security certificates on page 58.

ATTENTION

Failure to complete this step properly will result in your current security certificates being overwritten, possibly resulting in loss of any newly generated security certificate information.

3 Change directories to the location where the backup of the previous software release's security certificates are stored by typing.

```
# cd /opt/base/share/ssl/<SNxx_ddmmyyyy>
```

and press the Enter key.

where

SNxx_ddmmyyyy
is the name of the previous release's backup directory

Example
cd /opt/base/share/ssl/SN07_04032005

4 Verify the contents of the backup directory by typing

 # ls -l

and press the Enter key.

where

SNxx_ddmmyyyy
is the name of the new backup directory

Sample system response:

```
-rw-r--r--  1 root   root  1858 Dec 10 11:11
certificate.keystore

-rw-r--r--  1 root   root  190 Dec 10 11:11 gen_cert.txt

-rw-r--r--  1 root   root  3249 Dec 10 11:11 server.crt

-rw-------  1 root   root  887 Dec 10 11:11 server.key

-rw-r--r--  1 root   root  1254 Dec 10 11:11 trusted.crt
```

5 Use the following table to determine your next step:

If	Do
the backup directory is empty or contains files other than those shown in the previous example	go to step 10. You are either in the wrong backup directory or you did not properly back up the previous version's security certificates. If necessary, contact Nortel GNPS for assistance.
the backup directory contains files similar to the example shown in the previous step (files and the number of files may vary)	step 6

6 Copy the certificates to the /opt/base/share/ssl directory by typing

 # cp * /opt/base/share/ssl

and press the Enter key.

ATTENTION
You are about to overwrite the current security certificates on this unit.

7 Change directories to the /opt/base/share/ssl directory. Type

 # cd /opt/base/share/ssl

and press the Enter key.

8 Verify the contents of the backup directory were restored to the opt/base/share/ssl directory by typing

 # ls -l

and press the Enter key.

Sample system response:

```
-rw-r--r--  1 root   root  1858 Dec 10 11:11
certificate.keystore

-rw-r--r--  1 root   root  190 Dec 10 11:11 gen_cert.txt

-rw-r--r--  1 root   root  3249 Dec 10 11:11 server.crt

-rw-------  1 root   root  887 Dec 10 11:11 server.key

-rw-r--r--  1 root   root  1254 Dec 10 11:11 trusted.crt
```

Note: *File size values will vary.*

9 Repeat this procedure on the mate Session Server unit.

10 You have completed this procedure.

Rollback a Session Server NCGL platform software upgrade

Purpose of this procedure

This procedure describes how to use the CS 2000 NCGL Platform Manager software to rollback an NCGL platform load.

ATTENTION
This procedure should only be used as part high level activities for aborting or rolling back maintenance releases or major release upgrades.

Limitations and Restrictions

You can only rollback to a previous load if it still exists on the Session Server unit disk drive. If not, you must reinstall the load onto the disk drive from DVD-ROM disk or ESD ISO image. Refer to section Prepare for a major release upgrade on page 8 or Prepare for a maintenance release upgrade on page 31 for instructions to perform this activity.

Prerequisites

ATTENTION
This procedure assumes that you are experiencing problems with a maintenance release or major release upgrade on a single Session Server unit and that you have not upgraded the second unit in the node. If you have already upgraded both units with the and are having problems, then refer to section Perform an emergency maintenance release rollback activity on page 44 or Perform a major release rollback activity on page 22.

Action

At the Session Server GUI or Integrated EMS client

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

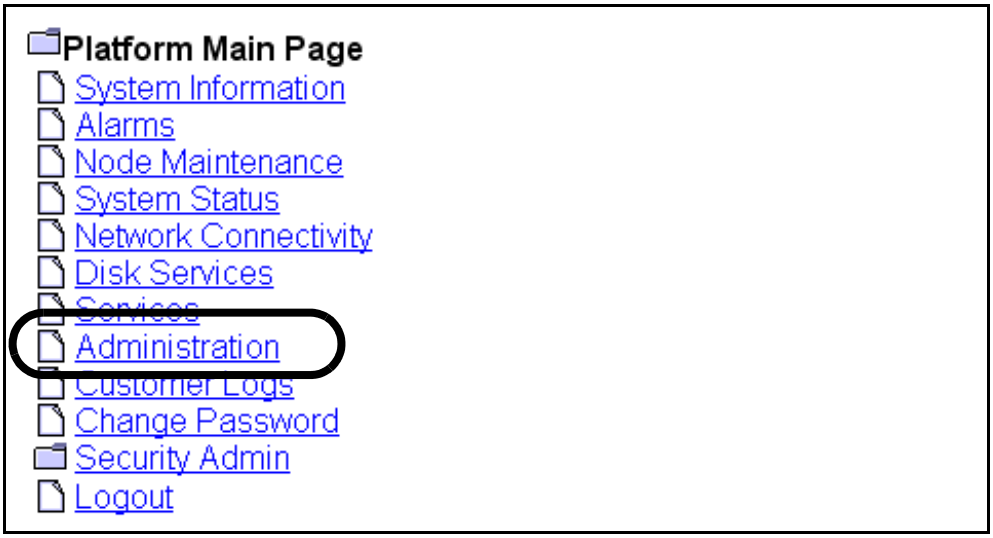
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

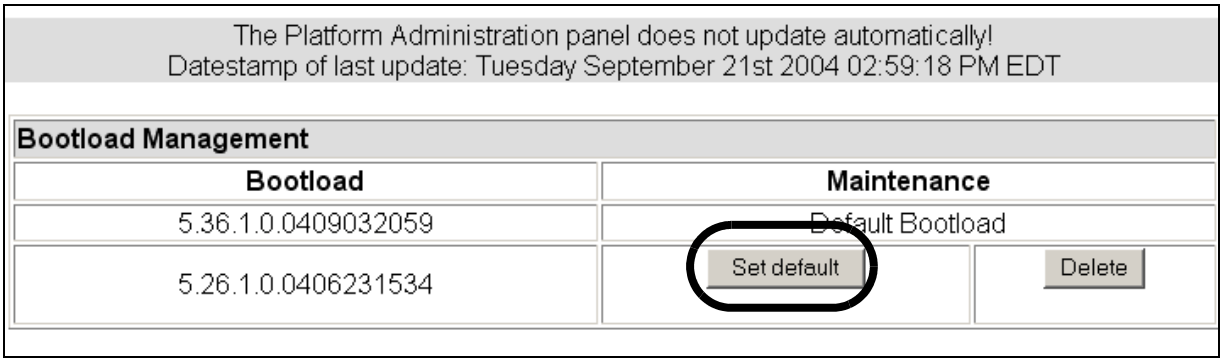
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

The Platform Main Page menu is displayed.

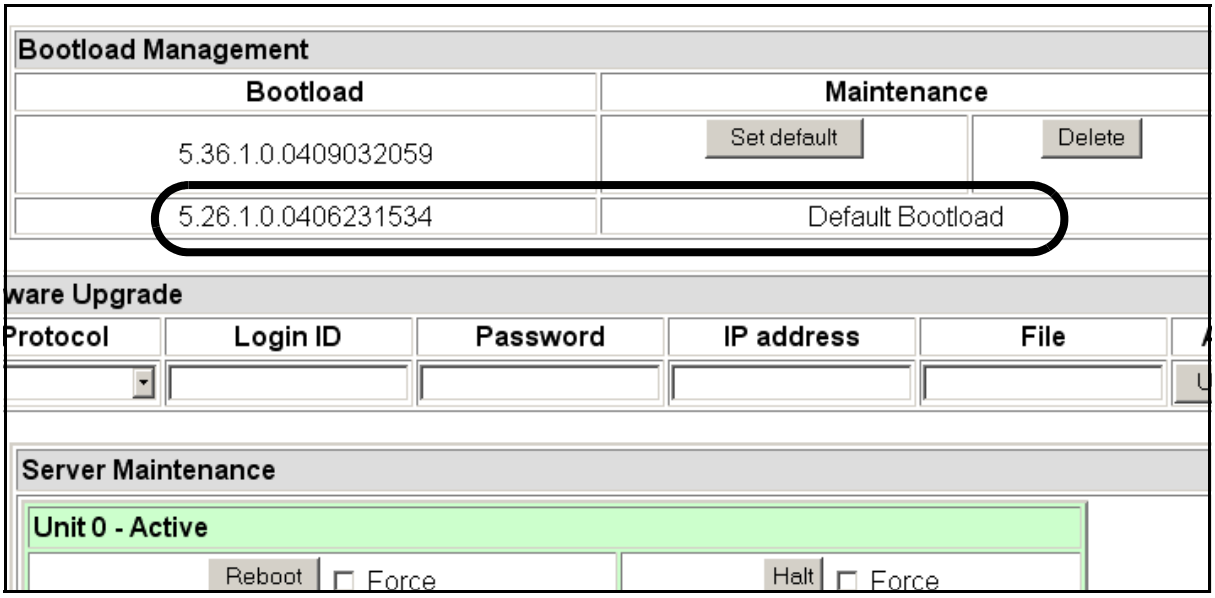
2 Click the **Administration** link.



3 Select the bootload version that you want to roll the NCGL platform back to and click the **Set default** button.



4 Verify that the default bootload has been set to the version previous to the upgrade.



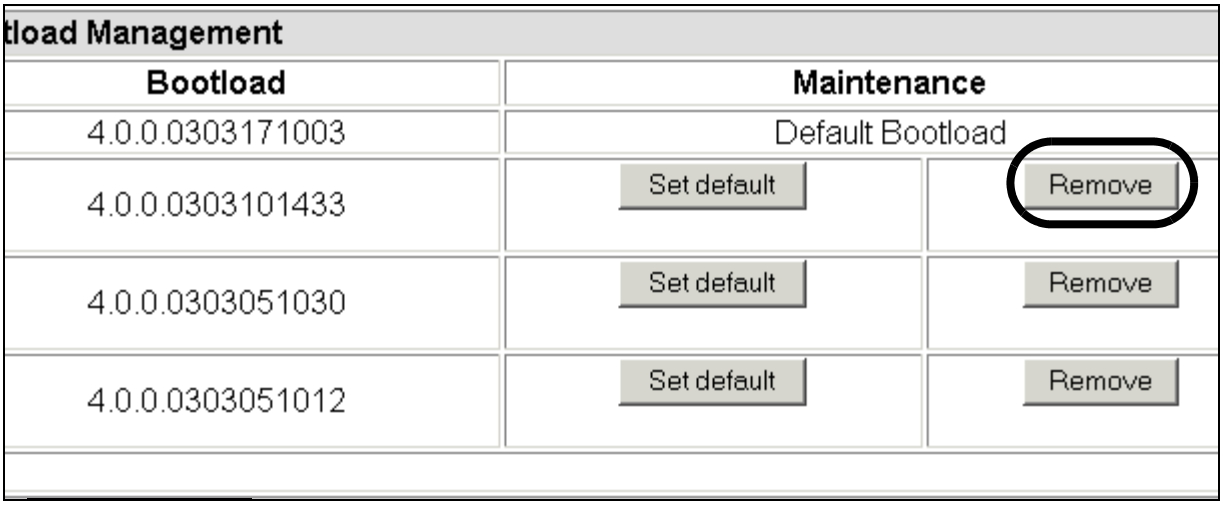
5 You have completed this procedure. Return to your applicable high-level activity.

Additional information

By default, the Session Server units retain previous bootloads. For housekeeping purposes, older bootload versions may be manually removed by clicking the **Remove** button.

Note: You cannot delete the bootload that is set to be the default bootload, nor can you delete the currently running bootload.

If a bootload image upgrade is requested and insufficient disk space is available in the `/boot` directory, the NCGL software deletes the oldest bootload from the `/boot` directory and performs the requested bootload image upgrade. The system can not delete a bootload that is set to be the default bootload.



Drop database synchronization for the SIP Gateway application

Purpose of this procedure

Use the following procedure to drop application database synchronization between the active and inactive Session Server units.

ATTENTION

This procedure should only be used as part of the high level activities Perform an emergency maintenance release rollback activity on page 44 or Perform a major release rollback activity on page 22.

Limitations and restrictions

Perform this procedure only on the active Session Server unit.

Once this procedure has been executed, the SIP Gateway application database continues in a non-synchronized state until a manual SwAct is performed.

CAUTION

Use care when using this procedure. This procedure may cause the loss of customer data.

Prerequisites

Ensure that you have backed up the SIP Gateway application database on the active unit before executing this procedure.

Action

If you are performing this procedure from a DVD-ROM disk, go to Procedure: Run dropSync script from a DVD-ROM disk on page 188.

If you are performing this procedure from an ESD delivered ISO image file, then go to Procedure: Run dropSync script from an ISO image file on page 189.

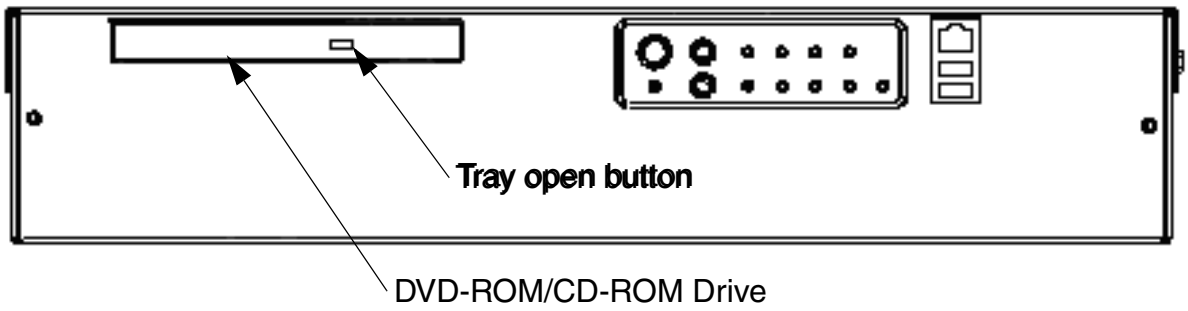
Procedure: Run dropSync script from a DVD-ROM disk

At the Session Server CLI or Integrated EMS client

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

2 Ensure that the latest version of the software installation DVD-ROM disk is inserted into the active unit before continuing.

Session Server Front Panel



3 At the prompt, type

mount /cdrom

and press Enter.

The operating system may respond with the following warning:

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

4 From the root level, at the prompt, type

./cdrom/Tools/dropSync

and press Enter.

5 After you are returned to the prompt, type

cd /

and press Enter.

6 Unmount the disk drive by typing

umount /cdrom

and pressing the Enter key.

7 If desired, press the tray open button and remove the DVD-ROM disk from the drive.

8 You have completed this procedure. Return to the applicable high-level activity.

Procedure: Run dropSync script from an ISO image file

At the Session Server CLI or Integrated EMS client

1 Log onto the active Session Server unit using a secure shell by typing

> **ssh -l <userid> <active_SS_IP_address>**

and pressing the Enter key.

where

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

active_SS_IP_address
is the IP address of the active Session Server unit

Example
ssh -l mtc 45.128.54.12

2 When prompted, enter your password.

3 Change to the root user by typing

$ **su - root**

and pressing the Enter key.

4 When prompted, enter the root password.

5 Verify that the CD/DVD-ROM drive on the active unit is not currently mounted to the /cdrom directory by typing

umount /cdrom

and pressing the Enter key.

6 At the prompt, type

mount -o loop /opt/swd/<ESD_ISO_directory>/<ESD_file_ISO> /cdrom

and press **Enter**.

where

ESD_file_ISO
is the name of the maintenance release or major upgrade ISO file

Example
mount -o loop /opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_MNCL.ISO. /cdrom

The operating system responds with the following warning:

```
mount: block device /dev/hda is
write-protected, mounting read-only
```

7 From the root level, at the prompt, type

./cdrom/Tools/dropSync

and press **Enter**.

8 After the application has completed installation, at the prompt, type

cd /

and press Enter.

9 Unmount the ISO image by typing

umount -f /opt/swd/<ESD_ISO_directory>/<ESD_file_ISO>

and pressing Enter.

Example
umount -f
/opt/swd/NGSS0070.70.P.NCL.NAP.VAULT.6.D/NGSS07_
MNCL.ISO

10 You have completed this procedure. Return to the applicable high-level activity.

Lock the SIP Gateway application

Purpose of this procedure

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

Limitations and restrictions

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

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

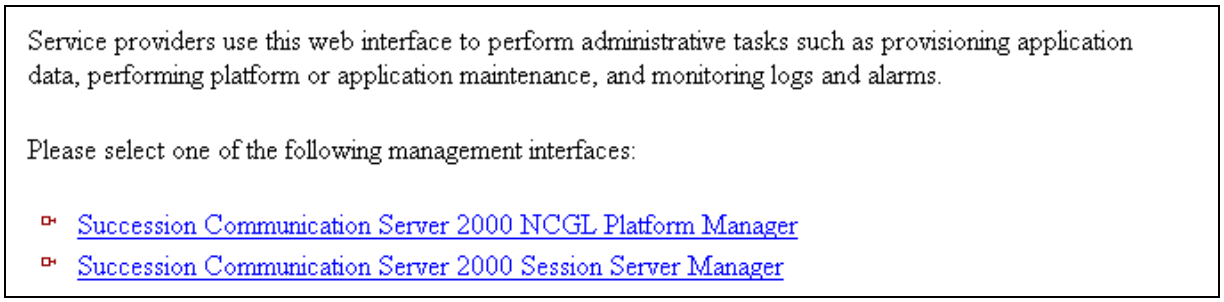
Prerequisites

There are no prerequisites for this procedure.

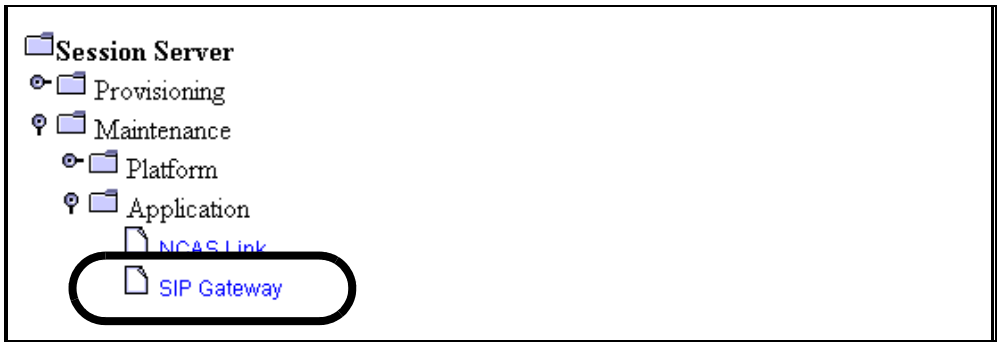
Action

At the CS 2000 Session Server Manager or Integrated EMS client

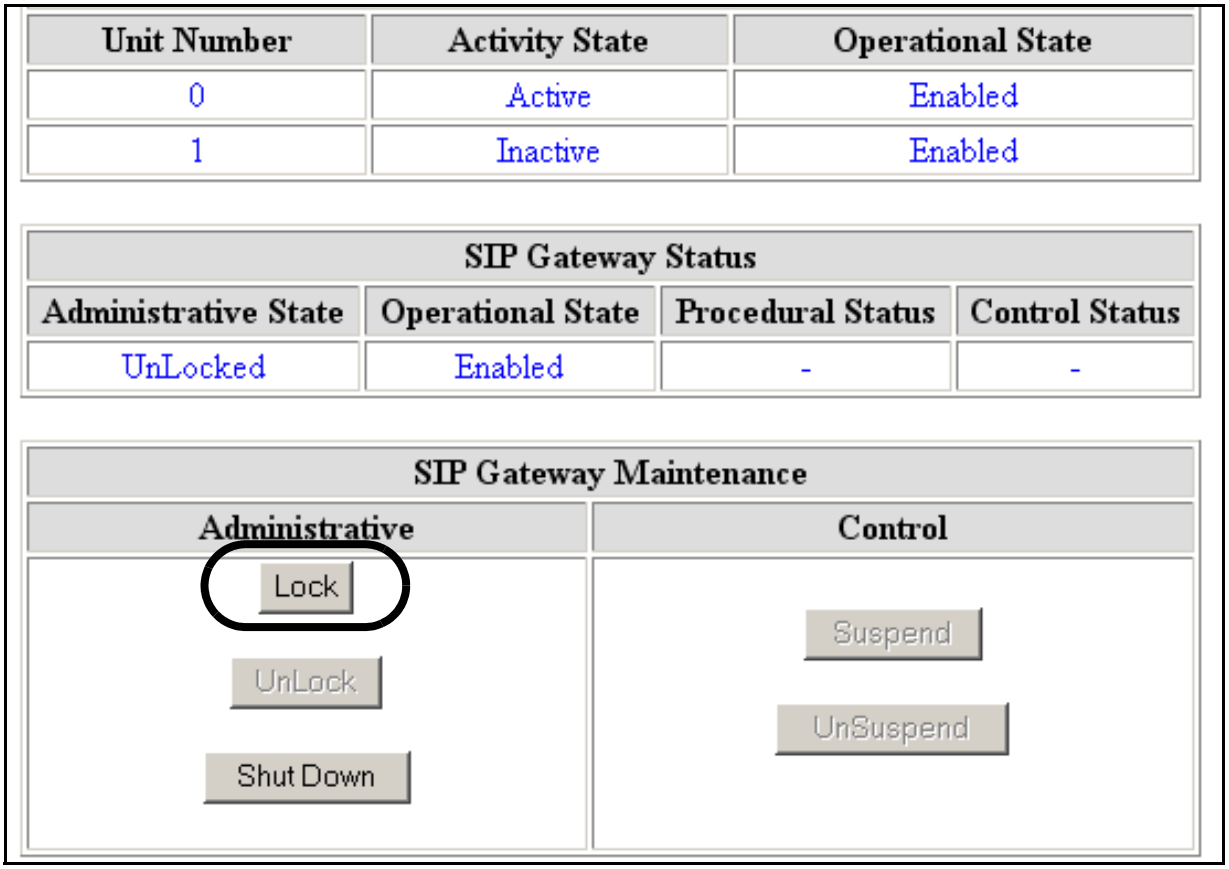
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.



2 Select **Session Server > Maintenance > Application > SIP Gateway**:



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

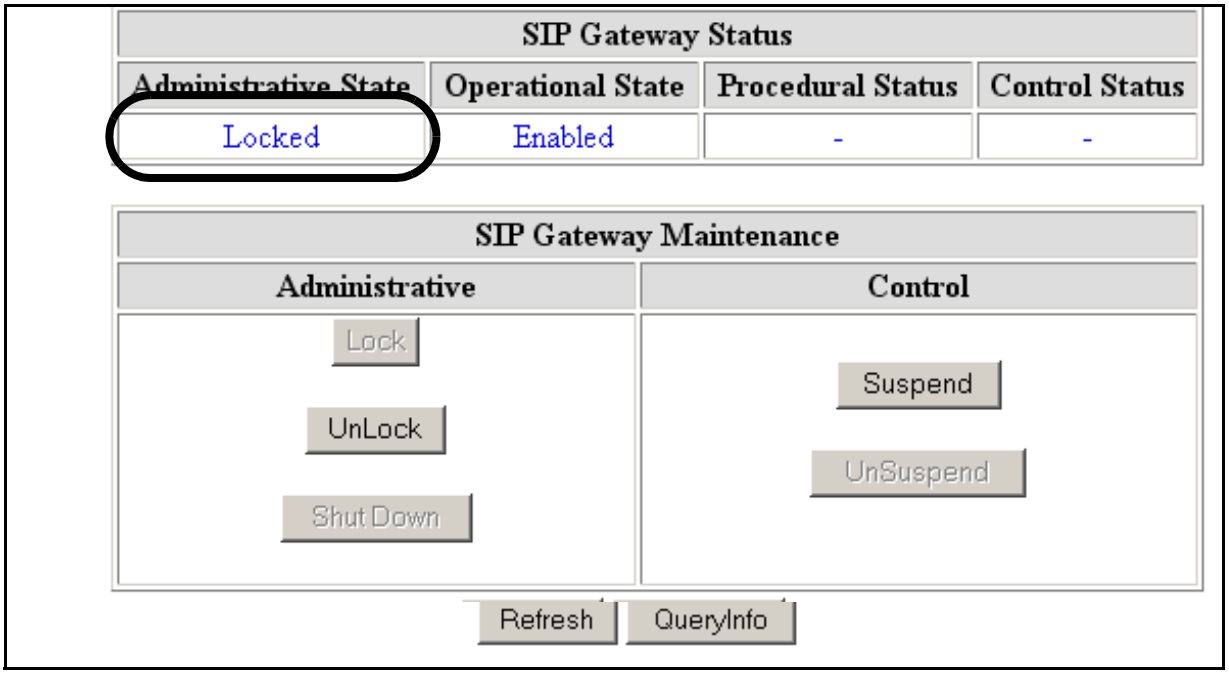


The system responds:

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

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

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



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

6 The procedure is complete.

Suspend the SIP Gateway application

Purpose of this procedure

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

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

Limitations and restrictions

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

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

Prerequisites

The SIP Gateway application must previously have been locked. If it is not locked or you are uncertain of the state of the application, refer to procedure Lock the SIP Gateway application on page 192.

Action

At the Session Server GUI or Integrated EMS client

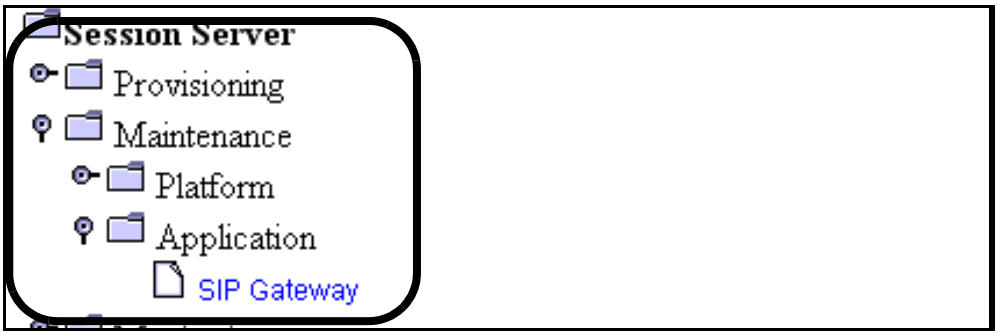
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

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

Please select one of the following management interfaces:

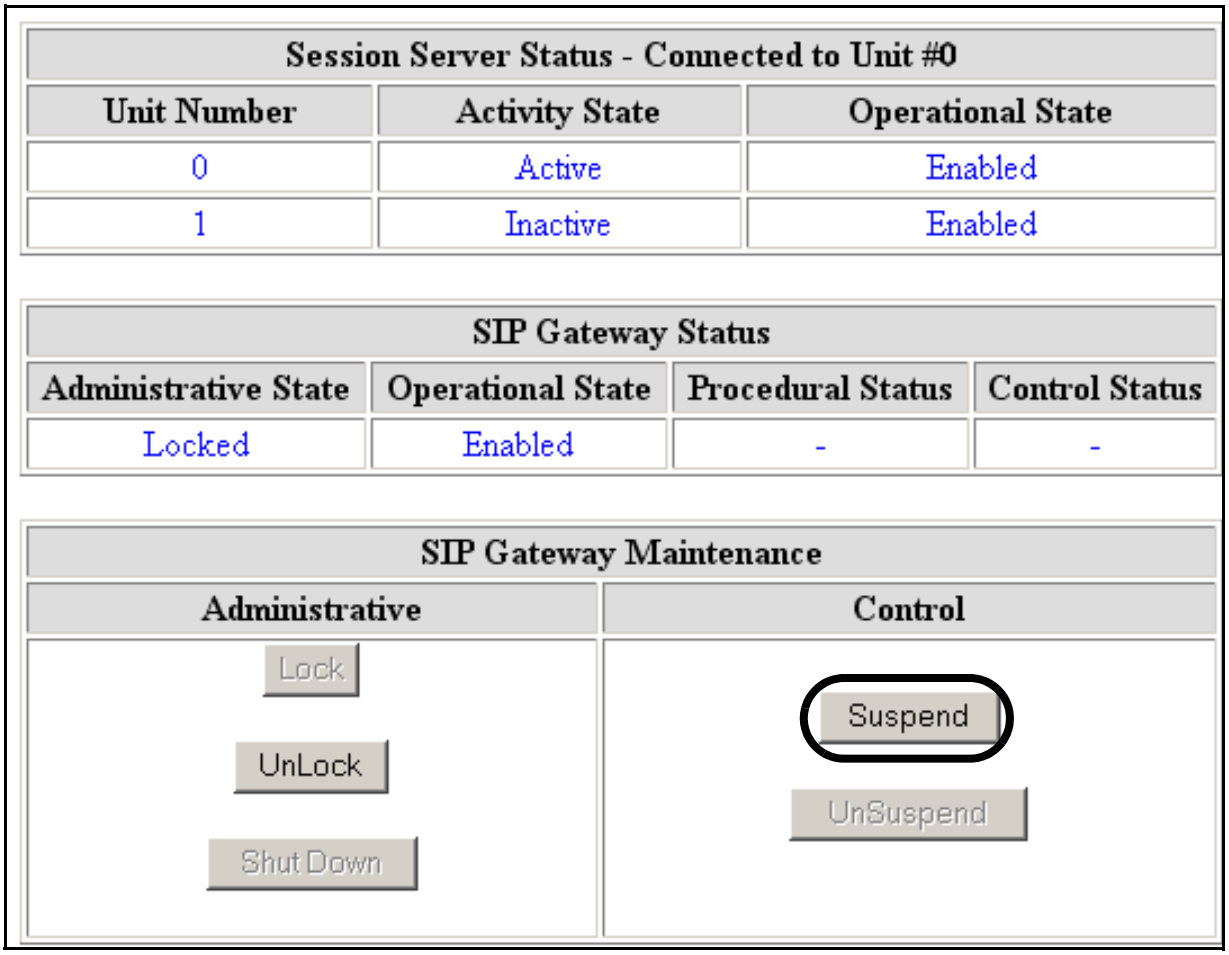
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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



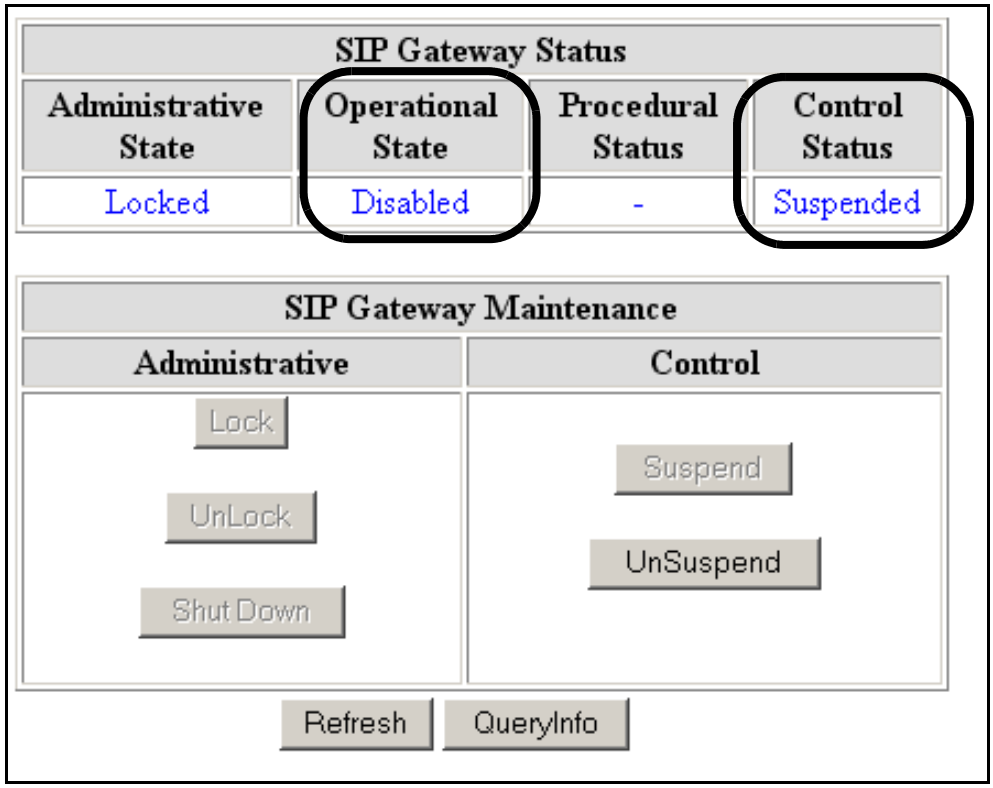
3 Click on the **SIP Gateway** folder to open it.

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



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

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



6 If applicable, restart the SIP Gateway application by executing procedures Unsuspend the SIP Gateway application on page 204 and Unlock the SIP Gateway application on page 208, in the order shown.

7 The procedure is complete.

View the operational status of the SIP Gateway application

Purpose of this procedure

Use the following procedure to view the service status of the SIP Gateway application. This procedure may be used as a standalone task or as part of a high-level activity.

Limitations and restrictions

This procedure provides instructions for determining the service status of the SIP Gateway application software only. For instructions on determining the status of the Session Server platform, refer to procedure View the operational status of a Session Server NCGL platform on page 119.

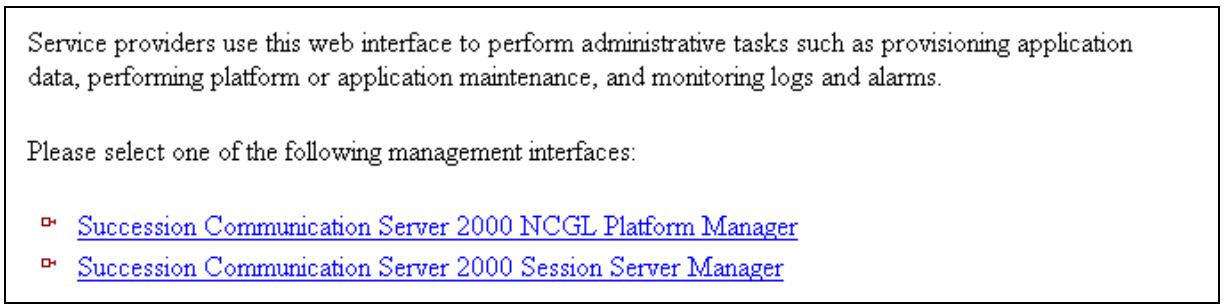
Prerequisites

There are no prerequisites for this procedure.

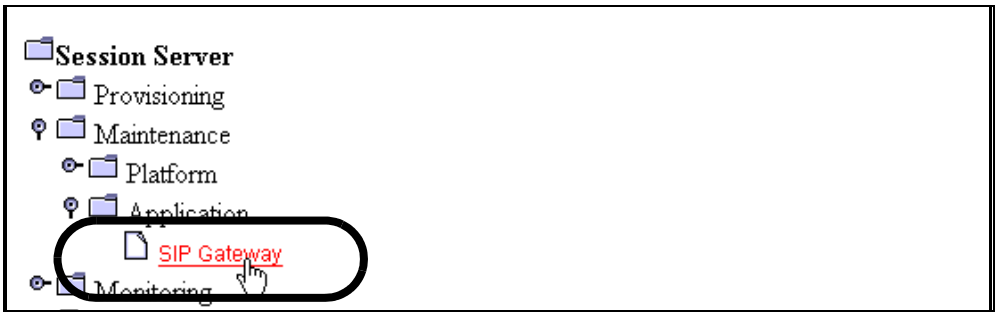
Action

At the Session Server GUI or Integrated EMS client

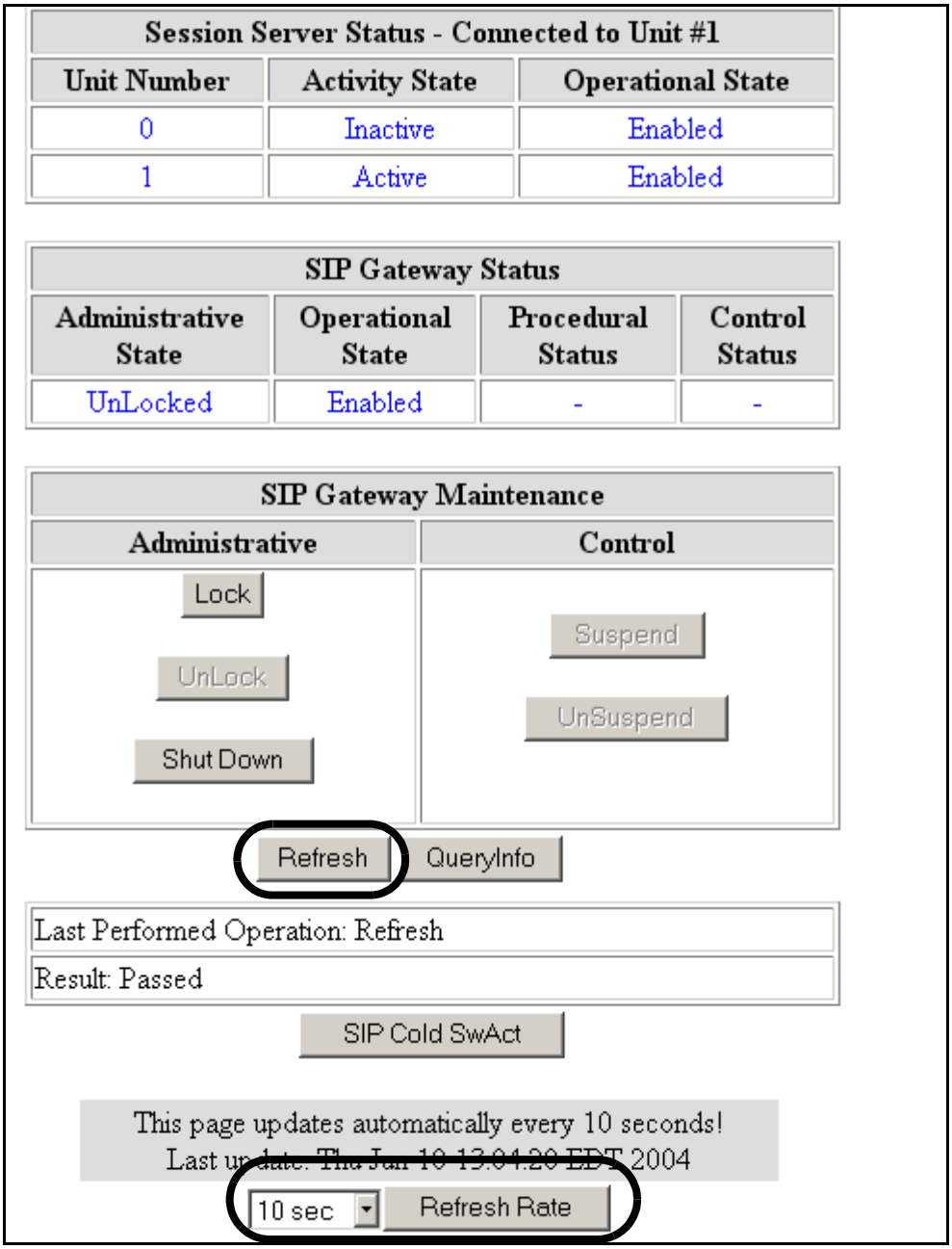
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.



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



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



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

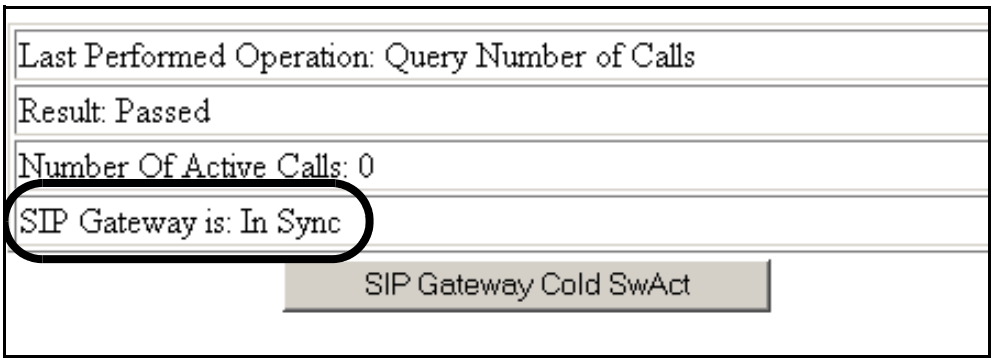
4 Refer to section Interpreting SIP Gateway application status and maintenance fields on page 201 to review the description of the various fields of this view.

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

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

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

6 To view the number of active calls currently being handled by the application and the sync status of the Session Server units, click the **QueryInfo** button.



7 The procedure is complete.

Interpreting SIP Gateway application status and maintenance fields

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

Session Server node status field descriptions

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

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

SIP Gateway application Status field descriptions

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

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

SIP Gateway Maintenance field descriptions and interpretation of service states

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

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

Unsuspend the SIP Gateway application

Purpose of this procedure

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

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

Limitations and restrictions

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

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

Prerequisites

The SIP Gateway application must previously have been suspended. If it is not suspended or you are uncertain of the state of the application, refer to procedure Suspend the SIP Gateway application on page 195.

Action

At the Session Server GUI or Integrated EMS client

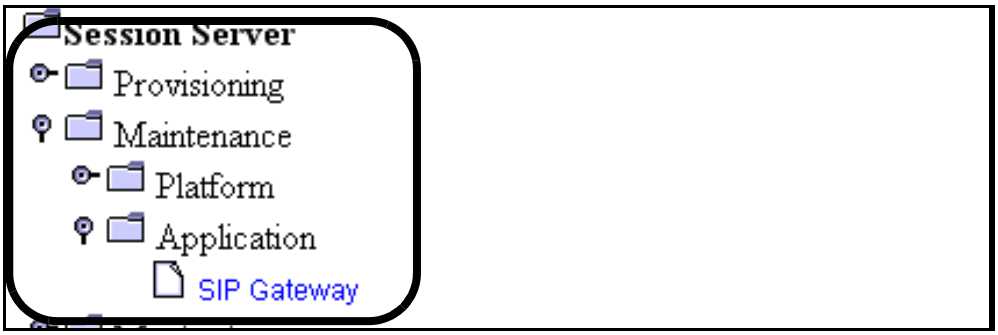
1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

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

Please select one of the following management interfaces:

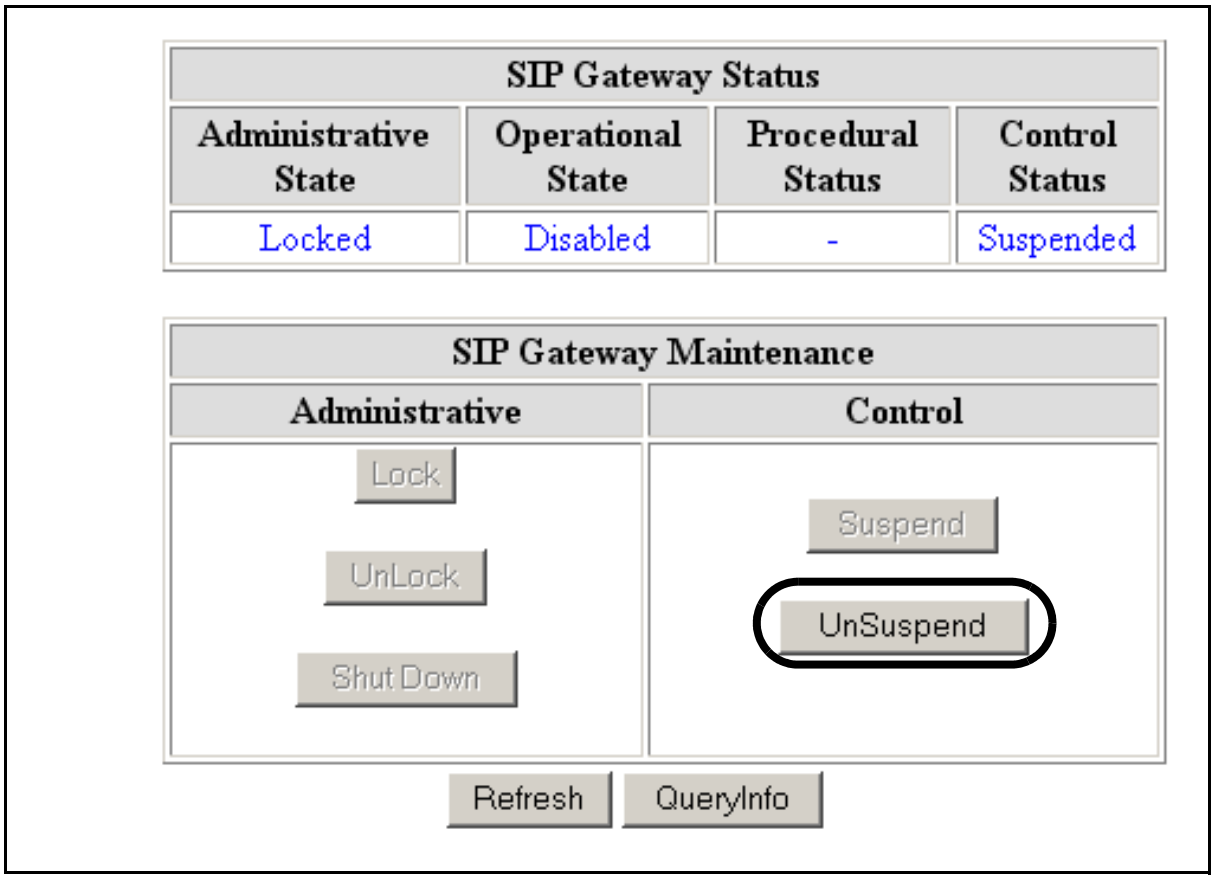
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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



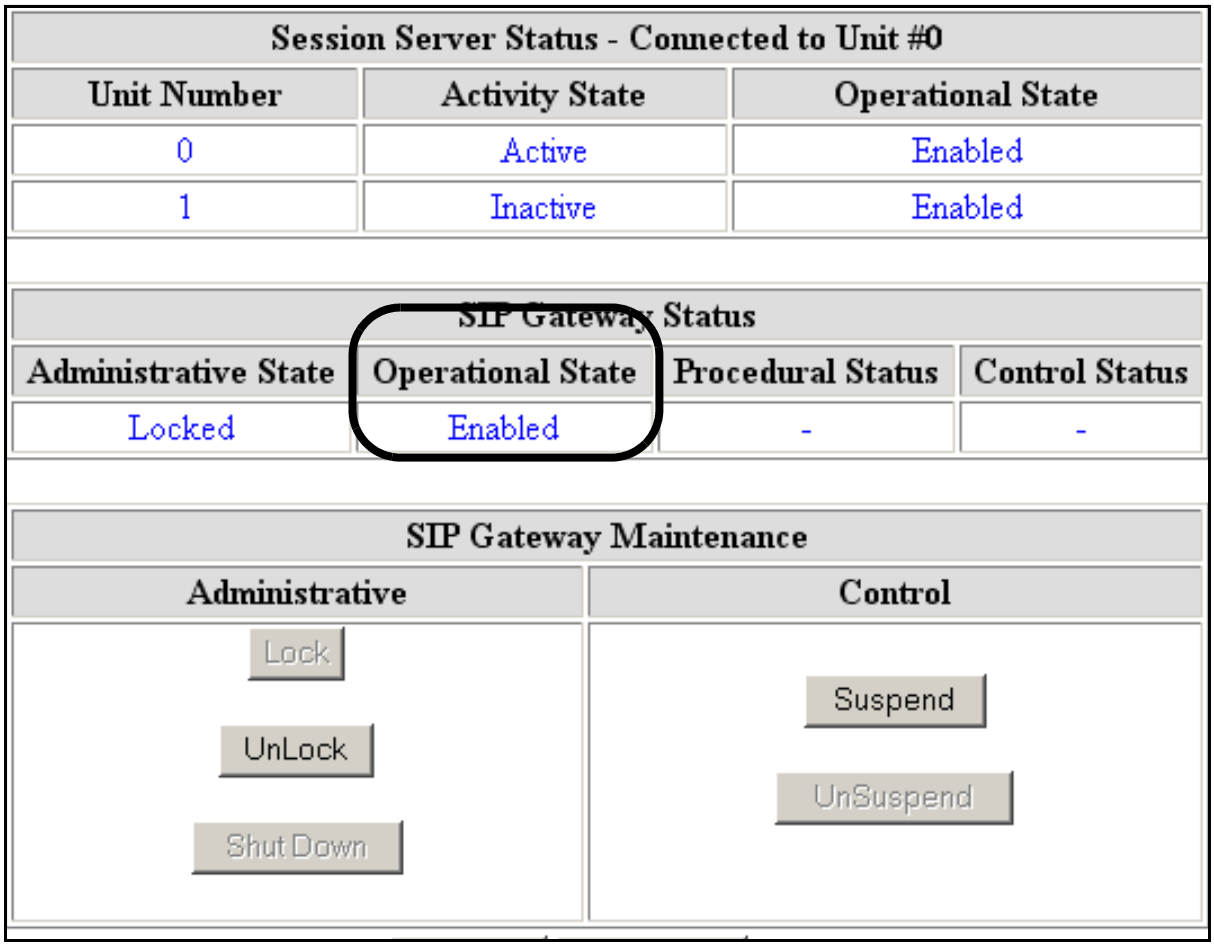
3 Click on the **SIP Gateway** folder to open it.

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



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

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



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

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

SIP Gateway Maintenance	
Administrative	Control
Lock UnLock Shut Down	Suspend UnSuspend

6 If necessary, bring the SIP Gateway application back into service by executing procedure Unlock the SIP Gateway application on page 208.

7 The procedure is complete.

Unlock the SIP Gateway application

Purpose of this procedure

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

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

Limitations and restrictions

This procedure provides instructions for changing the service status of the SIP Gateway application software only. For instructions on determining the status of the Session Server platform, refer to procedure View the operational status of a Session Server NCGL platform on page 119.

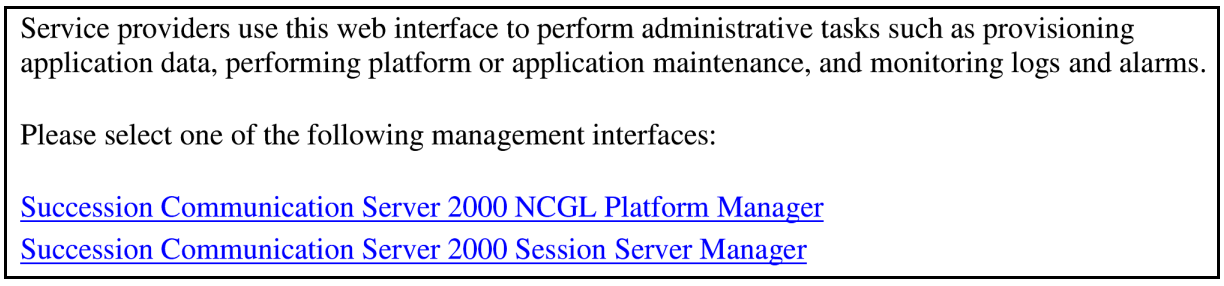
Prerequisites

The active Session Server unit must be in a locked Administrative state. If it is not locked or you are uncertain of the state of the application, refer to procedure Lock the SIP Gateway application on page 192.

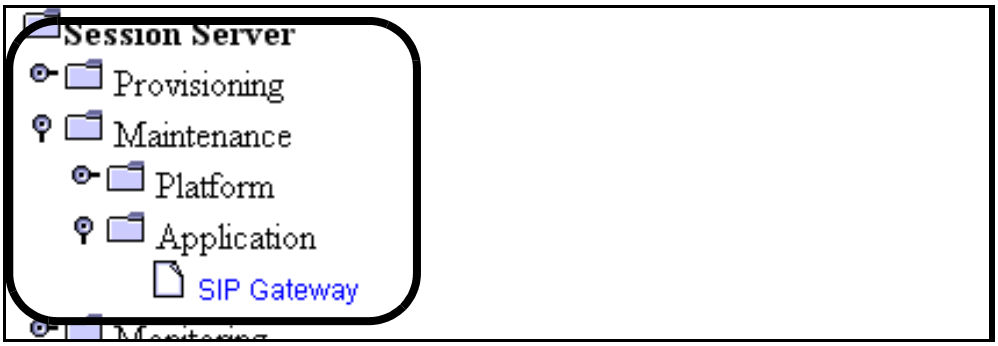
Action

At the Session Server GUI or Integrated EMS client

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

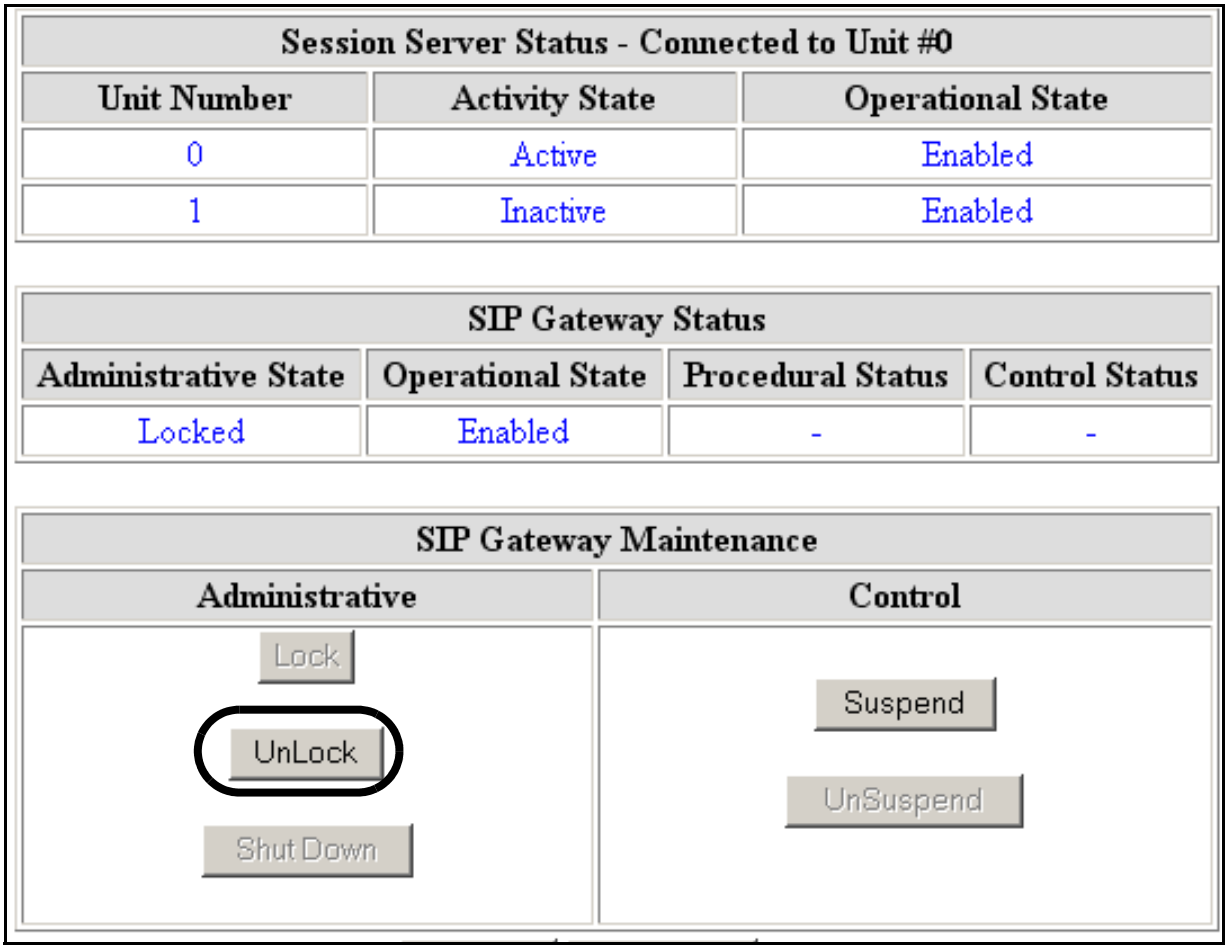


2 At the Session Server folder, click the **Maintenance folder,** then click the **Application** folder.



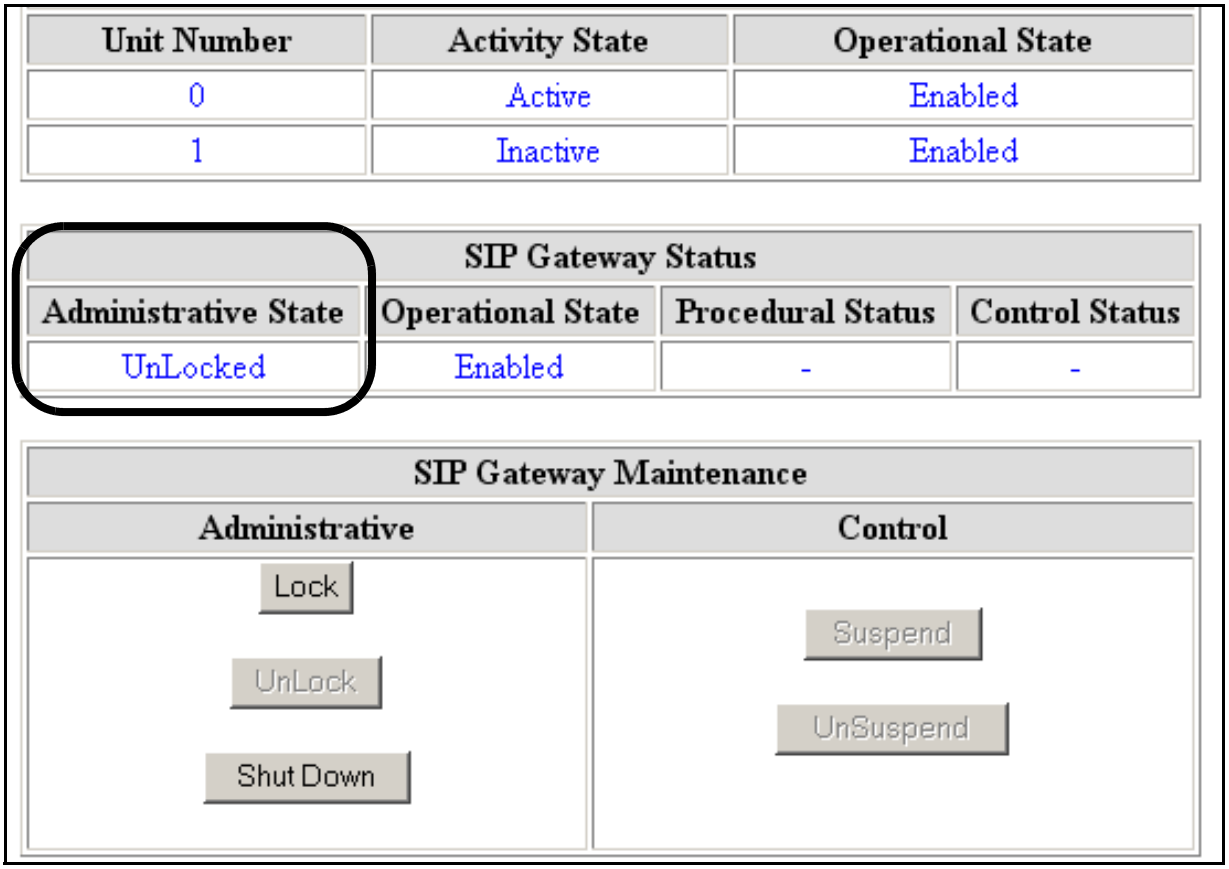
3 Click on the **SIP Gateway** folder to open it.

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



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

- the Administrative State changes to **Unlocked**



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

SIP Gateway Status

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

SIP Gateway Maintenance

Administrative	Control
Lock UnLock Shut Down	Suspend UnSuspend

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

6 The procedure is complete.

Prepare for a database restore on a Session Server unit

Purpose of this procedure

Use this procedure to prepare for a restoration of the SIP Gateway application database from a backup copy to the active unit.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of a high level upgrade activity, found in the Session Server Upgrades NTP, NN10349-461.

Limitations and Restrictions

CAUTION

Performing a restore of the SIP Gateway application database to the active unit is a service affecting activity and can cause data mismatches at the CS 2000 call server.

ATTENTION

For security reasons, you can only copy the database file from a remote server to the /users/mtc directory on the unit and you must use the secure copy command **scp** to perform this activity.

Automatic backup of the SIP Gateway application database occurs at 1:00 AM each day on both Session Server units. This configuration setting cannot be modified and does not impact the use of this procedure.

The name of the backup database file is *solid.db.* Do not modify this name.

Prerequisites

You must have secure copy (scp) access to the Session Server unit from the remote system or other server location from where the database backup file solid.db is copied.

Action

From the remote server where the backup database file is located

1 Log onto the remote server, locate and navigate to the directory where the backup copy of the database file is stored.

2 Secure copy the database file to the Session Server unit you are restoring a backup copy of the database to by typing

```
$ scp solid.db mtc@<SS_IP_address>:
```

and pressing the Enter key.

where

SS_IP_address
is the IP address of the Session Server unit

The database file is copied to the /users/mtc directory on the target Session Server unit. This is the only Session Server directory that files can be copied into from an external server.

At the Session Server CLI or Integrated EMS client

3 Log onto the Session Server unit you are restoring a backup copy of the database to, and change to the root user.

4 Move the solid.db file you copied in step 2 from the /users/mtc directory to the /opt/apps/database/solid/backup directory by typing

```
$ mv /users/mtc/solid.db
/opt/apps/database/solid/backup
```

and pressing the Enter key.

5 Change directory to the backup database directory by typing

```
$ cd /opt/apps/database/solid/backup
```

and pressing the Enter key.

6 Verify that the correct version (based on the file date) of the solid.db database file that you want to restore is located in the directory by typing

```
$ ls -l /opt/apps/database/solid/backup
```

and pressing the Enter key.

7 Verify that the presence of files *solid.ini* and *solmsg.out* files are also in the /opt/apps/database/solid/backup directory.

ATTENTION

The restorebackup.sh script does not run if you do not have the solid.ini and solmsg.out files located in the correct directory.

8 If the solid.ini file is not present, copy it into the backup directory by typing

```
$ cp /opt/apps/database/solid/dbfiles/solid.ini
/opt/apps/database/solid/backup/solid.ini
```

and pressing the Enter key

9 If the solmsg.out file is not present, copy it into the backup directory by typing

```
$ cp
/opt/apps/database/solid/dbfiles/solmsg.out
/opt/apps/database/solid/backup/solmsg.out
```

and pressing the Enter key

10 Change the ownership of all files in the backup directory by typing

```
$ chown soliddb *
```

and pressing the Enter key.

11 Change the group of all files in the backup directory by typing

```
$ chgrp adm *
```

and pressing the Enter key.

12 Change the access permissions for all files in the backup directory by typing

```
$ chmod 600 *
```

and pressing the Enter key.

13 The database is now ready to be restored. You have completed this procedure. Return to the high-level activity.

Additional information

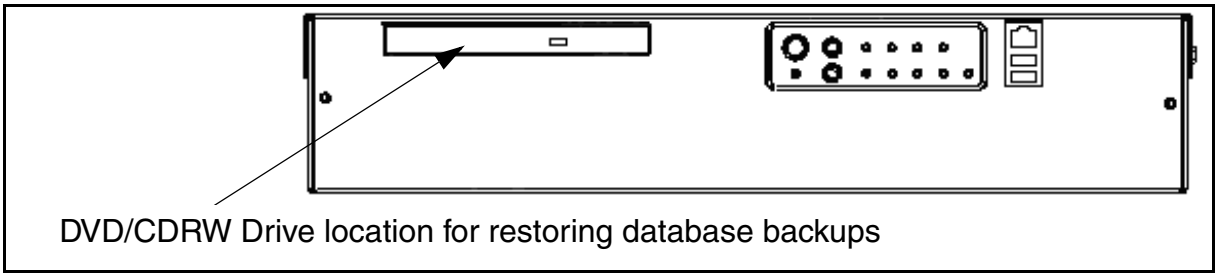
This section provides additional information regarding database restore activities.

To restore a backup database saved to a CD.

If you must restore a database backup that has been saved to a CD, you must first copy the database file from the CD to the default backup directory on the active Session Server unit. The selected backup database file must be restored to the following location:

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

To restore a backup of the database file to the backup directory, you must use a Session Server command line interface to copy the database file from a CD or CD-RW disk containing a copy of the back up database file to the opt/apps/database/solid/backup directory.



DVD/CDRW Drive location for restoring database backups

Ensure that you remove the CD disk from the DVD/CDRW drive, and store it in a safe place when you are done.

To restore a database backup saved to another system

If you must restore a database backup that has been saved to another system, you must first copy the database file from the remote system back to the default backup directory on the active Session Server unit. The selected backup database file must be restored to the following location:

/opt/apps/database/solid/backup

To restore a backup of the database to the backup directory you must use a Session Server command line interface to copy the database file solid.db from the remote system to the opt/apps/database/solid/backup directory. You may also be able to remote copy the backup database file from the remote system to the Session Server opt/apps/database/solid/backup directory. However, for security reasons, you may need to consult your site network administrator for instructions and permission to perform a remote copy.

Perform a database restore to a Session Server unit

Purpose of this procedure

Use this service impacting procedure to restore a SIP Gateway application database from a backup copy to the active Session Server units.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of a high level upgrade activity, found in the Session Server Upgrades NTP, NN10349-461.

Limitations and Restrictions

CAUTION

This procedure can only be executed on the active unit. Performing a restore of the SIP Gateway application database to the active unit is service affecting, and can cause data mismatches at the CS 2000 call server.

Prerequisites

You must first have completed procedure Prepare for a database restore on a Session Server unit on page 212.

Action

At the Session Server CLI or Integrated EMS client

1. Log onto the active Session Server unit you are restoring a backup copy of the database to, and change to the root user.
2. Change directories by typing

   ```
   $ cd /opt/apps/database/solid_install
   ```

   and pressing the Enter key.
3. Run the database restore script by typing

   ```
   $ ./restorebackup.sh
   ```

   and pressing the Enter key.
4. You have completed this procedure. Return to the high-level activity.

Editing and viewing object properties using Java Web Client

Application

Use this procedure to edit or view the properties of objects that are displayed in the IEMS topology using Java Web Client.

Prerequisites

None

Action

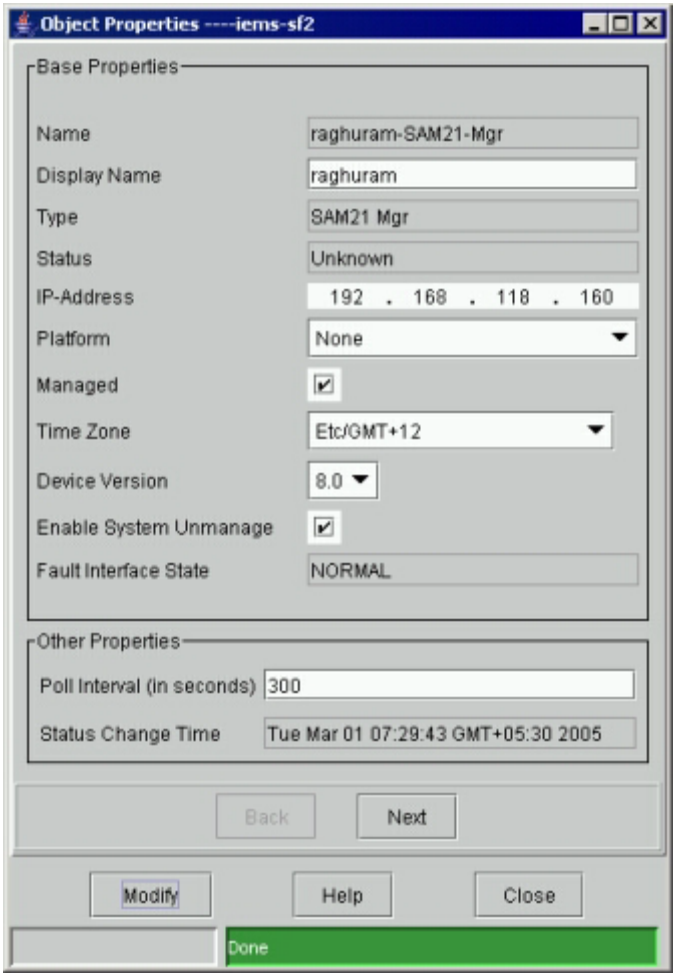
At the IEMS workstation

1. Launch the IEMS Java Web Start Client. Refer to Launching IEMS Java Web Start Client in *Integrated EMS Basics*, NN10329-111.
2. Select the required object in the Integrated EMS Topologies tree under Applications.

   Note: The properties of an object from the Inventory panel of Integrated EMS tree can also be viewed. To view the Inventory object properties, select the object in the Integrated Topologies tree under Applications to open the Inventory view. Double-click the required row in the Inventory view.
3. Right-click the map symbol and select the **Managed Object Properties** menu item or double-click the map symbol to open the Object Properties window.

   Note: The object properties displayed can differ for each component.

   A window similar to the following figure opens.



4 Modify the object properties listed in the table below if required.

Managed object properties in Java Web Client

Field	Description
Name	Displays a unique name for the object
Display Name	Edit the name displayed in the topology for the object
Type	Displays the type of object (element manager, EMS, EMS platform or NE)
Status	Displays the status of the object
IP-Address	Edit the IP address of the object

Managed object properties in Java Web Client

Field	Description
Platform	Select the platform where the object resides from the drop-down list
Managed	Indicates whether the object is managed or unmanaged
Time Zone	Select the time zone of the geographical location where the object exists from the drop-down list
Device Version	Select the device version of the managed object from the drop-down list
Enable System Unmanage	Enable or disable the System_Unmanaged state. Refer to the System_Unmanaged state section of Configuring the Message Overload Controller parameters in *Integrated EMS Fault Management*, NN10334-911.
Poll Interval	Edit the Poll Interval for status updates
Status Change Time	Displays the last status change time of the object
Note: For the following objects, only the Display Name and the Managed field can be modified. • SDM platform, APS EMS application, CS 2000 Core, Call Agent Core, IMX/CSE MX, Media Proxy, Media Gateway 7480/15000, MSS 15000	

5 Select your next step.

If	Do
you do not want to modify any other properties	go to step 6
you want to view or modify the fault interface or performance interface properties	go to step 8

6 Click the **Modify** button to update the changes.

7 Go to step 16.

8 Click the **Next** button to proceed to the Fault Interface window.

A window similar to the following figure opens.

9 Edit or view the fault interface properties of the object as required.

Note: The Details panel dynamically changes according to the fault interface of the EMS/NE.

10 Select your next step.

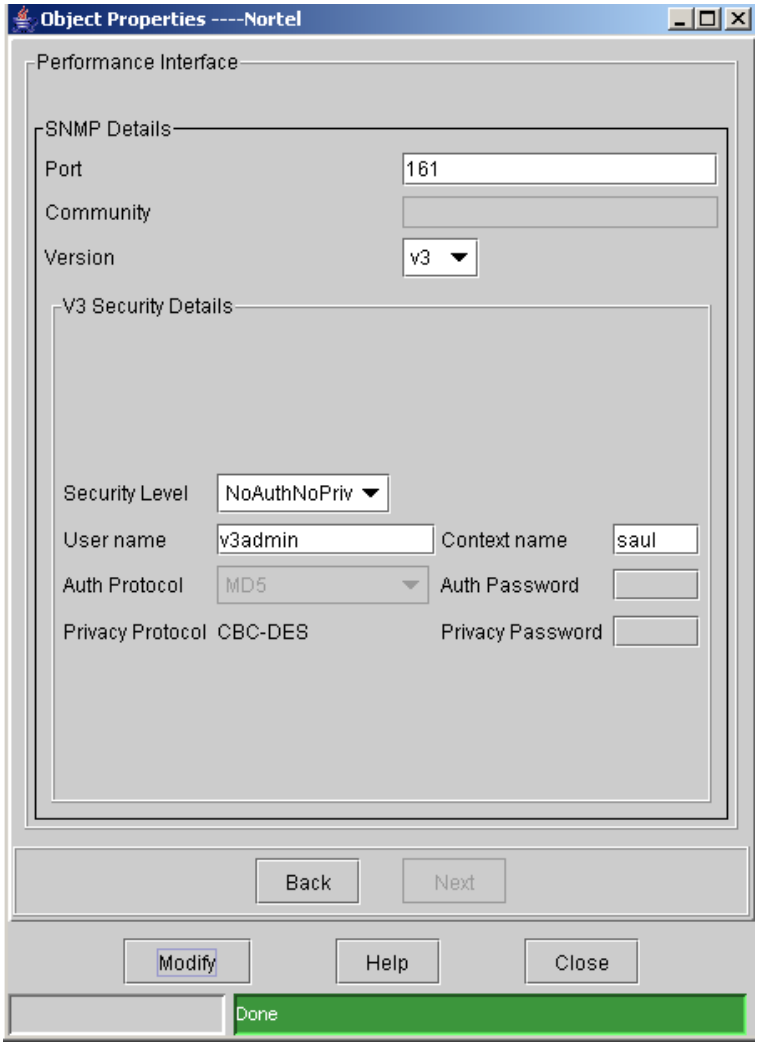
If	Do
you do not want to modify any other properties	step 11
you want to view or modify the performance interface properties	step 13

11 Click the **Modify** button to update the changes.

12 Go to step 16.

13 Click the **Next** button to proceed to the Performance Interface window.

A window similar to the following figure opens.



14 Edit or view the performance interface properties of the object as required.

15 Click the **Modify** button to update the changes.

16 You have completed this procedure.

Editing and viewing object properties using Web Client

Application

Use this procedure to modify or view the properties of an object in the IEMS topology using Web Client.

Prerequisites

None

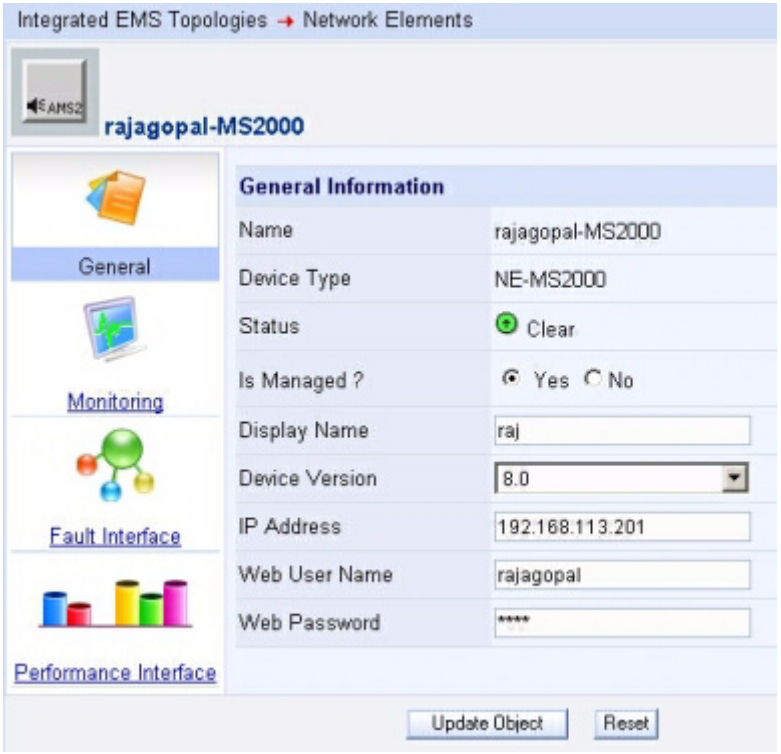
Action

At the IEMS workstation

1. Launch the IEMS Web Client. Refer to Launching the IEMS Web Client in *IEMS Basics*, NN10329-111.
2. Select the **Integrated EMS Topologies** tab.
3. Navigate to the required topology node in the Integrated EMS Topologies tree.
4. Click the map symbol label to open the **General Information** window.

   Note: The object properties displayed can differ for each component.

   A window similar to the following figure opens.



5 Select each vertical tab and modify the object properties listed in the table below if required.

Managed object properties in Web Client

Field	Description
General	
Name	Displays the unique object name of the managed object
Device Type	Displays the type of object (element manager, EMS, EMS platform or NE)
Status	Displays the status of the object
Is Managed?	Indicates whether the object is managed or unmanaged
Display Name	Displays the name or label displayed in map symbol
Device Version	Select the version of the device from the drop-down list

Managed object properties in Web Client

Field	Description
IP Address	Modify the IP address of the object
Web User name	Enter your web user name
Web Password	Enter your web password
Monitoring	
Last Status Update Time	Displays the time when the status of the managed object last changed
Last Status Change Time	Displays the time when the status of the managed object last changed
Status Polling Interval (secs)	Modify the Poll Interval for status updates

Managed object properties in Web Client

Field	Description
Fault Interface	
If the details are present for the selected object, the details can be modified.	
Performance Interface	
If the details are present for the selected object, the details can be modified.	

6 Click the **Update Object** button to update the changes.

7 You have completed this procedure.