Carrier VoIP

Session Server Trunks Fault Management

NN10332-911

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

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

Contents

New in this Release

The following sections list what's new in SST fault management in (I)SN09U.

Features

Session Server Fault Handling Enhancements (A00012735)

This activity extends the coverage of hardware faults handled by the Session Server NCGL Platform Manager software and thus increases the reliability of the Session Server platform. This activity involves the detection and reporting of hardware faults in the following areas:

- Power Supplies
- Fan Speeds
- System Temperature
- System Voltage
- Miscellaneous Hardware Elements

For more information, refer to the following log report topics in *Carrier Voice over IP Fault Management Logs Reference* (NN10249-911):

- XTS382
- XTS383
- XTS682
- XTS683

Other changes

The task flow diagrams "SST fault management task flow" (page 9) and "Dead office recovery task flow" (page 30) are replaced.

The procedure "Viewing SIP Gateway application log files" (page 38) has been added to enable users to view a variety of log files related to the SIP gateway application.

A description of new SST alarms introduced in the SN09U release has been added in Appendix "New SST alarms for SN09U release" (page 95).

Fault management overview

The Session Server Trunks (SST) uses self-testing, automated diagnostics and log reporting systems to support maintenance activities and to manage faults. These systems raise alarms and generate logs when the following types of hardware or software events occur:

- fault or failure conditions
- correction or resolution of fault or failure conditions
- when a preset operating performance or resource capacity threshold is crossed or exceeded
- a condition occurs that is transient or cannot be repaired.

Fault management for the SST platform encompasses:

- setting up resource thresholds such as monitoring disk usage
- activating monitoring of specified resources such as disk drives or file systems
- monitoring alarms at the CS 2000 Server NCGL Platform Manager or CS 2000 Session Server Manager GUIs
- reviewing log reports using the CS 2000 Server NCGL Platform Manager or CS 2000 Session Server Manager GUIs or the NGCL CLI (command line interface)

Because SST can be configured to transfer log reports to the OSS network, the log reports may be available to IEMS or other third-party OSS applications. Otherwise, they are available on the disk drives of either unit.

Fault clearing is dependent on the timely resolution of alarm conditions. Alarms cannot be manually cleared without first removing the alarm condition.

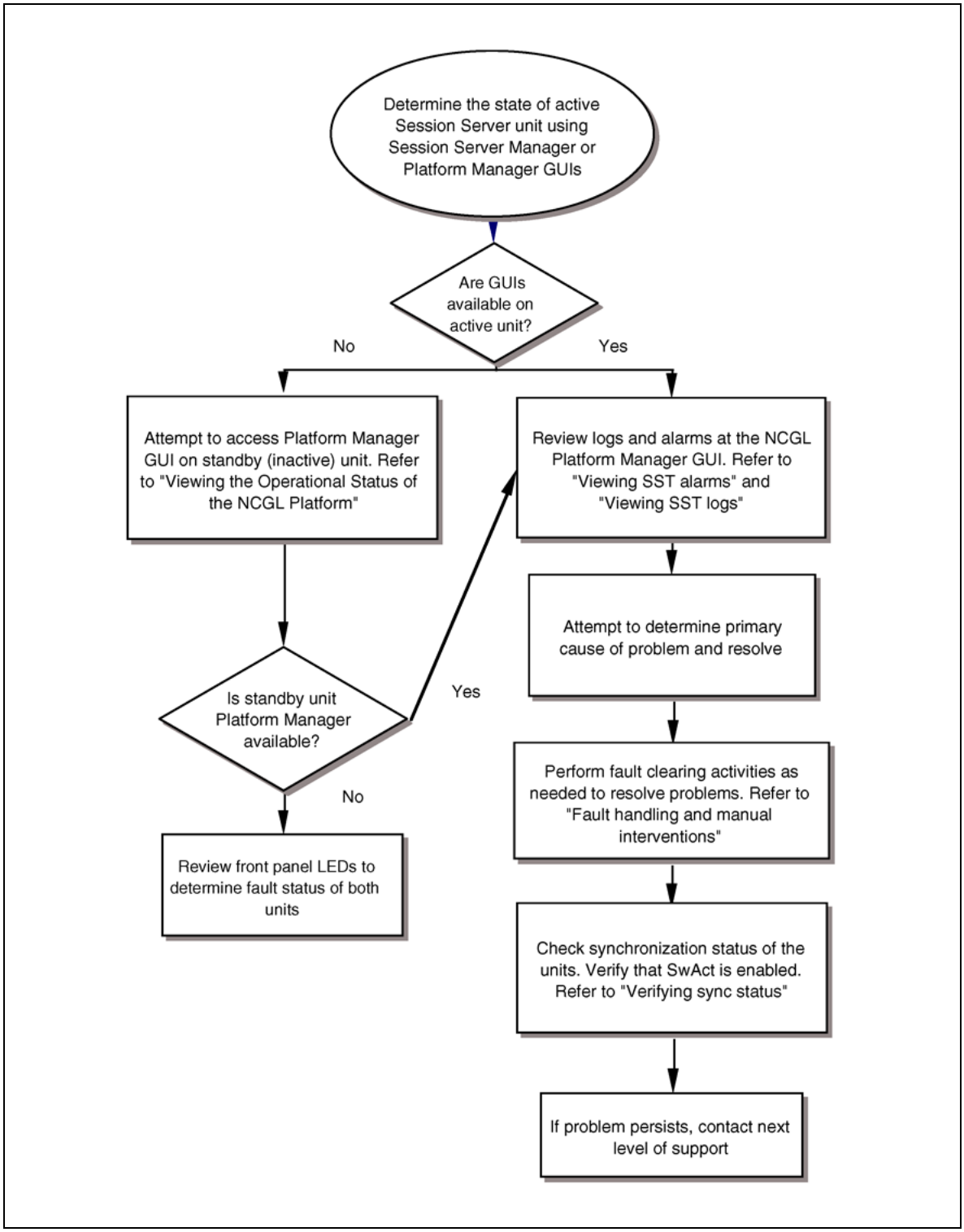
Some hardware faults may require part replacement. This NTP provides instructions for replacing an entire SST unit (the standby unit only). For instructions on replacing individual field replaceable units (FRUs) that make

up an SST unit, refer to the HP Carrier-Grade Server cc3310 Product Guide, HP part number: cc3310_Product, available either from your vendor or from the Hewlett-Packard web site.

Fault handling and correction on the SST node

The following flowchart shows the overall process for performing fault handling on the SST platform.

SST fault management task flow



Fault handling and manual interventions

The following table provides a summary of the fault handling behavior in response to various fault conditions. In some cases, fault management behavior is automatically initiated by the system node maintenance. In most cases, other actions must be performed by service personnel. In all cases, refer to the customer logs for more detailed information and a history about the fault event.

Fault Event	Action
Total Loss of LAN Connectivity on the active unit when both units are operational	System SwActs to the inactive unit. Reset former active unit if the condition persists. After LAN connectivity is restored and reset completes, verify that the inactive unit comes back into sync with the active unit.
Total Loss of LAN Connectivity on the active unit with no standby unit available	Wait about two minutes and reset the active unit. (The wait time accommodates SDM/CBM and router upgrade outages.)
Total Loss of LAN Connectivity for both units	Wait about two minutes and reboot the active unit; wait 60 seconds and reboot inactive unit.
Single Ethernet link Outage on one or both units	If necessary the system automatically switches the active Ethernet link. Monitor for Ethernet recovery by viewing alarms and logs.
Loss of Point to Point Connectivity between units when both units are operational	Consult alarms and logs views on the active unit to determine the fault details. System automatically continues to communicate with mate unit using the LAN connections.
Platform Time Out or Power Cycle on an active unit when both units are operational	System SwActs and the inactive immediately takes over; former active reboots.
Platform Time Out or Power Cycle on an inactive unit	The inactive unit reboots automatically.
Platform Time Out or Power Cycle when only the a single unit is available and active	The single, active unit reboots and determines mastership.
Total Disk Outage on active unit when both units are operational	The system automatically SwActs over to the inactive unit. Consult alarms and logs views on the newly active unit to acquire fault details and to determine action. Consider replacing drives on affected unit.
Total Disk Outage on active unit with no standby unit operational	Consult alarms and logs views for fault details. Contact next level of support.
Total Disk Outage on inactive unit both units are operational	Consult alarms and logs views in the GUIs on the active unit to determine fault details. First reboot inactive unit as an attempt to clear the fault, then replace faulty drive(s) on inactive unit.

Troubleshooting SIP-T trunk group link status on the CS 2000

In the CS 2000, the association of a trunk group to an access link is defined in table SIPLINK. The status of an access link can be monitored by posting the associated SIP-T trunk group at the MAPCI;MTC;TRKS;DPTRKS level of the MAP. The CS 2000 receives link status information from the SIP-T GWCs (gateway controllers), that receive access link status messages from the SST and pass them on to the CS 2000.

The status of the access link on the SST is determined using a link auditing mechanism. Any change in link status is immediately propagated to each SIP-T GWC, then to the CS 2000. As long as there is stable communication between the CS 2000, at least one SIP-T GWC, and the SST, the status of a SIP-T trunk in the CS 2000 should mirror that of its associated access link.

For a trunk to be In-service (INSV) at the DPTRKS MAP level, all of the following conditions must exist:

- On the SST, the access link associated with the trunk must be mapped to a Remote SIP Server.
- On the SST, the associated Remote SIP Server must have at least one active IP connection. During a link audit, an active connection is defined as one of the following:
  - For a Remote SIP Server configured to support SIP OPTIONS messaging for heartbeats, a connection is active if the SST is receiving timely 200 OK responses to its SIP OPTIONS requests on at least one of the IP connections to the remote server.
  - For a Remote SIP Server that doesn't support OPTIONS for heartbeats, a connection is active if the SST is successfully sending and/or receiving SIP messages at a level above the failed message threshold on at least one of the IP connections to the remote server. By default the connection is considered active until indicated otherwise by exceeding the failed message threshold during call processing.
- The SST application administrative state must be UNLOCKED.
- On the CS 2000, at least one SIP-T GWC must be shown to be in-service at the MAPCI;MTC;TRKS;DPTTRM level of the MAP.

When all of these conditions are met, the SST sends an access link status message indicating the link is up to each SIP-T GWC. The SIP-T GWCs then propagate the message to the CS 2000, resulting in the state of the trunk group changing to In-service.

Once a trunk group is in-service, a failure of any of the first three conditions causes the SST to send an Access Link Status message indicating the link is down to each SIP-T GWC. The GWCs then propagate the message to the CS 2000 and the CS 2000 changes the trunk group status to SYS.

If a situation occurs where there are no longer any in-service SIP-T GWCs, the CS 2000 changes the state of the trunk group to SYS. This is the only time the CS 2000 undertakes unsolicited action to remove a link from service; otherwise, link status in the CS 2000 is completely under the control of the SST. In other words, when at least one SIP-T GWC is in-service at the DPTTRM level, the only way an associated trunk group's state can be changed (other than by manual intervention) is if the SST sends an access link status message to report the state change.

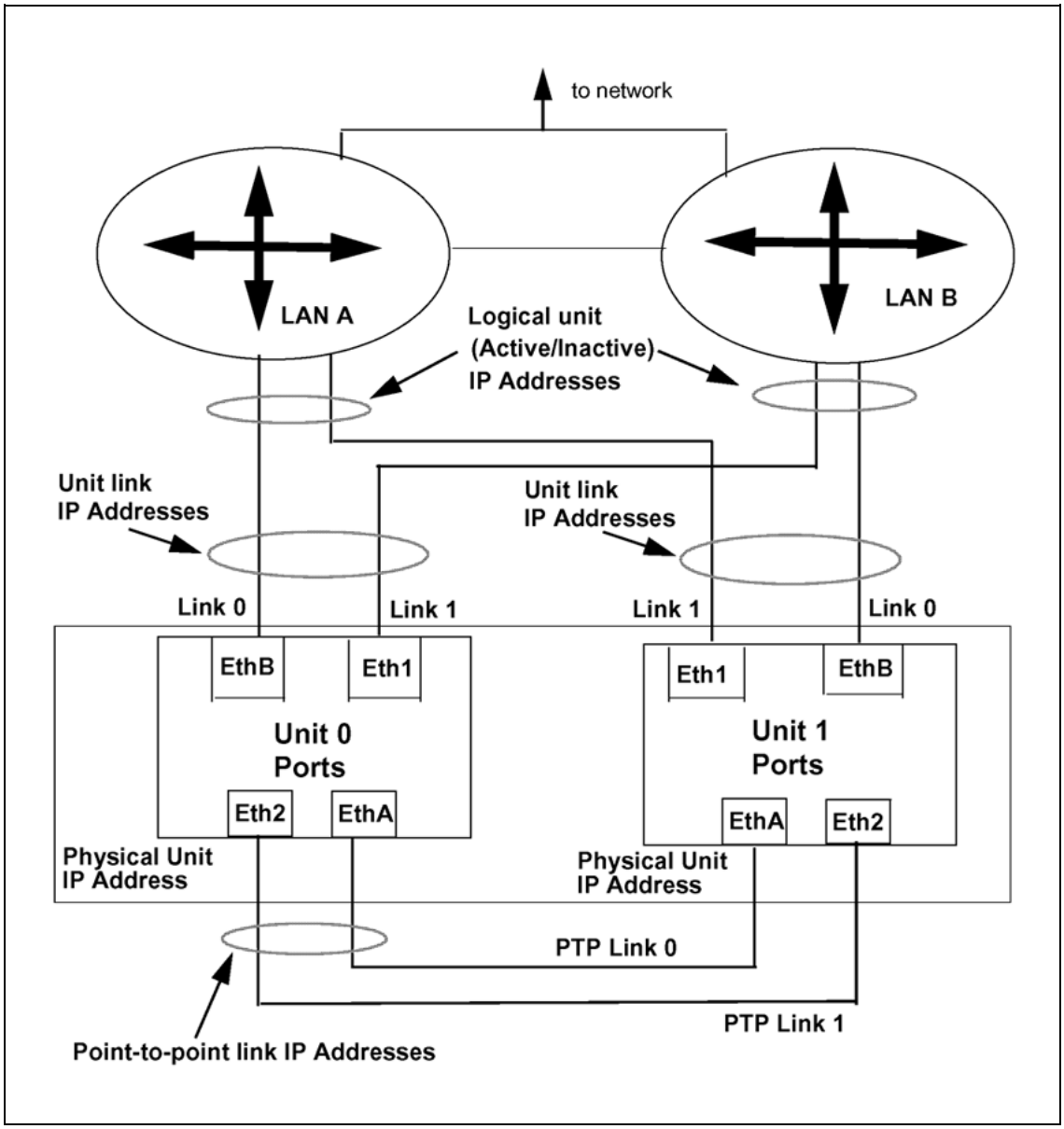
If the SST goes out of service due to a system failure or because of improper shutdown (which would disrupt the ability to send the access link status message to the SIP-T GWCs), all in-service SIP-T trunks associated with any access links on the SST remain in-service.

Troubleshooting point-to-point Ethernet links

Use the following section to help in troubleshooting problems with the point-to-point (PTP) links on each SST unit. PTP links are used as communication links between SST units to maintain fault tolerant redundancy. Do not confuse the PTP links with the other links connecting each SST unit with the central office LAN.

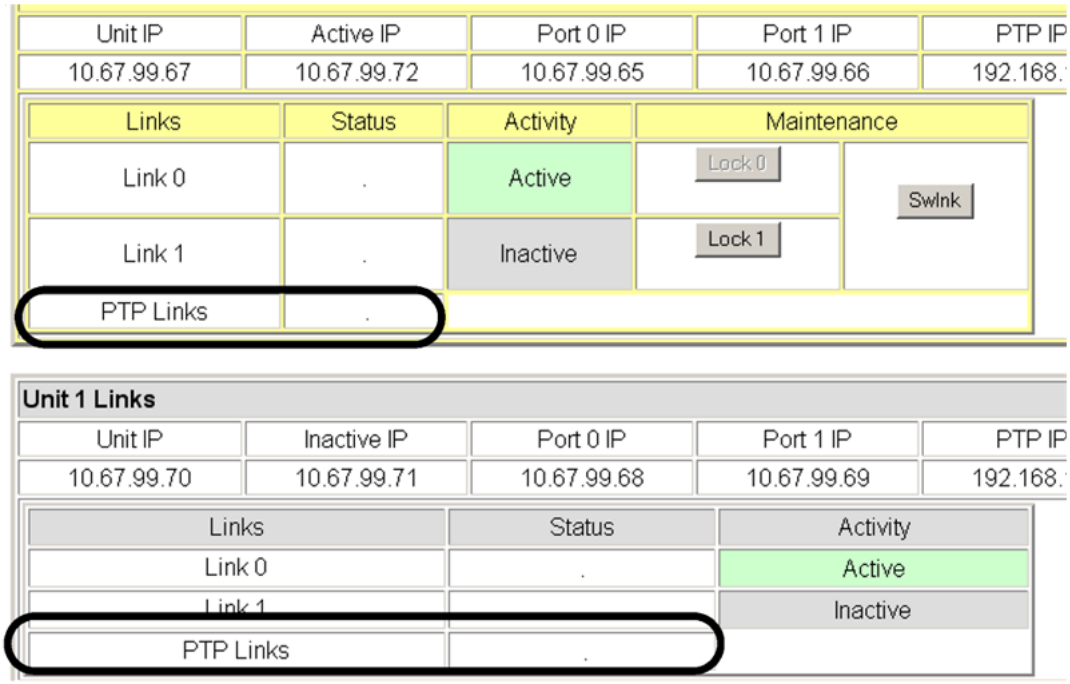
The following figure shows all port and link connections for both units. Port ethB of each unit is connected directly to a LAN switch, while port eth1 is connected to the redundant LAN switch. Ports ethA and eth2, used for the PTP links on each unit are cross-connected to the mate ports on the mate units.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

Physical map of SST Ethernet links and ports



If a single PTP link goes down, an alarm is raised and an XTS335 log generated; however, from the Network Connectivity page the status of the PTP links continues to be marked as "." which means that the links are in service. The PTP status field on the Network connectivity page only show that there is a problem if both PTP links go down, as would be the case if an entire unit is taken out of service. The following figure indicates the location of the status indicator for the PTP links on each unit.

Locating PTP link status on the Network Connectivity page



The following is an example of the alarm that is generated when a single PTP link goes down. The section of the alarm message in bold highlights the key difference from the alarm message raised when both PTP links are down:

```
Communications Communications Subsystem Failure  Thursday
July 22nd 2004 09:43:04 AM cablab.ss.unit1  Major Link0:
INSV, mateCon: AVAIL, netCon: AVAIL;  Link1: INSV, mateCon:
AVAIL, netCon: AVAIL; PTPLink:  PTP0-SYSB, mateCon: AVAIL;
```

The following is an example of the alarm that is generated when both PTP links go down. The section of the alarm message in bold highlights the key difference from the alarm message raised when a single PTP link is down:

```
Communications Communications Subsystem Failure  Thursday
July 22nd 2004 10:32:34 AM cablab.ss.unit1  Major Link0:
INSV, mateCon: AVAIL, netCon: AVAIL;  Link1: INSV, mateCon:
AVAIL, netCon: AVAIL; PTPLink:  BOTH_SYSB, mateCon: UNAVAIL;
```

Fault management tools and utilities

Fault management for the SST is provided by the following interfaces:

- CS 2000 NCGL Platform Manager
- CS 2000 Session Server Manager
- Session Server platform CLI (command line interface) or console

In most cases, these interfaces are accessed using the IEMS application, however, some cases may require you to access them directly from a console connection directly connected to one of the SST units.

Monitoring and analyzing alarms

Alarms can be viewed on the CS 2000 Session Server Manager alarm page. The alarms view sorts alarms by severity, most severe first, then by time, oldest first.

View of the CS 2000 Session Server Manager alarms page

Unit	Activity	Jam	State	Connectivity	Host Name	Last Update Time
1	Active	no	. 1C+	.	sp2k-2	01:41:40

The Alarms panel updates every 45 seconds
Datestamp of last update: Friday April 30th 2004 01:41:23 PM EST

Type	ID	Timestamp	Host	Severity	Description
Communications	Out of Service	Friday April 30th 2004 01:36:25 PM	sp2k-1	Critical	SIP Gateway Application System Busy
Communications	Application Subsystem Failure	Friday April 30th 2004 01:36:31 PM	sp2k-2	Major	SIP Gateway Application Mtc Out Of Sync
Communications	Application Subsystem Failure	Friday April 30th 2004 01:36:24 PM	sp2k-1	Major	SIP Gateway Application Mtc Out Of Sync

Alarms can also be viewed using the IEMS Alarm Manager view. Although the alarm information is organized and presented differently in the IEMS Alarm Manager, the same data is made available. For information about viewing alarms, refer to *IEMS Fault Management* (NN10334-911).

Alarms provide notification that an event has occurred that requires attention. Alarms are generated when problems or conditions are detected that can change the performance or operating state of a node and its connectivity with the network. Administration of the network elements requires monitoring for alarms and checking that functions continue without interruption.

SST has the capability to generate alarms to report faults for the following conditions:

- network connectivity
- maintenance action failure
- mate communication

- disk usage
- memory usage
- disk mirroring failures

Alarms are formatted and displayed as defined in CCITT X.733 (Systems management: Alarm reporting function) as follows: the alarm type, alarm ID, timestamp, hostname, level of severity and a description of the alarm condition. The alarms that are raised at this panel are the ones currently active on the system. The alarms view updates in real time (it displays alarms as soon as they are raised, and removes them from the display as soon as they are cleared). The alarm page updates every 45 seconds and the user also has the option of invoking a re-query of alarms.

Alarms also provide notification of problems or conditions that can change the performance or working state of the SST, associated GWCs, gateways or other related network components.

Alarm types

There are 5 CCITT X.733 alarm types used by the SST which specify the alarm category for a give alarm. Valid alarm types are:

Type	Alarm Type
	No alarm
1	Communications alarm
2	Quality of service (QoS) alarm
3	Processing error alarm
4	Equipment alarm
5	Environmental alarm

Alarm Identification

The alarm ID specifies, in general terms, why the given alarm was raised. Alarm IDs are shown in the following table.

Alarm IDs and descriptions

ID	General Description	ID	General Description
1	Adapter error	30	Material supply exhausted
2	Application subsystem failure	31	Multiplexer problem
3	Bandwidth reduced	32	Out of memory
4	Call establishment error	33	Output device error
5	Communications protocol error	34	Performance degraded

ID	General Description	ID	General Description
6	Communications subsystem failure	35	Power problem
7	Configuration or customization error	36	Pressure unacceptable
8	Congestion	37	Processor problem
9	Corrupt data	38	Pump failure
10	CPU cycles limit exceeded	39	Queue size exceeded
11	Dataset or modem error	40	Receive failure
12	Degraded signal degradedSignal	41	Receiver failure
13	DTE-DCE interface error	42	Remote node transmission error
14	Enclosure door open	43	Resource at or nearing capacity
15	Equipment malfunction	44	Response time excessive
16	Excessive vibration	45	Retransmission rate excessive
17	File error	46	Software error
18	Fire detected	47	Software program abnormally terminated
19	Flood detected	48	Software program error
20	Framing error	49	Storage capacity problem
21	Heating/ventilation/cooling	50	Temperature unacceptable
22	Humidity unacceptable	51	Threshold crossed
23	I/O device error	52	Timing problem
24	Input device error	53	Toxic leak detected
25	LAN error	54	Transmit Failure
26	Leak detected	55	Transmitter Failure
27	Local node transmission error	56	Underlying resource unavailable
28	Loss of frame	57	Version mismatch
29	Loss of signal	101	Authentication Failure
			Note: ITU-T X.733 alarm ids from 58 to 100 are reserved. That is not yet assigned.
102	Breach of Confidentiality	103	Cable Tamper
104	Delayed Information	105	Denial of Service
106	Duplicate Information	107	Information Missing
108	Information Modification Detected	109	Information Out of Sequence
110	Intrusion Detection	111	Key Expired
112	Non Repudiation Failure	113	Out of Hours Activity
114	Out of Service	115	Procedural Error

ID	General Description	ID	General Description
116	Unauthorized Access Attempt	117	Unexpected Information
118	Unspecified Reason		

Alarm timestamp

The alarm timestamp specifies the date and time when the alarm was raised. The date and time given were current on the unit at the time the alarm was raised.

Alarm host

This field shows the host name on which alarm was raised. Since there are two units per node, there are two host names to which the alarms apply.

Alarm severity

The alarm severity specifies the seriousness of an alarm. Alarm severity can be one of the following:

- Warning:

  Indicates the detection of a potential or impending service affecting fault.

- Minor

  : Indicates the detection of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious fault.

- Major

  : Indicates that a service affecting condition has developed and an urgent corrective action is required.

- Critical:

  Indicates that a service affecting condition has developed and immediate corrective action is required.

Alarm description

The alarm description provides specific details about an alarm. The following is a sample alarm description:

```
Communications Communications Subsystem Failure Thursday July
22nd 2004 09:43:04 AM ss.unit1 Major Link0:  INSV, mateCon:
AVAIL, netCon:  AVAIL; Link1:  INSV, mateCon:  AVAIL, netCon:
AVAIL; PTPLink:  PTP0-SYSB, mateCon:  AVAIL;
```

Generating alarm-associated logs

For every alarm raised or cleared a log entry is displayed in the logs view and is also generated to the customer log file (if enabled at commissioning).

Redirecting trouble alarms to an SNMP server

Depending on your site network configuration, SST alarms may be directed to an SNMP server such as the IEMS server rather than to the CS 2000 Session Server Manager alarms view. Trouble alarms must then be viewed using the available SNMP server's alarm viewing tool (like the IEMS).

If an SNMP server is defined, using the commish tool, for receiving alarms, then logs associated with those trouble alarms do not appear at the CS 2000 Session Server Manager.

Alarms and LED fault indicators on the front panel

Hardware platform alarms raised by the HP servers are indicated by the LED alarm indicators on the front and rear panels.

Refer to the Hewlett-Packard document *HP Carrier-Grade Server cc3310 Product Guide* (HP part number: cc3310_Product) for information on managing cc3310 hardware faults, hardware LED designations, etc.

This document and other HP hardware-related information is available on the Hewlett-Packard web site at www.hp.com.

Unit level alarm states and severity

The alarms page displays alarm info for each of the units and individual alarm details for the active unit.

View of the unit summary alarms box

Unit	Activity	Jam	State	Connectivity	Host Name	Last Update Time
1	Active	no	. 1C+	.	sp2k-2	01:41:40

Each alarm state includes a color-coded alphanumeric value that represents the number of alarms in that state being raised and the severity associated with the alarm. If an alarm state has multiple alarms raised, the state field displays the most severe alarm in that state, and the number of alarms in the severity group. The button may also include a plus (+) symbol to indicate alarms of a lower severity also exist. The colored alarm buttons are listed below, in order of severity:

- No alarm -- grey with single in-service dot (.) symbol
- Unknown state -- blue with one dash (-) symbol
- Minor -- orange with the alphanumeric "1m"
- Major -- red with the alphanumeric "1M"
- Critical -- red with the alphameric "1C"

A critical alarm does not necessarily cause the system to SwAct. For a complete list of conditions that could cause the system to reset please refer to section "Monitoring and analyzing logs" (page 21).

Example alarms

Example alarm condition	Display
Two critical alarms in a particular alarm state	a red button with "2C"
Two critical alarms and one warning in a particular alarm state	a red button with "2C+"
One major alarm, one minor alarm, and one warning in a particular alarm state	a red button with "1M+"

Alarm page limitations

There are some limitations to the alarms page in the CS 2000 NCGL Platform Manager and CS 2000 Session Server Manager:

- The alarms page sort order cannot be modified. It defaults to sorting by alarms severity, then by time. The alarms page also does not support filtering of alarms.
- The alarms page header scrolls out of sight if the browser client is not large enough to view all alarms or if the user scrolls to the bottom of the window to view the oldest alarms.
- If the system date/time are changed after an alarm is raised, the alarms page does not update its timestamps. The timestamps shown at the alarms page were those current at the time that the alarms were raised.
- The alarms page refreshes automatically every 45 seconds. The refresh period is set by the system and can not be changed.

  If the system threshold values are changed after an alarm is raised, the alarms page does not update its values in the description field. The threshold values shown at the alarms page are the values that were current at the time that the alarms were raised. In general, any of the description text in an alarm is valid at the time the alarm was raised and is never updated.

Database monitoring

Software runs constantly to monitor for the following conditions:

- when contact with the database on the active unit is lost, a system SwAct is initiated and appropriate alarms and logs are generated
- when the database processes on either the active or inactive units go out of service, they are automatically restarted

- when a database corruption on the standby unit is detected, the database is removed and the database from the active unit is copied to the standby unit and appropriate logs and alarms are generated

Procedures for monitoring alarms

Use the following procedure to monitor alarms:

Procedure
"Viewing SST alarms" (page 34)

Monitoring and analyzing logs

Log reports include status and activity reports, regarding hardware or software faults, test results, changes in state and other temporary events or conditions likely to affect the performance of the system. Either a system action or a manual action can generate a log report with an associated alarm raising or clearance. Information shown about a particular log includes the type, timestamp, severity, and description.

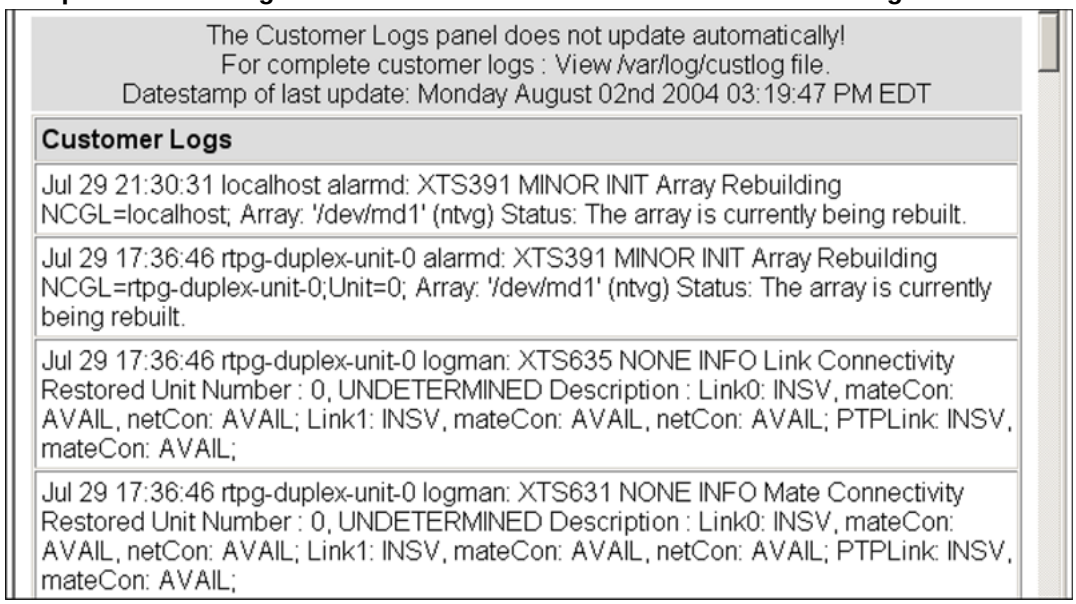
Customer logs are recorded to disk in **`/var/log/custlog`**. The logs page of the CS 2000 Session Server Manager reads this file to display log reports though the file can also be reviewed, copied and printed. Log files can also be loaded into a spreadsheet application for further analysis.

If the unit was configured during commissioning to transfer SNMP alarm traps to an OSS network, log reports related to the raising or clearing of alarms are not recorded to disk, but are only available on the IEMS or other third- party OSS application.

If the unit is configured to transfer logs to a remote server, all logs that are ordinarily viewable from the logs page of the CS 2000 Session Server Manager or local log file on the disk drive are sent to the log server.

The following sample logs page is generated by the CS 2000 Session Server Manager. The logs page displays a maximum of the most recent 2000 line entries from the current custlog file.

Sample customer logs viewed from the CS 2000 Session Server Manager


The Customer Logs panel does not update automatically!
For complete customer logs : View /var/log/custlog file.
Datestamp of last update: Monday August 02nd 2004 03:19:47 PM EDT

Customer Logs

Jul 29 21:30:31 localhost alarmd: XTS391 MINOR INIT Array Rebuilding NCGL=localhost; Array: '/dev/md1' (ntvg) Status: The array is currently being rebuilt.

Jul 29 17:36:46 rtpg-duplex-unit-0 alarmd: XTS391 MINOR INIT Array Rebuilding NCGL=rtpg-duplex-unit-0;Unit=0; Array: '/dev/md1' (ntvg) Status: The array is currently being rebuilt.

Jul 29 17:36:46 rtpg-duplex-unit-0 logman: XTS635 NONE INFO Link Connectivity Restored Unit Number : 0, UNDETERMINED Description : Link0: INSV, mateCon: AVAIL, netCon: AVAIL; Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink: INSV, mateCon: AVAIL;

Jul 29 17:36:46 rtpg-duplex-unit-0 logman: XTS631 NONE INFO Mate Connectivity Restored Unit Number : 0, UNDETERMINED Description : Link0: INSV, mateCon: AVAIL, netCon: AVAIL; Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink: INSV, mateCon: AVAIL;

Viewing logs for alarms that are redirected to an SNMP server

If an SNMP server was defined during commissioning to receive alarms, alarms are viewed on that server and logs associated with those alarms are not generated to the customer log file because alarm-related log generation is suppressed when SNMP servers are defined. If the IEMS server is your SNMP server, then it displays your trouble alarms and keeps an alarm history. For a history of alarms, refer to your SNMP server, not the CS 2000 Session Server Manager.

Mapping alarms to logs

The best way to map trouble alarms to log entries is by comparing the log and alarm descriptions along with the time and date stamps to obtain a match.

Managing the contents of log files

Fields within the log files are delimited (separated) by a ^M (control-M) to facilitate parsing with a spreadsheet program.

The system log management utility checks every hour to see if the custlog file's contents exceed 5 MB. If they do, the file is saved and rotated. A series of up to 20 versions of the custlog file plus the current log file are kept on disk at any time. Each successive file has a number appended to the filename. This higher the sequence number, the older the log file. The oldest log file is always custlog.20.

Customer logs on the SST

Customer logs (SIPC, SIPM, SIPS, DBSE, SIPGW, CRTM and XTS logs) are generated to bring state change information, errors, or other events occurring on the platform (XTS logs) and within the SIP Gateway application to the attention of the customer. For example, when the SIP Gateway application starts (unlocks) or stops (locks) customer log is generated. When an alarm condition occurs, customer log information, is generated to the /var/log/custlog directory on the SST, and is also forwarded to the IEMS OSS interface or other another generic OSS interface that is on the CS-LAN.

The SIP Application Maintenance process is responsible for generating all call processing state change logs (SIPC and SIPGW), maintenance (SIPM) related logs, and database state change logs (DBSE) for the SIP Application. This process generates three types of customer logs:

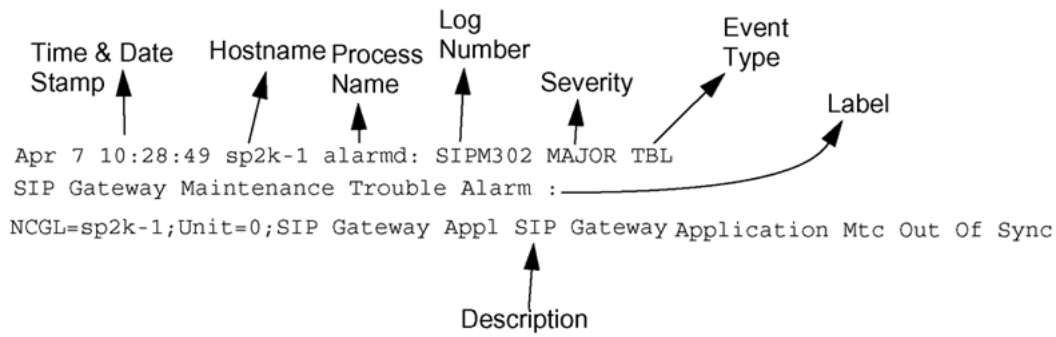
- state change logs (informational)
- trouble logs
- alarm trouble logs

Unless alarms are redirected to an SNMP server, every alarm that is raised by the NGCL operating system has an associated XTS300-series log generated. Once the alarm condition is cleared, a complementary XTS600-series log is generated.

Customer log histories can be only viewed by directly accessing the custlog file using the SST CLI (command line interface). Log files can also be downloaded using FTP to a PC or other system capable of connecting to the SST on the secure CS-LAN.

The following diagram shows a sample customer log entry in the log file, along with an anatomy of its content:

Format and content of a SIP Gateway application (SIPC, SIPM or DBSE) log



Format and content of an NCGL operating system (XTS) log

```
<time stamp> <hostname> <process name> <Name> <Number> <Severity> <Event Type>
<Label>
<Description>

* Nov 12 15:54:56 loopback alarmd: NXTS802 MINOR INIT Array: '/dev/md0'
* |               |        |       |   |   |     |    |      |
* |               |        |       |   |   |     |    |      +--- description
* |               |        |       |   |   |     |    +---------- label
* |               |        |       |   |   |     +--------------- event type
* |               |        |       |   |   +--------------------- Severity
* |               |        |       |   +------------------------- log number
* |               |        |       +----------------------------- log name
* |               |        +------------------------------------- process name
* |               +---------------------------------------------- hostname
* +-------------------------------------------------------------- time stamp
```

Use the following procedures to access logs:

Procedure	NCGL platform or SIP GW application
"Viewing SST logs" (page 36) from the CS 2000 Session Server Manager or CS 2000 NCGL Platform Manager	All
"Viewing and saving log files" (page 40) (for log reports) from the NCGL operating system	All

The following table displays all available logs that are generated by the SIP Gateway application and the NCGL platform.

Customer log	SIP GW application and NCGL platform
CPUM300	SIP GW Application
CTRM700 and CTRM701	SIP GW Application
DBSE300	SIP GW Application
NCAS325 through NCAS601	SIP GW Application
NMSS115 through NMSS118	SIP GW Application
SIPC301 through SIPC750	SIP GW Application
SIPM300 through SIPM500	SIP GW Application
SIPS300 through SIPS606	SIP GW Application
STGW700	SIP GW Application

Customer log	SIP GW application and NCGL platform
XTS300 through XTS399	NCGL
XTS638 and XTS676 through XTS679	NGCL

Logs generated on the CS 2000

Some customer logs are generated on the CS 2000. These logs belong to the NGSS log group and are related to the CS2B0008 and CS2B0009 SOC (service option codes) used to support SIP trunking on the CS 2000 and GWC. For more information about the logs in the NGSS log group, refer to the *Carrier Voice over IP Fault Management Logs Reference Manual* (NN10275-909).

Remove and replace a unit or component

The following items are field replaceable:

- the entire unit
- disk drives
- power supply modules
- DVD-ROM drive

All other component failures should be handled by replacing the entire unit.

Replacing an entire unit

The intent of replacing the entire unit is to facilitate component or unit replacement so that the node can be returned to fault tolerant service capability as soon as is possible.

Replacing hard disk drives

Each unit operates using a disk mirroring (RAID 1) scheme. If a disk drive fails on the active unit, a SwAct is automatically performed by the system to the standby unit and an alarm raised. Call processing is not impacted.

A failed disk drive can be removed and replaced with a spare. Failed disk drives can be replaced without removing the unit from the frame.

Replacing power supply modules

A failed power supply module can be removed and replaced with a spare. Failed power supply modules can be replaced without removing the unit from the frame.

Replacing the CDRW/DVD-ROM drive

A failed CDRW/DVD-ROM drive can be removed and replaced with a spare. Failed drives can be replaced without removing the unit from the frame; however, the unit must be taken out of service.

Remove and replace procedures

The following component and unit remove and replace procedures are available for SST.

Procedure	Hardware, platform or SIP GW application
"Replacing an SST unit" (page 65)	entire unit
"Replacing an SST hard drive" (page 74)	hard disk drive
"Replacing an SST power supply" (page 83)	power supply module
"Replacing an SST CDRW/DVD-ROM drive" (page 81)	CDRW/DVD-ROM drive

Routine maintenance

This section provides a list of activities used to perform routine maintenance. Routine maintenance is required to ensure the components continue normal operation over time.

Adhering to a proper routine maintenance schedule can prevent faults from occurring. Perform the following routine maintenance activities at the specified time intervals. For assistance with these tasks, refer to the *HP Carrier-Grade Server cc3310 Product Guide*, HP part number cc3310_Product.

Consult your Nortel installation staff for additional maintenance practices and guidelines.

Tasks to be performed daily

Component	Task	Document	Notes
SST	Monitor alarms and logs	*Session Server Trunks Fault Management* (NN10332-911)	

Tasks to be performed weekly

Component	Task	Document	Notes
SST	Inspect the LEDs front panel of both units; ensure there are no faults indicated	*HP Carrier-Grade Server cc3310 Product Guide*, HP part number: cc3310_Product	acquire HP guide from HP.com web site

Tasks to be performed per office schedule

Component	Task	Document	Notes
SST	Clean the DVD-ROM drive	*HP Carrier-Grade Server cc3310 Product Guide*, HP part number: cc3310_Product	
SST	Monitor the fan exhaust cowlings for dust buildup. There are no air filters or fan filters to replace.	no formal procedure required	Refer to your site maintenance guidelines for removing excess dust.
SST	After each upgrade or MR applied electronically, clean up unused iso images in the /opt/swd directory.	no formal procedure required	

Preventive maintenance

This section provides a list of procedures used to perform preventive maintenance for Carrier VoIP components. Preventive maintenance is required on components to prevent service impacting fault conditions.

Tasks to be performed daily

Component	Task	Document	Notes
SST	Monitor alarms and logs	*Session Server Trunks Fault Management* (NN10332-911)	

Component	Task	Document	Notes
GWC	Monitor GWC logs to verify connectivity has not been lost with the SST and to identify any call processing problems.	*GWC Fault Management* (NN10090-911)	Schedule can be adjusted to correspond to GWC log monitoring schedule.
XA-Core	Monitor logs to verify that DPT trunks do not unexpectedly go out of service. Each outage should have corresponding logs in the SST to explain why and the lack of corresponding SST logs indicates a problem.	*CS 2000 Fault Manageme nt* (NN10083-911)	Schedule can be adjusted to correspond to XA-core log monitoring schedule.

Tasks to be performed per office schedule

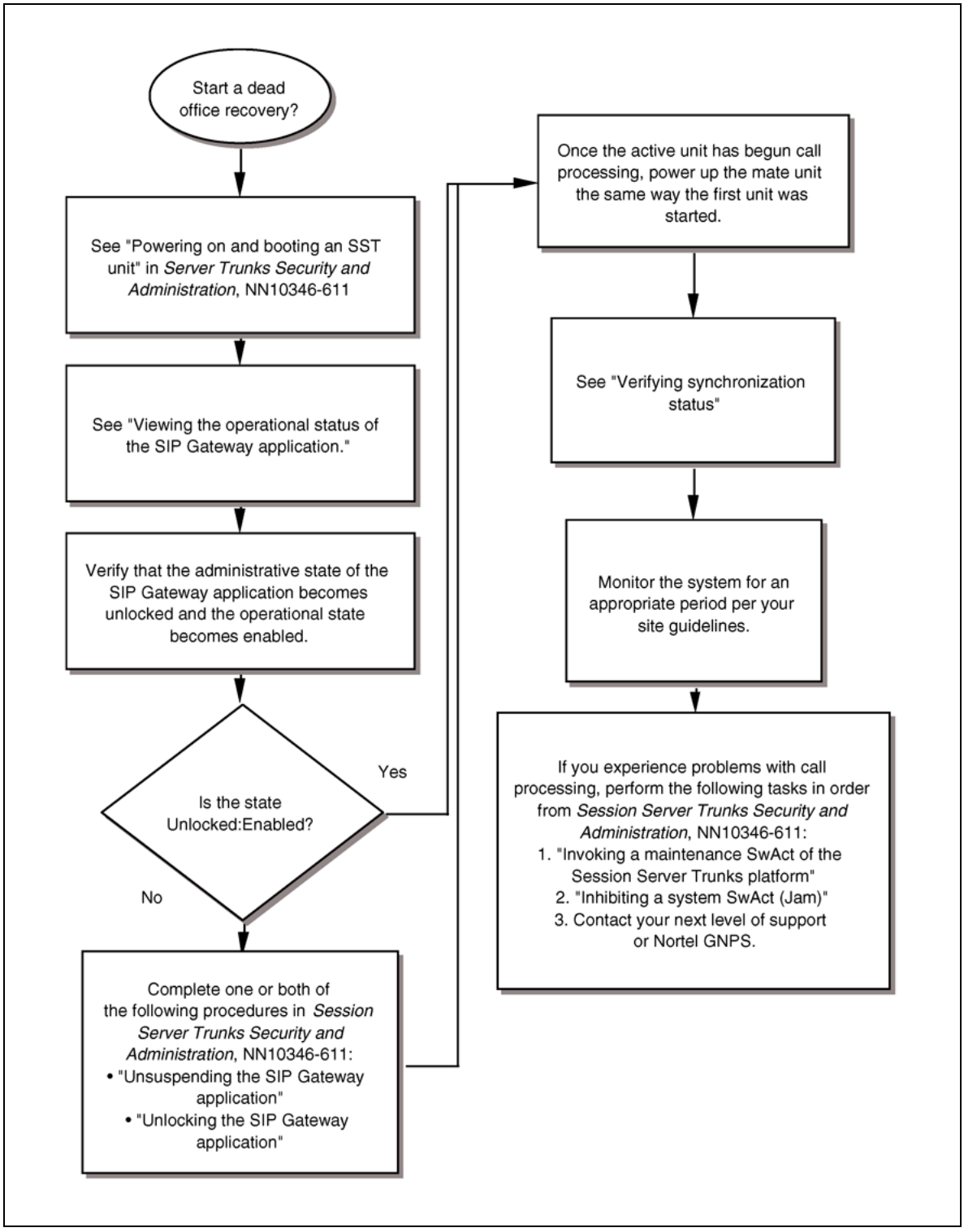
Component	Task	Document	Notes
SST	Clean the DVD drive	*HP Carrier-Grade Server cc3310 Product Guide*, HP part number: cc3310_Product	
SST	Inspect the LEDs front panel of both units; ensure there are no faults	*HP Carrier-Grade Server cc3310 Product Guide*, HP part number: cc3310_Product	acquire HP guide from HP.com web site
SST	Periodically check the /opt/apps/logs directory to verify that sufficient space exists in that file system. Clean up old log and trace files as needed to make more space.	This document	
SST	Check that cables and connectors are secure at both the front and rear of each chassis. Also, inspect the integrity of all cabling to ensure there is no frayed wiring.	no formal procedure required	

Performing a dead office recovery of an SST node

Execute the procedures in the following task flow to restart an SST node.

There are no network component dependencies related to when either of the units is booted. The SST, XA-Core, and GWCs can come back into service in any order. Once the active unit has booted and the SIP Gateway application initializes, it reads its state file and attempts to return to the state that it was in previously (for instance, Unlocked:Enabled). Call processing resumes as soon as the GWCs are in service and responding to discovery messages from the SIP Gateway application.

Dead office recovery task flow



Restoring a SIP Gateway application database

Database backups are made to secure the information stored in the SIP Gateway application database. If there is a complete failure or loss of both units in the node or if an unrecoverable corruption in the database on the active unit occurs, a backup copy of the database can be restored to the active unit.

There is only a single backup copy of the database saved on each unit. It contains the last or most recently backed up copy (within the last 24 hours) of the database. The database on each unit is automatically backed up at 1:00 AM each day. In addition, manual backup of the database on an as needed basis such as when an upgrade activity is scheduled. It is recommended that manual backups be performed on the active database.

Applying a backup copy of the database restores the active database to its state when the backup was made. The database must be restored to the active unit. Once the restore operation is complete, and the active unit is brought back into an Enabled Operational state (the SIP Gateway application is unsuspended, unlocked, and fault tolerance restored, synchronization of the standby unit database to the active unit database begins.

The following table lists the procedures available to restore the SIP Gateway application database from a backup copy.

Database restore procedures

Procedure
"Restoring SST" (page 86)

Individual procedures

ATTENTION

Although you can complete some of the procedures in the following sections on their own, you must perform most as part of a higher level activity. See "Fault management overview" (page 7).

Viewing SST alarms

Purpose of this procedure

This procedure provides access to the platform and SIP Gateway application service-related alarms that are currently active on the SST.

A customer log entry is generated for each alarm raised and cleared.

Limitations and restrictions

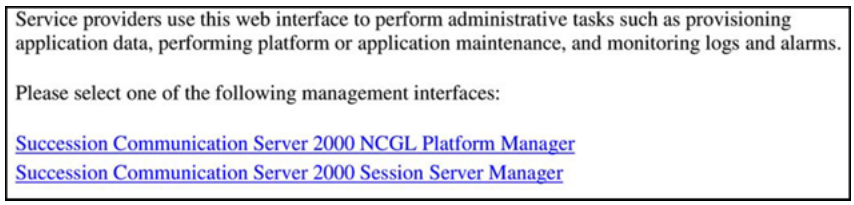
Alarms cannot be sorted, filtered or removed using this procedure.

Prerequisites

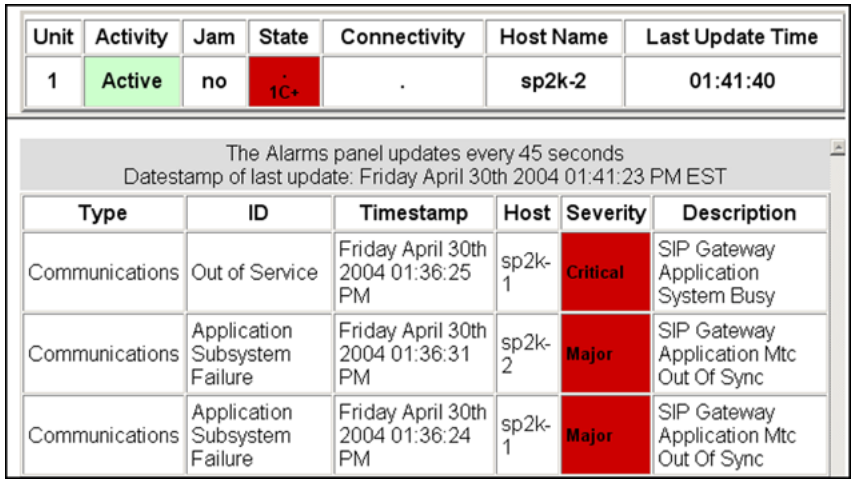
This procedure has no prerequisites.

Action

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



2	From either view, click the **Alarms** link. *The Alarms page is displayed.*



Unit	Activity	Jam	State	Connectivity	Host Name	Last Update Time
1	Active	no	1C+	.	sp2k-2	01:41:40

The Alarms panel updates every 45 seconds
Datestamp of last update: Friday April 30th 2004 01:41:23 PM EST

Type	ID	Timestamp	Host	Severity	Description
Communications	Out of Service	Friday April 30th 2004 01:36:25 PM	sp2k-1	Critical	SIP Gateway Application System Busy
Communications	Application Subsystem Failure	Friday April 30th 2004 01:36:31 PM	sp2k-2	Major	SIP Gateway Application Mtc Out Of Sync
Communications	Application Subsystem Failure	Friday April 30th 2004 01:36:24 PM	sp2k-1	Major	SIP Gateway Application Mtc Out Of Sync

3 Using the alarms view, refer to "Monitoring and analyzing alarms" (page 15) for assistance in reviewing and correlating alarms to logs and to troubleshooting activities.

The overall unit alarm state is only shown in the CS 2000 NCGL Platform Manager view.

—End—

Viewing SST logs

Purpose of this procedure

This procedure provides access to the platform and SIP Gateway application service-related logs that are currently active on the SST.

You cannot save or print log entries or log file contents using this procedure.

Limitations and restrictions

Only the most recent logs generated are viewable from the GUIs using this procedure. To view log histories, refer to procedure "Viewing and saving log files" (page 40).

Logs viewed using this procedure include:

- DBSE logs (SIP Gateway application database)
- CTRM logs (application)
- STGW logs (application)
- SIPC logs (application)
- SIPM logs (application)
- SIPS logs (application)
- XTS logs (platform)

Logs entries are recorded in a file located at /var/log/custlog.

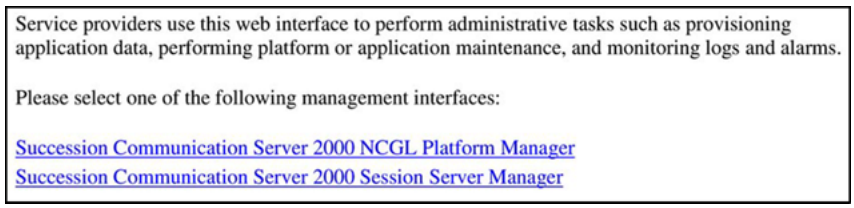
When viewing logs from an IEMS rather than the Session Server GUIs, log headers may differ slightly from what is shown in this document; however the content of the logs does not differ between the views.

Prerequisites

Alarm conditions must be created or cleared to generate logs entries.

Action

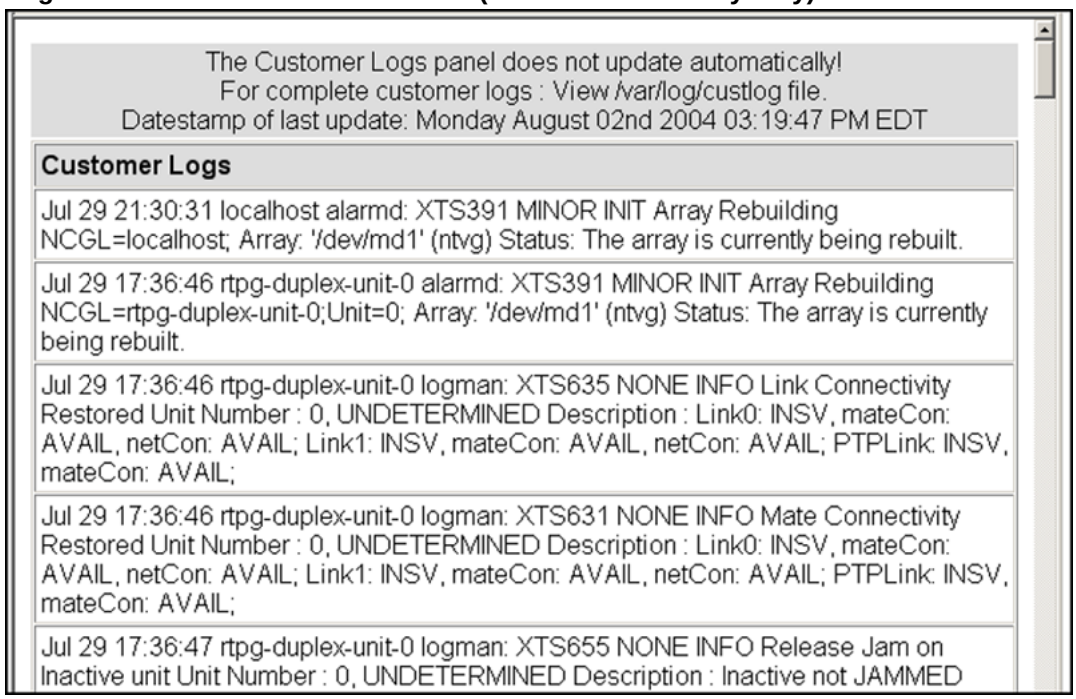
Step	Action
	At the CS 2000 Session Server Launch Point
1	Select either the **Succession Communication Server NCGL Platform Manager or Succession Communication Server 2000 Session Server Manager** from the launch point menu.



2 From either view, click the **Logs or Customer Logs** link.

The logs page is displayed.

Logs view from Session Server GUIs (view from IEMS may vary)



3 Using the logs view, refer to "Monitoring and analyzing logs" (page 21) for assistance in reviewing, analyzing and correlating logs to alarm activity and to troubleshooting activities.

—End—

Viewing SIP Gateway application log files

Purpose of this procedure

This procedure instructs you in how to capture SIP Gateway application logs into a single tar file. The data collected is saved in a file located in the /tmp directory.

Limitations and restrictions

The output TAR file contains the following logs:

- Unit status
- CPU utilization
- Memory utilization
- Status of sockets used by application
- Status of application threads
- Application cache data
- SIP signaling statistics
- Traps (tracelog.* files)
- Customer logs
- Design logs
- NGSS Load information
- Swerrs (traceError files)

The tool does not require root permission for execution.

Prerequisites

None.

Action

Step	Action
	At the Session Server console
1	Log onto the Session Server console as mtc user and enter your password.
2	At the prompt, navigate to the bin directory by typing `$ cd /opt/apps/bin` and press the Enter key.

3 Generate the SIP Gateway application log tar file by typing

```
./sipgwlc
```

and press the Enter key.

4 Secure copy the log file to a remote system by typing

```
$ scp <filename> <user>@<machine>
```

where

<filename> is the filename of the log tar file that you want to secure copy.
<user> is the username for the remote machine.
<machine> is the IP address of the remote machine.

Example

```
scp /tmp/sipgw.logs.6586.tar.gz willy@10.10.10.10
```

5 To view the log files from a windows-based system, goto to Step 7.

To uncompress the log tar file on a unix-based system, type

```
gunzip <filename>
```

where

<filename> is the filename of the log tar file that you want to secure copy.

Example

```
gunzip sipgw.logs.6586.tar.gz
```

6 Extract the files from the log tar file by typing

```
tar -xvf <filename>
```

where

<filename> is the filename of the log tar file that you want to secure copy.

Example

```
tar -xvf sipgw.logs.6586.tar.gz
```

7 To view the contents of the log tar file on a windows-based machine, open the file using WINZIP.

—End—

Viewing and saving log files

Purpose of this procedure

This procedure instructs you how to transfer log files to another system that has secure access to the CO LAN using FTP (file transfer protocol) for later printing or storage. SST log files are saved as ASCII text files and stored on the SST hard drive.

You can also use this procedure to retrieve and save the same log files for later importing into spreadsheet applications used for data analysis.

Limitations and restrictions

If logs were set up to be forwarded to the OSS at commissioning time, then log entries are not generated to the customer log file on the SST hard drives.

This procedure assumes that there is no local or network printer available to the SST platform.

The system log management utility checks every hour to see if the custlog file's contents exceed 5 MB. If they do, the file is saved and rotated. A series of up to 20 versions of the custlog file plus the current log file are kept on the SST at any time. Each successive file has a number appended to the filename. This higher the sequence number, the older the log file. The oldest log file is always custlog.20.

Prerequisites

You must have access to the SST console, either through a direct connection at the rear of the active SST unit or through the IEMS application.

Action

Step	Action
	At the Session Server console
1	Log onto the Session server console as mtc user and enter your password.
2	At the prompt, navigate to the file level where log files are stored by typing `$ cd /var/log` and press the Enter key.

```
[mtc@zn0jc mtc]$ cd /var/log
[mtc@zn0jc log]$ ls
apache          designlog       netmonhistory    netmonhistory.5  ntp.3
boot-04141227   maillog         netmonhistory.1  nt_fsck.log      ntp.drift
boot.log        messages        netmonhistory.2  ntp              secure
cron            misc.log        netmonhistory.3  ntp.1            spooler
custlog         netmonhistbufs  netmonhistory.4  ntp.2            traplog
[mtc@zn0jc log]$
```

3 Review the contents of a custlog file by typing

>cat<custlog_filename.#>|more

and pressing the enter key.

where

custlog_filename.# is the version-name of the custlog file you want to display.

Example

```
cat custlog.12 |more
```

Press the space bar to scroll through the file if its contents are larger than the screen can display.

4 Log to the remote system where you are sending the log files by typing

$ ftp<hostid>

and pressing the Enter key.

where

<hostid> is the name of the remote system that has secure access to the CS-LAN where you are sending the log files.

5 For each of the log files that you want to save, print or process, FTP them to the remote system by typing

$ put<logfilename>

and pressing the Enter key.

where

<logfilename> is the name of a log file from the following list:

- custlog (for SIP Gateway application and NCGL logs)

—End—

Additional information

The following table shows the contents for customer supported log files for this release:

Log Content	Location	Log Types
SIP GW Application logs	/var/log/custlog	All SIPxnnn logs All DBSEnnn logs All STGWnnn logs
Security certificate management logs	/var/log/custlog	All CTRMnnn logs
NCGL Operating System logs	/var/log/custlog	ALL XTS logs

Viewing the operational status of the SIP Gateway application

Purpose of this procedure

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

Limitations and restrictions

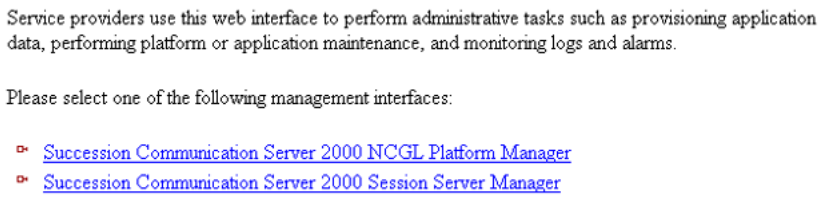
This procedure provides instructions for determining the service status of the SIP Gateway application software only. For instructions on determining the status of the platform and operating system, refer to procedure "Viewing the operational status of the NCGL platform" (page 48).

Prerequisites

There are no prerequisites for this procedure.

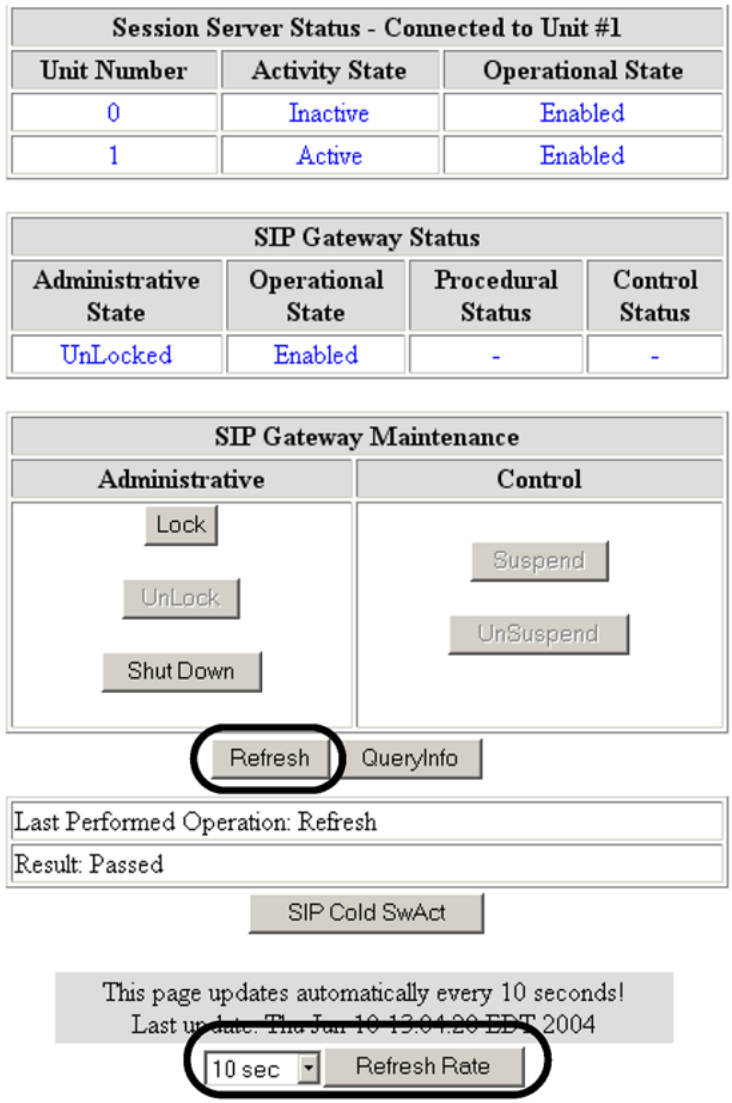
Action

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



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

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



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

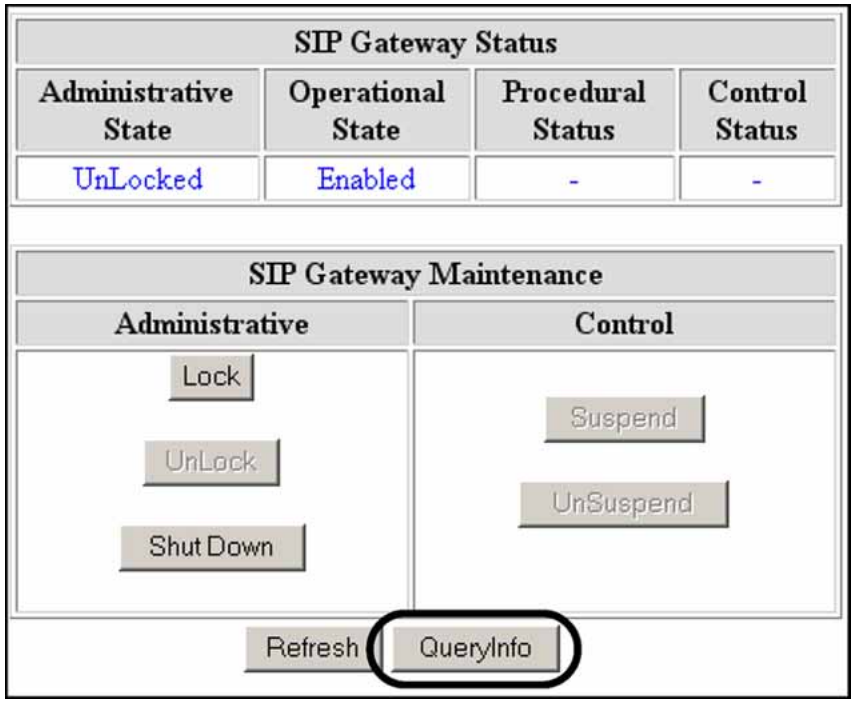
4 See "Interpreting SIP Gateway application status and maintenance fields" (page 46) to review the description of the various fields of this view.

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

5 The following service affecting actions are available:

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

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



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

—End—

Interpreting SIP Gateway application status and maintenance fields

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

Node status field descriptions

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

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

SIP Gateway application Status field descriptions

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

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

SIP Gateway Maintenance field descriptions and interpretation of service states

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

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

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

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

Viewing the operational status of the NCGL platform

Purpose of this procedure

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

Limitations and restrictions

This procedure provides instructions for determining the service status of the SST NCGL platform only. For instructions on determining the status of the SIP Gateway application, refer to procedure "Viewing the operational status of the SIP Gateway application" (page 43).

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

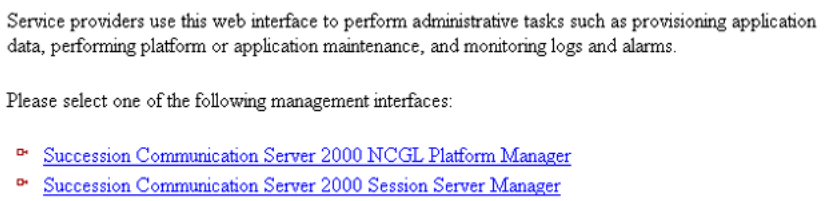
This procedure does not describe how to view customer logs or alarms. For detailed instructions about viewing customer logs or alarms, refer to procedures in *Session Server Trunks Fault Management* (NN10332-911).

Prerequisites

There are no prerequisites for using this procedure.

Action

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



The Platform Main Page menu is displayed.

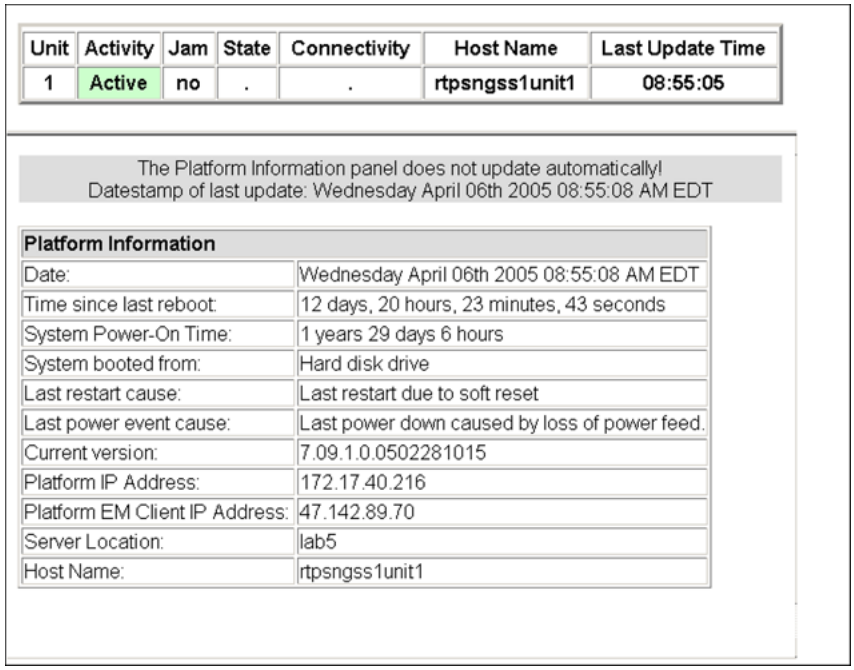
2 Use the following table to determine your next step:

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

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

ATTENTION

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



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

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

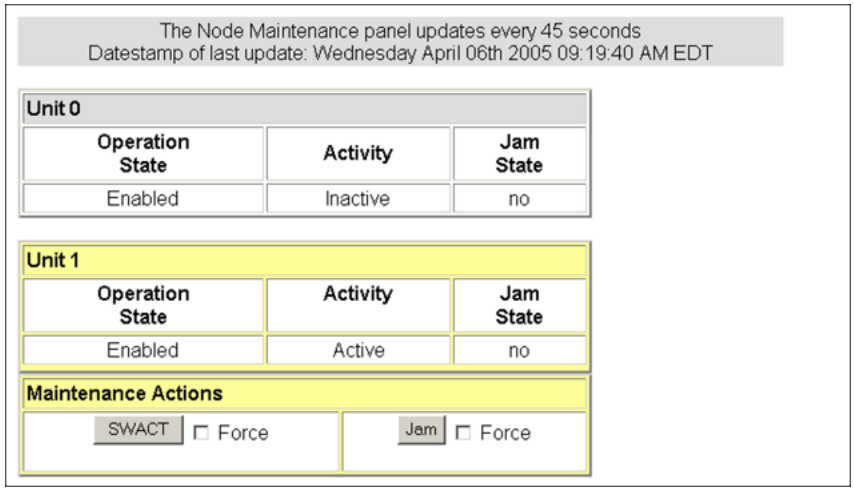
Platform Information	
Date:	Wednesday April 06th 2005 08:55:08 AM EDT
Time since last reboot:	12 days, 20 hours, 23 minutes, 43 seconds
System Power-On Time:	1 years 29 days 6 hours
System booted from:	Hard disk drive
Last restart cause:	Last restart due to soft reset
Last power event cause:	Last power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

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

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

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

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

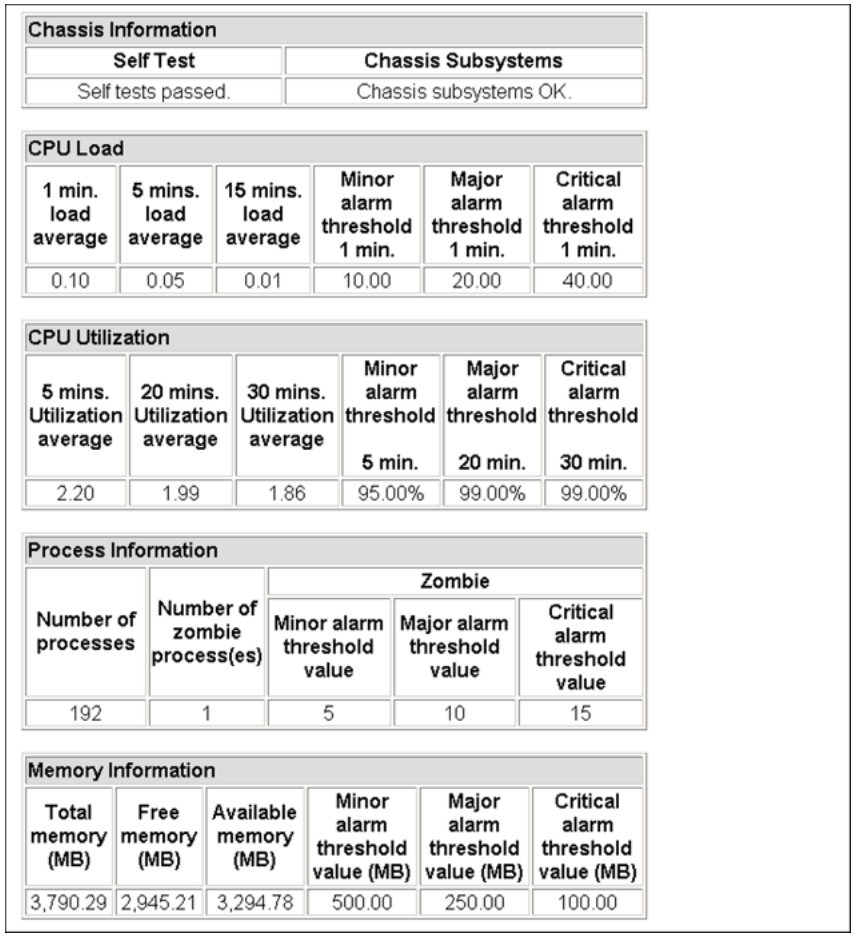


The Node Maintenance panel is refreshed every 45 seconds.

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

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

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



Chassis Information

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

CPU Load

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

CPU Utilization

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

Process Information

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

Memory Information

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

The Chassis Information panel is not automatically refreshed.

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

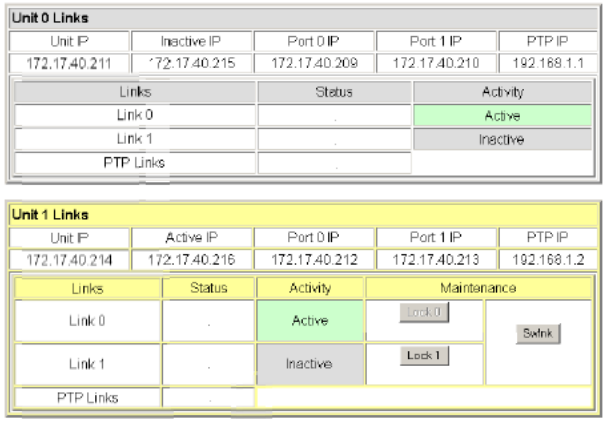
Field	Description
Load average threshold values	indicates the 1 minute CPU load average utilization threshold value in percentages. When the set threshold value is exceeded, the appropriate minor, major or critical alarm is raised.
CPU Utilization	
Utilization average	indicates the 5, 20 and 30 minute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

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

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

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

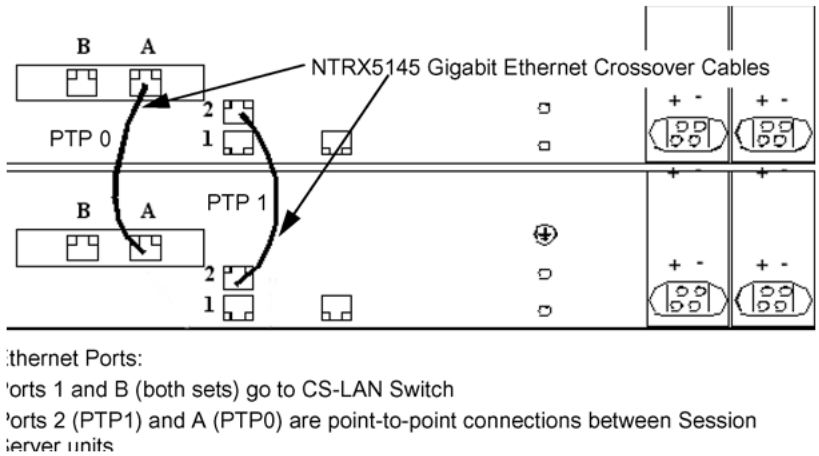
The Network Connectivity panel is refreshed every 45 seconds.



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

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

Crossover and LAN Ethernet cable connections for SST units



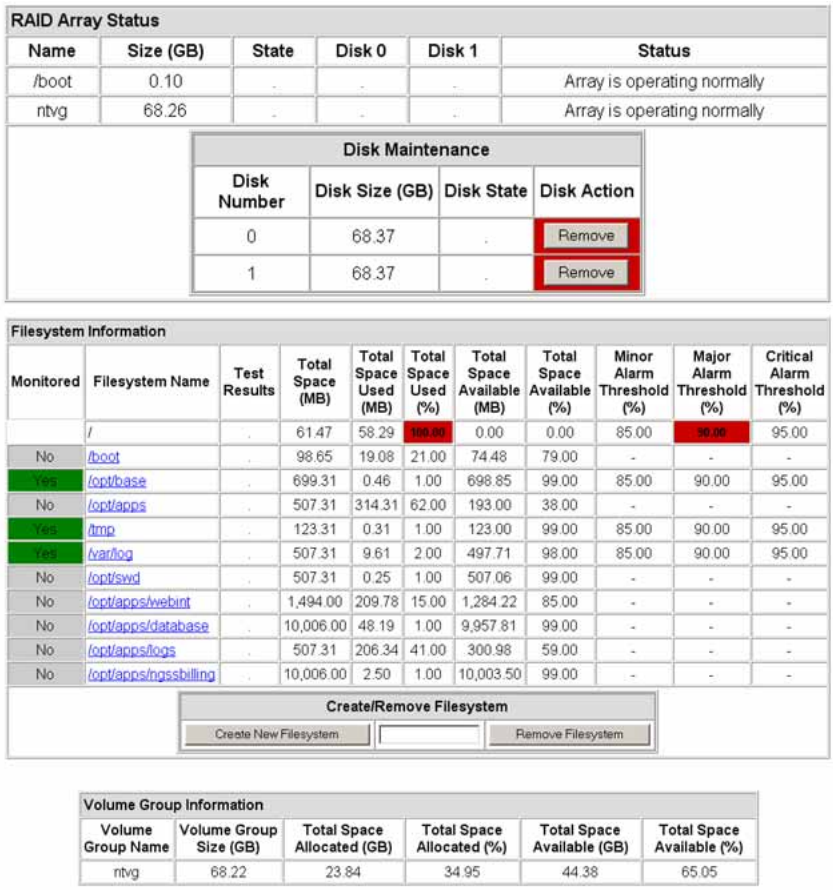
thernet Ports:
orts 1 and B (both sets) go to CS-LAN Switch
orts 2 (PTP1) and A (PTP0) are point-to-point connections between Session erver units

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

ATTENTION

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

To create and remove file systems, refer to Creating a filesystem and Removing a filesystem.



RAID Array Status

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

Disk Maintenance

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

Filesystem Information

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

Create/Remove Filesystem

Create New Filesystem | Remove Filesystem

Volume Group Information

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

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

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

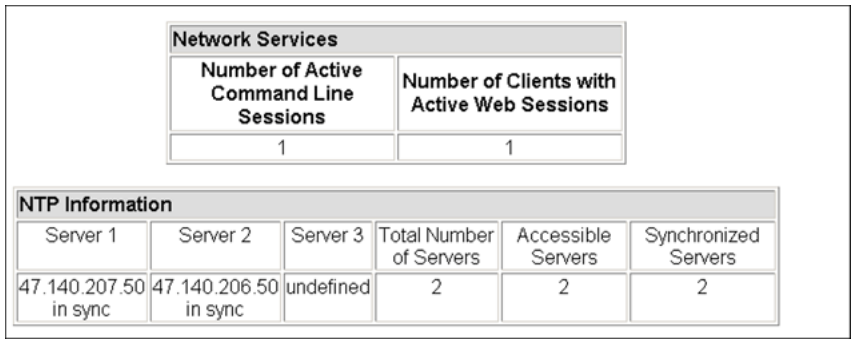
Field	Description
Filesystem Information: Major Alarm Threshold (%)	maximum amount of disk space (in %) that can be used before a major alarm is raised indicating that the set threshold has been exceeded
Filesystem Information: Critical Alarm Threshold (%)	maximum amount of disk space (in %) that can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

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

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

ATTENTION

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



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

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

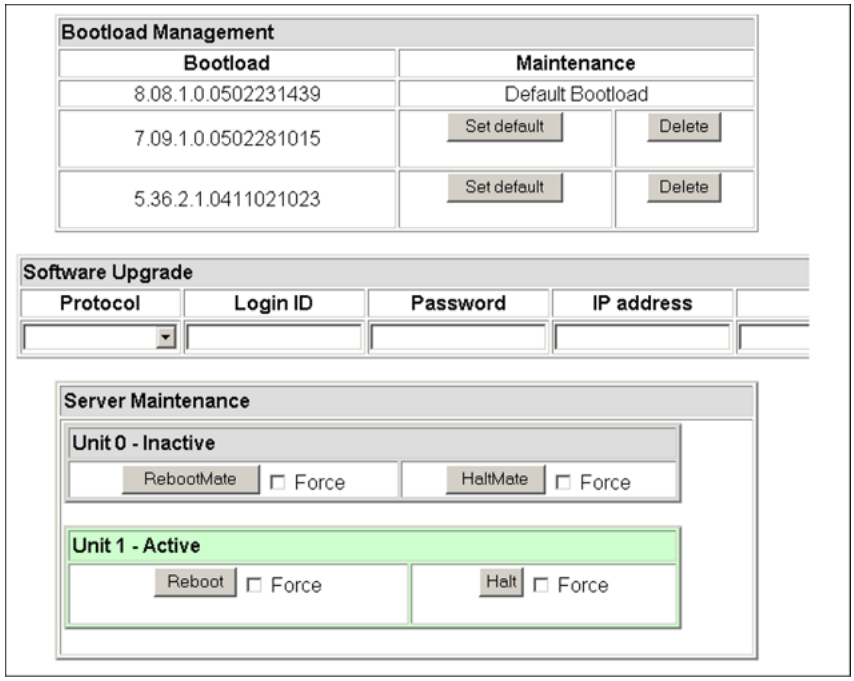
Field	Description
Network Services: Number of Active Command Line Sessions	number of command line interface (CLI) sessions (both remote and local) on the unit
Network Services: Number of Clients with Active Web Sessions	number of clients running one or more web GUI sessions
NTP Information: Server1 -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

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

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

ATTENTION

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



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

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

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

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

You are returned to the login page

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

—End—

Verifying synchronization status

Purpose of this procedure

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

Limitations and restrictions

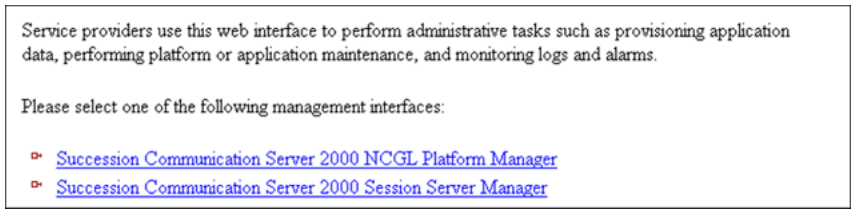
There are no restrictions for performing this procedure.

Prerequisites

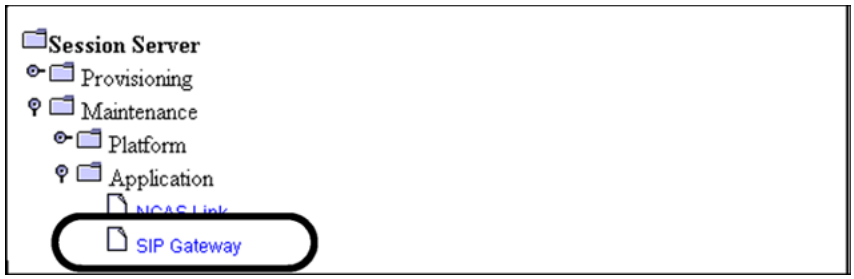
There are no prerequisites for performing this procedure.

Action

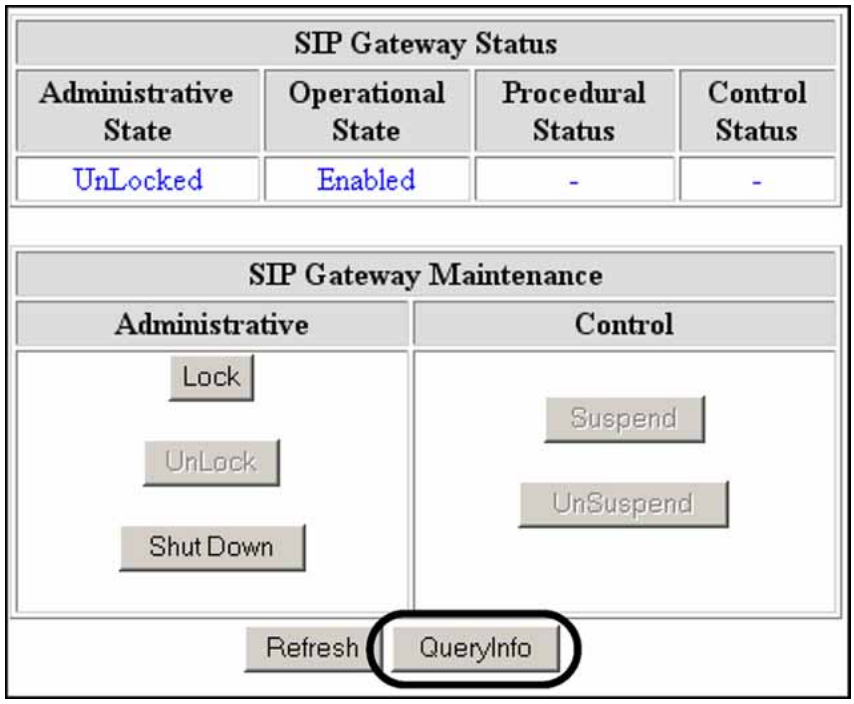
Step	Action
	At the CS 2000 Session Server Manager or IEMS client
1	Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.



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

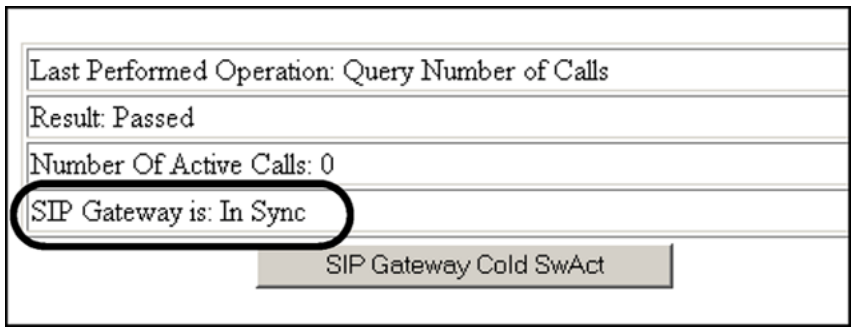


3	At the bottom of the SIP Gateway Maintenance panel, click **QueryInfo**.



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

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



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

—End—

Replacing an SST unit

Purpose of this procedure

This procedure provides the steps for removing and replacing a faulty SST unit with a spare. It is intended to facilitate unit replacement so that the SST node can be returned to fault-tolerant service capability as soon as is possible.

Limitations and restrictions

ATTENTION

This procedure should only be used on an inactive SST unit. If the unit you want to replace is the active unit, a system SwAct must be performed. Refer to the procedure "Invoking a maintenance SwAct of the SST platform" in *Session Server Trunks Security and Administration* (NN10346-611).

This procedure does not instruct you how to install additional SST nodes into your network. Refer to your Nortel installation support representative for support in adding new SST nodes to your network.

Prerequisites

CAUTION

Observe the general safety precautions against personal injury and equipment damage outlined by your site safety guidelines at all times.

This procedure assumes that you have fully operational SST node made up of both active and inactive units, and that you are able to SwAct service and callp activity.

Action

Step	Action
	At the CS 2000 Session Server Manager
1	Execute the procedure "Inhibiting a system SwAct (Jam)" in *Session Server Trunks Security and Administration* (NN10346-611).

ATTENTION

Executing this procedure generates an alarm/log XTS300.

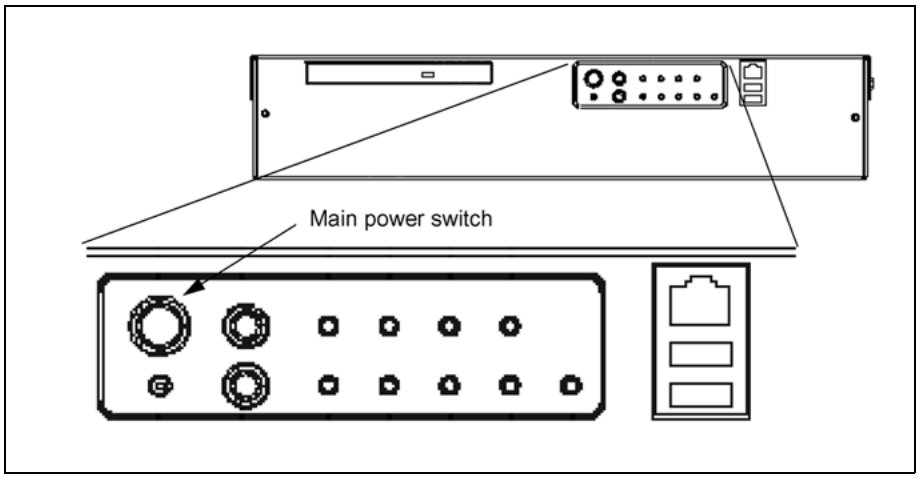
2 Determine if the SST unit to be replaced is still in service by executing procedure "Viewing the operational status of the NCGL platform" (page 48).

3 Use the following table to determine your next step:

If	Do
the SST unit to be replaced is still in service,	Refer to procedure "Halting (shutting down) an SST unit" in *Session Server Trunks Security and Administration* (NN10346-611).
the SST unit to be replaced is not in service,	continue with the next step

At the front panel of the SST chassis

4 Turn off the power to the SST unit being replaced at the main power switch located on the front panel of the SST chassis as shown below.



At the rear of the SST chassis and SAM-F frame

5 Label and remove the Ethernet cables from the rear of the chassis, referring to the table of "Additional installation and removal information" (page 71) as needed.

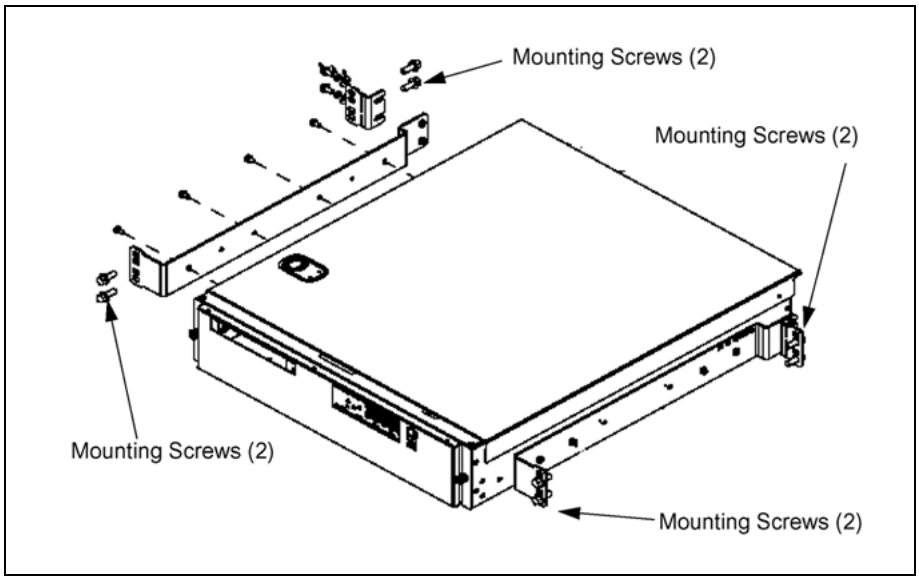
6 Label and remove the two Ethernet crossover cables (NTRX5145) from the rear of the chassis, referring to the table of "Additional installation and removal information" (page 71) as needed.

7 Remove the power supply cables (NTRX5199 or NTRX5146) from the rear of the SST chassis, referring to the table of "Additional installation and removal information" (page 71).

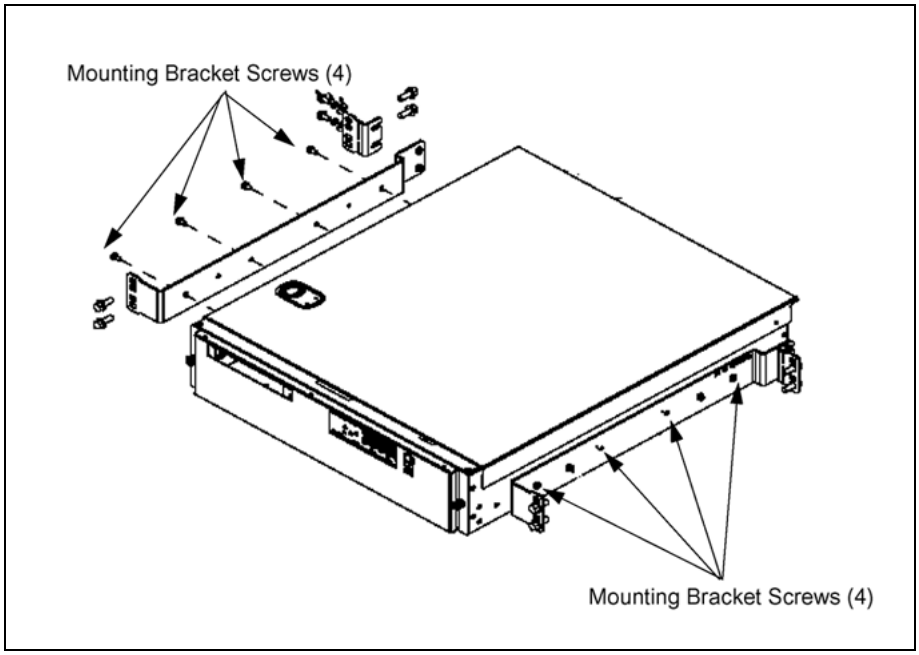
8 Remove the ground cable (NTRX5198) from the rear of the SST chassis as shown in figure "SST unit rear view of ports and ground connection" (page 71).

9 If the SST chassis is connected to the alarm system, disconnect the alarm cable (NTRX5179) from the DB15 connector, referring to the table of "Additional installation and removal information" (page 71) as needed.

10 Unscrew and remove the chassis mounting screws that hold the SST chassis in the SAM-F frame and remove the SST unit from the frame. There are four screws at the front of the chassis and four screws at the back of the chassis (eight screws total), as shown in the following figure.



11 If necessary, remove the mounting brackets from the old unit and mount them on the replacement unit. There are four screws that hold each mounting bracket to the sides of the SST unit chassis (eight screws total), as shown in the following figure.



12 Insert the replacement SST unit into the same slot (either mounting position 68 or 72) in the SAM-F frame and secure using the mountings screws that you removed in step 10.

13 If the SST chassis is connected to the alarm system, connect the alarm cable (NTRX5179) to the DB15 connector, referring to the table of "Additional installation and removal information" (page 71) as needed.

14 Connect the ground cable (NTRX5198) to the rear of the SST chassis at its connect point as shown in figure "SST unit rear view of ports and ground connection" (page 71).

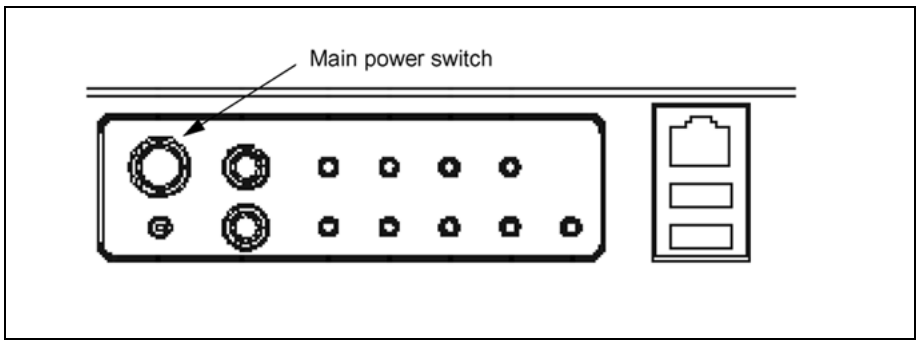
15 Attach and secure the power cables (NTRX5199 or NTRX5146) to the rear of the replacement SST chassis, referring to the table of "Additional installation and removal information" (page 71) as needed.

16 At the power supply panel, reapply power to the replacement SST chassis, referring to the table of "Additional installation and removal information" (page 71) as needed.

17 Connect the two Ethernet crossover cables (NTRX5145) to the replacement SST chassis, referring to the table of "Additional installation and removal information" (page 71) as needed.

18 Connect the Ethernet cables to the replacement SST chassis, referring to the table of "Additional installation and removal information" (page 71) as needed.

19 Power up the replacement SST unit by pushing the power button on the front panel, then go to the SST console.

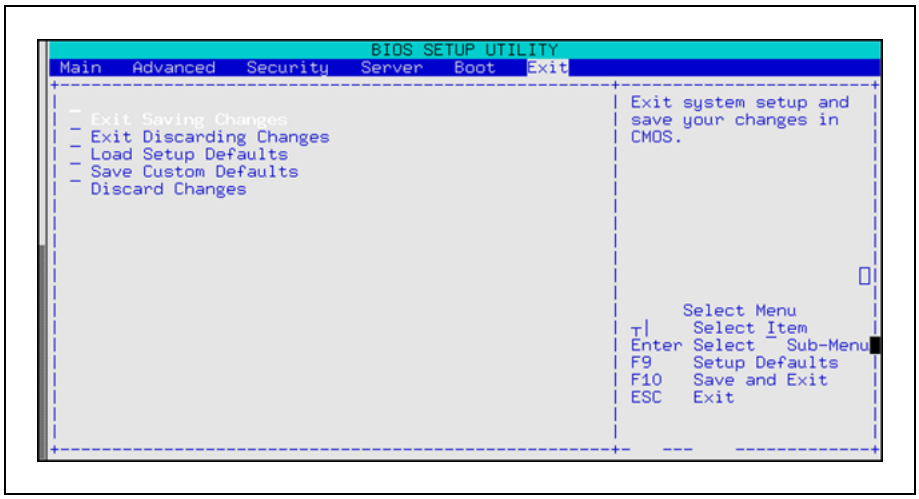


The green power LED lights and the SST unit boots attempts to boot from disk.

At the Session Server console

20 At the BIOS information screen, press the **<F2>** key to abort booting from disk and to enter the BIOS setup.

The main BIOS setup screen appears.



21 Verify that the BIOS on the new unit is configured properly by completing the procedure "Reconfiguring the SST BIOS" in *Session Server Trunks Configuration Management* (NN10338-511).

After this procedure is completed, the unit automatically reboots.

22 Complete the procedure "Reprovisioning the SST NCGL platform software" in *Session Server Trunks Configuration Management* (NN10338-511).

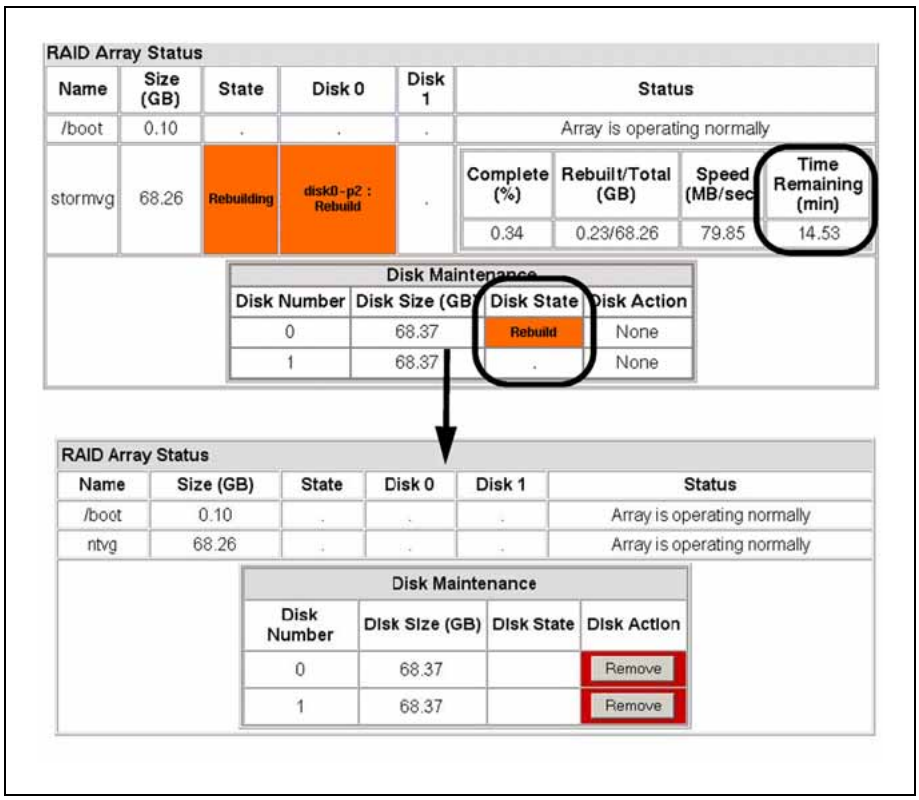
23 Complete the procedure "Upgrade/rollback/reinstall a Session Server application" in *Carrier Voice over IP Network Upgrade* (NN10440-450).

At the CS 2000 Session Server Launch Point

24 Access the CS 2000 NCGL Platform Manager GUI via your normal method (IEMS or console interface).

25 Go to the Disk Services page using procedure "Viewing the operational status of the NCGL platform" (page 48) and confirm that the newly replaced unit is rebuilding the disk drive array.

The RAID Array Status screen indicates that the array is rebuilding.



Wait the suggested time indicated in the Time Remaining field for the rebuild to complete, then continue with this procedure.

26 Execute procedure "Viewing SST alarms" (page 34) and ensure that all alarms raised related to this remove and replace activity are addressed and cleared.

27 Increase the size of /var/log to 4 GB (4000) for the inactive unit. For detailed steps, refer to the procedure "Increasing filesystem size" in *Session Server Trunks Configuration Management* (NN10338-511).

28 Repeat step 24 and step 27 for the active unit.

29 Determine the synchronization status of the two units using the procedure "Verify synchronization status of Session Server units" in *Session Server Trunks Security and Administration* (NN10346-611) to verify that both units are synchronized.

30 Execute the procedure "Enabling a system SwAct (Unjam)" in *Session Server Trunks Security and Administration* (NN10346-611).

Note: Executing this procedure generates an alarm clearing log XTS655.

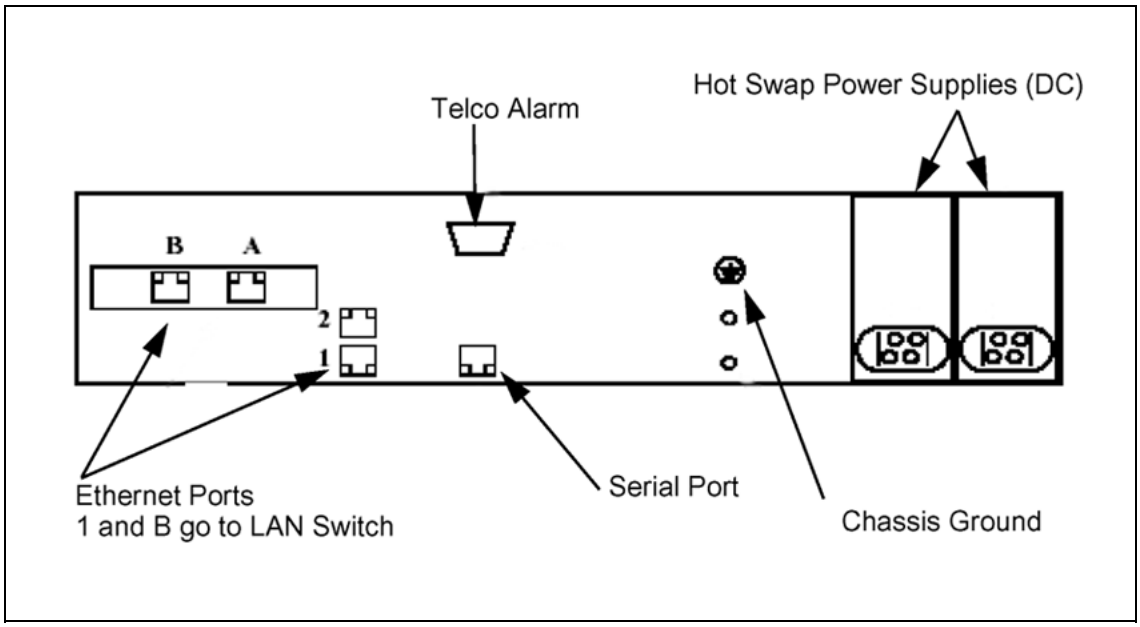
31 This procedure is complete.

—End—

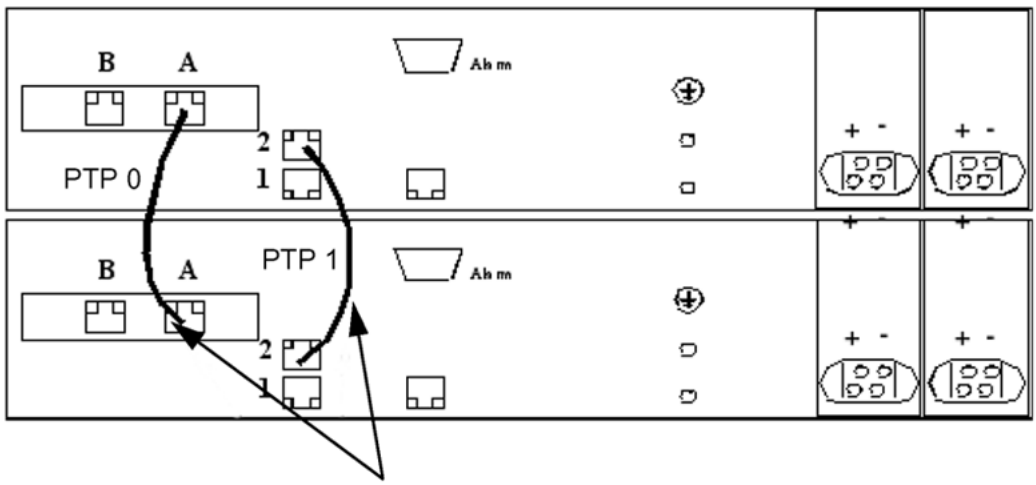
Additional installation and removal information

Use the following figures and table to assist you with removing and replacing an SST unit.

SST unit rear view of ports and ground connection



Crossover Cable connections between SST units



NTRX5145 Gigabit Ethernet Crossover Cables

Ethernet Ports

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

SST - SAM-F frame Cable Connections

Cable Part No.	Function	Connection From	Connection To
NTRX5198	Session Server Ground	Frame Gnd at top of the frame	Session Server unit 00 Gnd
NTRX5198	Session Server Ground Cable	Frame Gnd at top of the frame	Session Server unit 01 Gnd
NTRX5146	Power Cable	BIP P17	Session Server unit 01 Input A (top screws)
			SAM16 Feed A
NTRX5146	Power Cable	BIP P20	Session Server unit 01 Input B (top screws)
			SAM16 Feed B
NTRX5199	Power Cable	BIP P16	Session Server unit 00 Input A (top screws)
NTRX5199	Power Cable	BIP P19	Session Server unit 00 Input B (top screws)
NTRX5179	Alarm Cable	BIP P10	Session Server unit 00 Alarm
			Session Server unit 01 Alarm
NTRX5132	Ethernet Cable	PP8600	Session Server unit 00 Ethernet Port 1
NTRX5132	Ethernet Cable	PP8600	Session Server unit 00 Ethernet Port B
NTRX5132	Ethernet Cable	PP8600	Session Server unit 01 Ethernet Port 1
NTRX5132	Ethernet Cable	PP8600	Session Server unit 01 Ethernet Port B
NTRX5145	Ethernet Crossover Cable	Session Server 00 Ethernet Port 2	Session Server unit 01 Ethernet Port 2

Replacing an SST hard drive

Purpose of this procedure

Perform this activity in the event of a disk failure in the RAID 1-type disk array of a standby SST unit.

Limitations and restrictions

It is recommended that you schedule this procedure during periods of low traffic conditions.

Prerequisites

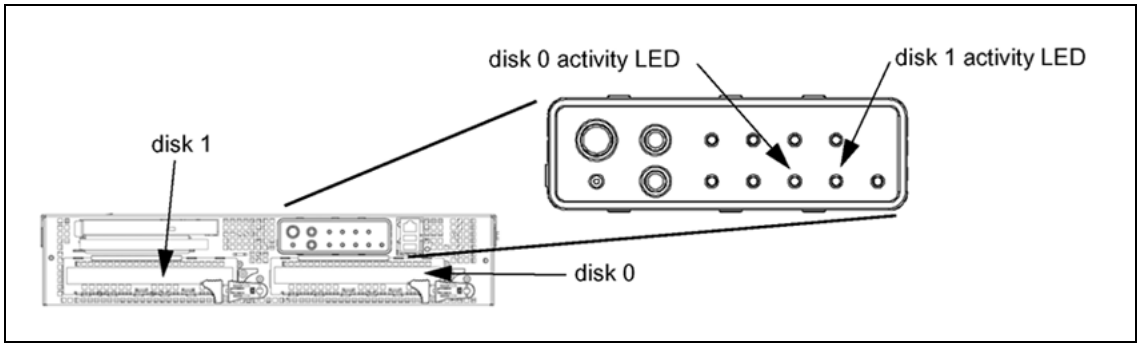
If applicable, ensure continued call processing by perform this procedure only on the standby unit. If the disk drive failure is on the active unit, perform a SwAct of the units using the procedure "Invoking a maintenance SwAct of the SST platform" found in the *Session Server Trunks Security and Administration* (NN10346-611).

Verify that a disk failure is reported by any of the following indicators:

- an XTS391 log report that indicates a physical disk has been removed from the array or a disk failure has occurred
- a major alarm raised
- the disk activity LED on the front panel of the SST chassis for a drive is red as shown in the following diagram. Refer to LED descriptions in the HP document HP Carrier-Grade Server cc3310 Product Guide (part number: cc3310_Product) for complete details.

Disk activity LED	Disk condition
off	no disk activity
green	disk is operating normally and is active
blinking green and red	disk is rebuilding
red	disk failure or disk is missing

Disk activity LEDs on SST front panel



Materials

This procedure requires one NTRX51GT -- 72 Gigabyte disk drive installed in its drive tray and one ESD wrist strap.

Action

Step	Action

At the CS 2000 NCGL Platform Manager on the active unit

1 Execute procedure "Inhibiting a system SwAct (Jam)" in *Session Server Trunks Security and Administration* (NN10346-611).

ATTENTION
Executing this procedure generates an alarm/log XTS300.

At the SST unit chassis

2 Determine which drive (either 0 or 1) failed in the unit. Refer to section "Alarms and LED fault indicators on the front panel" (page 19) and look for a lit red LED on the SST chassis front panel that would indicate the ID of the failed drive.

3 Complete procedure "Removing a hard drive from the NCGL operating system" (page 77).

4 Perform the hard drive replacement using procedures in the document *HP Carrier-Grade Server cc3310 Product Guide* (product number cc3310_Product).

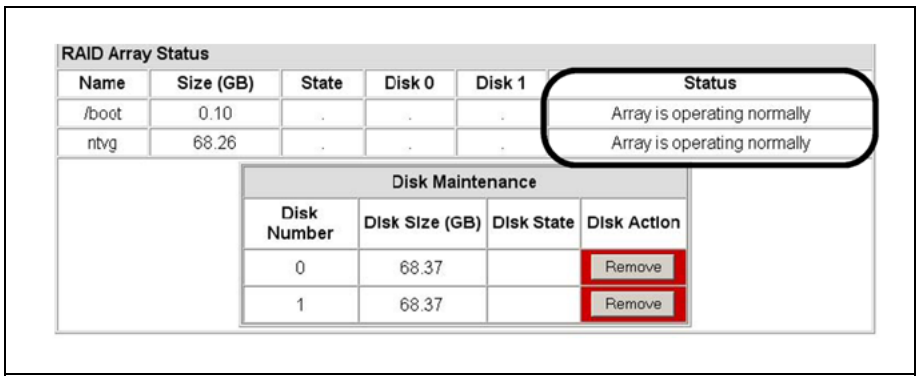
Once the disk drive is replaced, the SST unit immediately begins to rebuild the array. During the rebuild, the front panel LED for the disk drive alternates between red and green. If the SST chassis is wired to an external alarm system, a minor alarm is indicated with an amber LED.

If the disk is inserted into the SST chassis and the LED for the disk remains solid red for more than one minute after inserting the disk drive, remove then reinsert the disk drive.

At the CS 2000 NCGL Platform Manager on the active unit

5 Referring to procedure "Viewing SST alarms" (page 34), verify that all alarms related to this activity and the original disk failure condition have been cleared.

6 After the drive array has been fully rebuilt, the array status reports that the array is operating normally, as shown below. After all alarms related to the disk drive failure have been cleared, execute procedure "Verifying synchronization status" (page 63) to verify that the database for both units is synchronized.



7 Execute the procedure "Enabling a system SwAct (Unjam)" in *Session Server Trunks Security and Administration* (NN10346-611).

—End—

Removing a hard drive from the NCGL operating system

Purpose of this procedure

Perform this procedure to remove an instance of a hard disk drive from the NCGL operating system and the RAID array. This procedure should only be used as part of the high level activity "Replacing an SST hard drive".

Limitations and restrictions

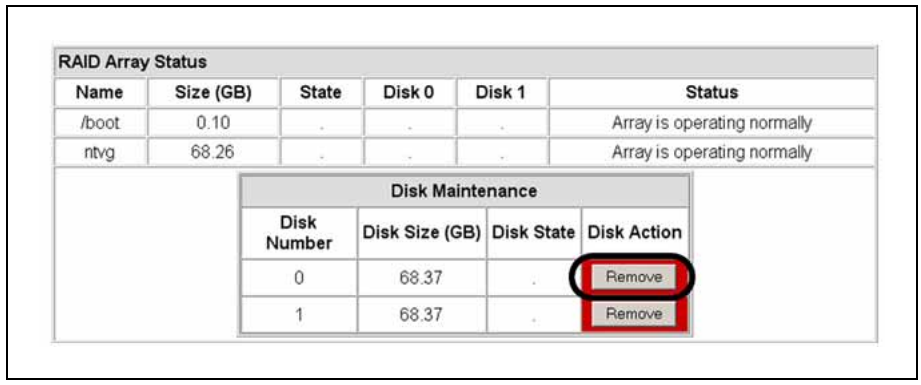
It is recommended that you schedule this procedure during periods of low traffic conditions.

Prerequisites

If applicable, ensure continued call processing by performing this procedure only on the standby unit, unless otherwise specified.

Action

Step	Action
	At an IEMS or client workstation
1	Log onto the inactive unit CS 2000 NCGL Platform Manager.
2	Click the **Disk Services** link. *The Platform Main Page menu is displayed.*
3	Determine which drive to remove from the array at the Disk Maintenance panel and click the applicable **Remove** button.
4	Click the **OK** button to verify removing the disk from the operating system.



The drive LED on the front panel changes to solid red and the operating system prepares for the disk to be removed.

A window appears indicating that the drive is being removed from the array.

Once the window disappears, the array status and disk maintenance areas are updated to reflect the removal of the disk.

The disk is now ready to be removed from the chassis.

5 Return to procedure "Replacing an SST hard drive" (page 74) to physically remove the hard drive from the unit.

—End—

Inserting a hard drive into the NCGL operating system

Purpose of this procedure

Perform this procedure to insert an instance of a hard disk drive into the NCGL operating system and the RAID array. This procedure should only be used as part of the high level activity "Replacing an SST hard drive".

Limitations and restrictions

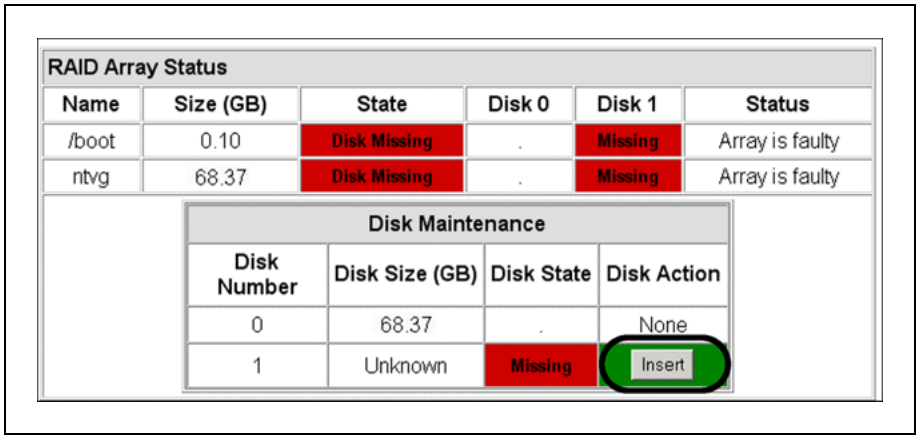
It is recommended that you schedule this procedure during periods of low traffic conditions.

Prerequisites

If applicable, ensure continued call processing by performing this procedure only on the standby unit, unless otherwise specified.

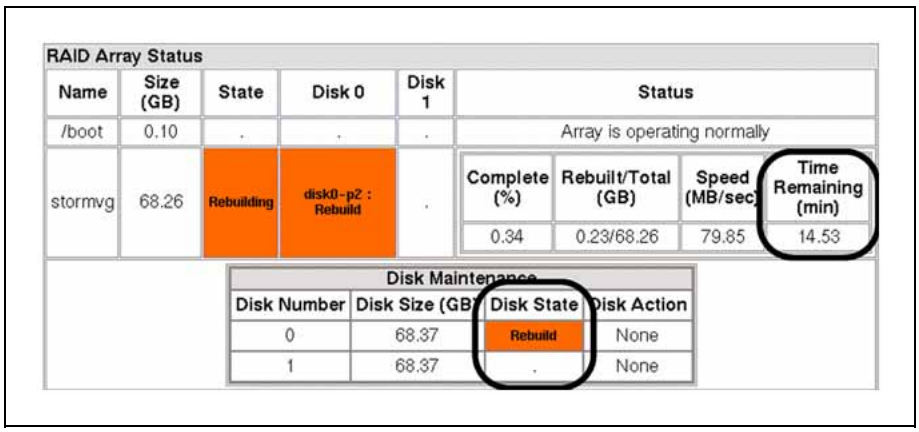
Action

Step	Action
	At the SST unit chassis
1	If applicable, log onto the inactive unit CS 2000 NCGL Platform Manager.
2	Click the **Disk Services** link. *The Platform Main Page menu is displayed.*
3	Select the disk to be inserted and click the **Insert** button to add the disk drive to the array and to begin rebuilding the array.



A window appears indicating that the insertion of the drive into the array is being performed.

4 After the disk insertion window disappears, use your browser refresh button and update the Disk Services page and the RAID Array Status panel.



RAID Array Status

Name	Size (GB)	State	Disk 0	Disk 1	Status
/boot	0.10	.	.	.	Array is operating normally
stormvg	68.26	Rebuilding	disk0-p2 : Rebuild	.	Complete (%): 0.34 / Rebuilt/Total (GB): 0.23/68.26 / Speed (MB/sec): 79.85 / Time Remaining (min): 14.53

Disk Maintenance

Disk Number	Disk Size (GB)	Disk State	Disk Action
0	68.37	Rebuild	None
1	68.37	.	None

The RAID Array Status screen indicates that the array is rebuilding. Additional XTS391 log reports indicate that a disk has been inserted to the array and the array is being rebuilt.

Wait the suggested time indicated in the Time Remaining field for the rebuild to complete, then continue with this procedure.

5 Return to procedure "Replacing an SST hard drive" (page 74) to physically remove the hard drive from the unit.

—End—

Replacing an SST CDRW/DVD-ROM drive

Purpose of this procedure

Use this procedure to replace a damaged or failed CD+RW/DVD drive in a standby SST unit.

Limitations and restrictions

Perform this procedure after physical damage to the CD+RW/DVD drive tray or a failure of the drive. A failure of the drive may be indicated by a failure to boot the unit from DVD-ROM, or if the SST unit fails to read a CD-ROM or DVD-ROM during an upgrade.

Prerequisites

To ensure continued call processing, perform this procedure only on the standby unit. If the drive failure is on the active unit, perform a SwAct of the units using the procedure "Invoking a maintenance SwAct of the SST platform" in *Session Server Trunks Security and Administration* (NN10346-611).

Materials

This procedure requires one NTRX51GQ — CD+RW/DVD drive installed in its drive tray and one ESD wrist strap.

Action

Step	Action

At the CS 2000 NCGL Platform Manager

1 Execute the procedure "Inhibiting a system SwAct (Jam)" in *Session Server Trunks Security and Administration* (NN10346-611).

ATTENTION
Executing this procedure generates an alarm/log XTS300.

2 Shut down the standby SST unit by completing the procedure "Halting (shutting down) an SST unit" in *Session Server Trunks Security and Administration* (NN10346-611).

At the front panel of the SST chassis

3 Perform the CDRW/DVD-ROM drive replacement using procedures in the document *HP Carrier-Grade Server cc3310 Product Guide* (part number: cc3310_Product).

4 Once the drive replacement is complete, press the power button to restore power to the chassis. Allow the unit to boot normally.

At the CS 2000 NCGL Platform Manager

5 After the unit has completed rebooting, refer to the procedure "Viewing SST alarms" (page 34), and verify that all alarms related to the drive failure condition and drive replacement have been cleared.

6 Execute the procedure "Verifying synchronization status of SST units" in *Session Server Trunks Security and Administration* (NN10346-611) to verify that both units are back in sync.

7 Execute the procedure "Enabling a system SwAct (Unjam)" in *Session Server Trunks Security and Administration* (NN10346-611).

—End—

Replacing an SST power supply

Purpose of this procedure

Use this procedure to replace an AC or DC power supply unit in an SST chassis. Each SST unit uses a redundant power supply system.

Limitations and restrictions

If the power supply failure is on the active unit, perform a SwAct of the units using the procedure "Invoke a maintenance SwAct of the SST platform" in *Session Server Trunks Security and Administration* (NN10346-611).

It is recommended that you schedule this procedure during periods of low traffic conditions.

Prerequisites

Verify that a power supply failure is indicated by:

- the power LED on the front panel indicates a fault condition in the power system. Refer to LED descriptions in the HP document *HP Carrier-Grade Server cc3310 Product Guide* (product number cc3310_Product) for complete details.
- the power supply LED at the rear of the power supply unit indicates a failure:

Rear power supply LED indicators

Power supply LED	Power supply condition
off	no power to any power supply units
amber	• no power to this power supply unit • power supply failure: over temperature (OTP), over voltage (OVP), over current (OCP), and under voltage (UV). • current limit -- applies to DC power supplies only
blinking green	power is applied to this power supply unit; only the standby power DC outputs are on
green	power is applied to this power supply and DC outputs are okay and on
blinking amber	power supply in alert condition - applies to AC power supplies only

Materials

This procedure requires one power supply, NTRX51GS for DC power or NTRX51NE for AC power, an ESD wrist strap, a small flat-bladed screwdriver, and a #2 Phillips screwdriver.

Action

ATTENTION
To maintain hot-plug capability, ensure that an active AC or DC power supply module is in the adjacent slot before replacing a power supply module.

DANGER
Use caution when disconnecting power from the chassis.

WARNING
Use caution when handling the power supplies. Attach an ESD wrist strap to a chassis or frame grounding point.

Replacing a DC power supply

Step	Action

At the CS 2000 NCGL Platform Manager

1 Execute the procedure "Inhibiting a system SwAct (Jam)" in *Session Server Trunks Security and Administration* (NN10346-611).

ATTENTION
Executing this procedure generates an alarm/log XTS300.

At the SST chassis

2 Perform the AC or DC power supply replacement using procedures in the document *HP Carrier-Grade Server cc3310 Product Guide* (product number cc3310_Product).

The procedure is available on the HP web site and can accessed as follows:

- Access www.hp.com.
- Search for "HP Carrier-Grade Server cc3310 Produce Guide".

- Under Product Quick Links, click "Product Manuals".
- Open "HP Carrier-Grade Server cc3310 Product Guide"
- Go to the section "Replacing Power Supply Modules".

If you cannot locate this procedure, contact your next level of support before proceeding.

At the CS 2000 NCGL Platform Manager

3 Referring to procedure "Viewing SST alarms" (page 34), verify that all alarms related to this failure condition have been cleared.

4 After all alarms related to the disk drive failure have been cleared, execute the procedure "Enabling a system SwAct (Unjam)" in *Session Server Trunks Security and Administration* (NN10346-611).

—End—

Restoring SST

Purpose of this procedure

Use this procedure to restore a backup copy of critical files to a unit.

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.

Prerequisites

You must have secure file transfer access, such as scp, to the unit from a remote host if the backup file is stored on a remote host.

Backups are also stored locally on each unit in directory **`/data/bkresmgr/backup`**.

CAUTION
Both units must be free of any Session Server Manager patches before the database is restored. This is accomplished by reinstalling the current version of the SIP Gateway application software (performed in step 1 below). It is not necessary to remove NCGL patches.

Action

Step	Action

At the NCGL CLI or IEMS client

1 If either unit has Session Server Manager patches applied, reinstall the current application software on both units by performing the procedure "Upgrade/rollback/reinstall an SST application" in *Nortel Carrier Voice over IP Upgrade and Patches* (NN10440-450).

ATTENTION
Do not reapply any Session Server Manager patches after the reinstall.

From the remote server where the backup database file is located

2 If the backup is stored on a remote host, copy the backup file to the unit.

Backup files are unit-specific. Ensure the backup file being copied from the remote host is the file that was originally created on the unit.

To use a secure copy, type

scp <backupfile> mtc@ <ip_address> : <dest_dir>

where

backupfile is a value like unit0.backupfile.2005-04-12_17-10.tgz and is identified by the hostname, date, and time that the backup occurred
ip_address is the IP address of the unit
dest_dir is the location to put the backupfile and is either blank to place it in /users/mtc, or a full path such as /data/bkresmgr/restore

The database file is copied to the target unit. If the local workstation is not on the CS LAN, copy the backup file to the server hosting the CS 2000 Management Tools first, and then transfer it between the server hosting the CS 2000 Management Tools and the SST unit.

At the NCGL CLI or IEMS client

3 Log in to the unit and change to the root user.

4 If the backup file was not transferred directly to /data/bkresmgr/restore, then move the backup file:

mv /users/mtc/<backupfile> /data/bkresmgr/restore

If restoring a local backup, the backup file is located in **/data/bkresmgr/backup**.

5 Change directory to the restore directory:

cd /data/bkresmgr/restore

6 Uncompress the backup:

tar xvzf <backupfile>.tgz

A listing of the files is printed to the screen and the files to restore are located in /data/bkresmgr/restore/data/bkresmgr/temp.

7 Change directory to the files:

cd /data/bkresmgr/restore/data/bkresmgr/temp

Jam the inactive unit and suspend call processing

8 Repeat the previous steps in this procedure on the mate unit.

At the CS 2000 Session Server Manager or IEMS client

9 Select Session Server > Maintenance > Platform > Node Maintenance from the left side menu.

The Node Maintenance panel opens in the right side.

10 Click Jam.

Two JInact alarms are raised.

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

The SIP Gateway Maintenance page opens in the right side.

12 Click Lock.

13 Click Suspend.

14 Perform any of the following restore activities and then perform "Unsuspend call processing and Unjam the inactive unit", later in this procedure.

- "Restore the database" (page 88)
- "Restore system data" (page 89)
- "Restore web files" (page 90)
- "Manually restoring security-related files" (page 92)These files are stored in a separate backup file, but restoring them as part of this procedure avoids an additional web server restart

Restore the database

CAUTION
Perform the following steps only if the database corruption has occurred on both units. If so, the database must be restored on the active unit.

At the NCGL CLI or IEMS client

15 Copy the database files:

```
cp -i solid.db
/opt/apps/database/solid/backup/solid.db

cp -i solid.ini
/opt/apps/database/solid/backup/solid.ini

cp -i solmsg.out
/opt/apps/database/solid/backup/solmsg.out
```

16 Set the attributes for the files in the backup directory:

```
chown soliddb /opt/apps/database/solid/backup/*
chgrp adm /opt/apps/database/solid/backup/*
chmod 700 /opt/apps/database/solid/backup/*
```

17 Restore the backup files:

```
/opt/apps/database/solid_install/restorebackup.sh
```

The following status is printed to the screen. The database on the inactive unit is synchronized to the restored database on the active unit.

```
Restoring database from backup
Stopping dbwatchdog.sh:                                    [  OK  ]
Stopping soliddb.sh:                                       [  OK  ]
Starting soliddb.sh:                                       [  OK  ]
Solid SQL Editor (teletype) v.04.10.0139
(C) Copyright Solid Information Technology Ltd 1993-2004
Execute SQL statements terminated by a semicolon.
Exit by giving command: exit;
Connected to 'tcp 1315'.
admin command 'hsb set primary alone'
       RC TEXT
       -- ----
        0 HotStandby server set to PRIMARY ALONE.
1 rows fetched.

admin command 'hsb netcopy'
       RC TEXT
       -- ----
        0 Copy started.
1 rows fetched.

SOLID SQL Editor exiting.
Starting dbwatchdog.sh:                                    [  OK  ]
```

18 If the database is the only item to restore, then unsuspend, unlock, and unjam the inactive unit. For assistance, refer to "Unsuspend call processing and Unjam the inactive unit," later in this procedure.

Restore system data

At the NCGL CLI or IEMS client

19 Copy the necessary files:

```
cd /data/bkresmgr/restore/data/bkresmgr/temp
cp -i hosts /etc
cp -i passwd /etc
cp -i group /etc
cp -i ntp.conf /etc
cp -i shadow /etc
cp -i ifcfg-eth0 /etc/sysconfig/network-scripts
cp -i netnodes /etc/sysconfig
```

```
cp -i ssh_host_dsa_key.pub
/opt/base/synch_local/common/etc/ssh

cp -i ssh_host_key.pub
/opt/base/synch_local/common/etc/ssh

cp -i ssh_host_rsa_key.pub
/opt/base/synch_local/common/etc/ssh
```

20 Set the permissions on the restored files:

```
chmod 755 /etc/hosts

chmod 755 /etc/passwd

chmod 755 /etc/shadow

chmod 755 /etc/group

chmod 755 /etc/sysconfig/netnodes

chmod 755
/etc/sysconfig/network-scripts/ifcfg-eth0

chmod 644
/opt/base/synch_local/common/etc/ssh/ssh_host_key.pub

chmod 644
/opt/base/synch_local/common/etc/ssh/ssh_host_dsa_key
.pub

chmod 644
/opt/base/synch_local/common/etc/ssh/ssh_host_rsa_key
.pub
```

21 Repeat the previous two steps on the mate unit.

Restore web files

At the NCGL CLI or IEMS client

22 Copy the files:

```
cd /data/bkresmgr/restore/data/bkresmgr/temp

cp -i redirect*.jsp
/opt/apps/webint/jakarta-tomcat-4.1.30/webapps/
<tag_name>/jsp

cp -i redirect_apps.php
/usr/local/apache/htdocs
```

Unsuspend call processing and Unjam the inactive unit

At the CS 2000 Session Server Manager or IEMS client

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

24 Click Unsuspend.

25 Click Unlock.

26 Select Session Server > Maintenance > Platform > Node Maintenance from the left side menu.

27 Click Unjam.

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

—End—

Manually restoring security-related files

Security related files are not stored in the automatically generated backup to guard against compromise of the keys in the event that a backup is stolen or misplaced.

Restored security files must be the same on both units of a node.

Locate the manual backup of security related files and restore the following files:

- /opt/base/share/ssl/certificate.keystore
- /opt/base/share/ssl/gen_cert.txt
- /opt/base/share/ssl/server.crt
- /opt/base/share/ssl/server.key
- /opt/base/share/ssl/trusted.crt

ATTENTION

If the unit is running SN09 software, optionally restore the files listed above to a location such as /users/mtc, and then use the cert_mgnt tool with option 3, Import certificates and private key, to restore the files to /opt/base/share/ssl and set the permissions correctly.

- /opt/base/synch_local/common/etc/ssh/ssh_host_dsa_key
- /opt/base/synch_local/common/etc/ssh/ssh_host_key
- /opt/base/synch_local/common/etc/ssh/ssh_host_rsa_key

Step	Action

At the NCGL CLI or IEMS

1 Login as the root user.

2 Change directories to the location where the backup of the security certificates are stored:

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

where

SNxx_ddmmyyyy is the name of the backup directory

```
cd /opt/base/share/ssl/SN09_12102005
```

3 Verify the contents of the backup directory:

```
ls -l
```

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
```

4 Determine your next step:

If	Do
the backup directory is empty or contains files other than those shown in the previous example	You are either in the wrong backup directory or you did not properly back up the security certificates. If necessary, contact Nortel GNPS for assistance. This procedure is complete.
the backup directory contains files similar to the display and the running software load is SN09	Run **cert_mgnt** and choose option 3. This restores the files and sets permissions correctly. This procedure is complete.
the backup directory contains files similar to the example shown in the previous step and the running software load is older than SN09	Continue to step 5to copy the files and set permissions manually.

5 Copy the files to the /opt/base/share/ssl directory:

```
cp * /opt/base/share/ssl
```

ATTENTION
This step overwrites the current security certificates on this unit.

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

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

7 Verify the contents of the backup directory were restored:

```
ls -l
```

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
```

File size values vary.

8 Set the permissions for the restored files:

```
chown root:root *
chmod 644 server.crt
chmod 644 gen_cert.txt
chmod 600 certificate.keystore
chmod 600 server.key
chmod 644 trusted.crt
```

9 Perform the step "Jam the inactive unit and suspend call processing" in "Restoring SST" (page 86).

10 Enter the following commands to restart the applications that use the restored files:

```
/usr/local/apache/bin/apachectl restart
/opt/apps/webint/tomcatd restart
/etc/init.d/sshd restart
```

11 Perform the steps in "Unsuspend call processing and Unjam the inactive unit" in "Restoring SST" (page 86)

12 Repeat this procedure on the mate unit.

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

—End—

Appendix A
New SST alarms for SN09U release

The following table provides a description of all new SST alarms introduced in the SN09U release.

New SST alarms for SN09U release

Alarm	Level	Description	Action
SIPC322 SIP CallP <hostname> GcpListenerRecvFromFaileed	Major	This alarm indicates that a UDP read error was detected by the GCPListener task.	While this alarm is active, it indicates that the SST is not receiving UDP messages from the DPT GWCs. The customer should switch back to the inactive SST server.
	None	This alarm is cleared on the next successful read from this UDP socket.	None.
SIPC325 SIP CallP <hostname> Number of unresponsive SIP Server IPs exceed <level> threshold	Critical > 85% loss Major 51% > 84% loss Minor 1% > 50% loss	These alarms are raised when the SST detects a loss of signaling to one or more remote SIP servers. Each of the three categories; Critical, Major, and Minor, indicates the percentage of remote IP addresses that are not responding to the	For every remote IP address which loses a heartbeat, a corresponding SIPC625 log is created. Refer to *Carrier Voice over IP Fault Management Logs Reference Volume 3* (NN10275-909V3) for a description of the SIPC625 log.

Alarm	Level	Description	Action
		OPTIONS heartbeat.	This log contains the remote IP address which is not responding to the OPTIONS heartbeat. Check the status of the remote SIP servers identified in the SIPC625 logs and the signaling paths from the SST to the remote SIP servers.

Carrier VoIP

Session Server Trunks Fault Management

Publication: NN10332-911
Document status: Standard
Document version: 04.02
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

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