Session Server Fault Management

What’s new in (I)SN08

The following features are covered in the SN08 release of this NTP:

- Feature A00007270 - This feature provides for Overload Controls on the Session Server SIP Gateway application. Most of this feature is not customer visible; however, changes to log SIPC310 have been made to support this feature.
- Feature A00006893 - This feature provides TLS security on the signalling paths (but not the call content) between the Session Server-SIP Gateway application and a similarly configured remote SIP application server or call server. Logs supporting TLS security and security certificate management are covered in this NTP.

Fault management strategy overview

The Session Server 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 Session Server 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)

> ***Note:*** Because Session Server can be configured to transfer log reports to the OSS network, the logs reports may be available to Integrated EMS or other 3rd 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 Session Server unit (the standby unit only). For instructions on replacing individual field replaceable units (FRUs) that make up a Session Server 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 management tools and utilities

Fault management for the Session Server is provided by the following interfaces:

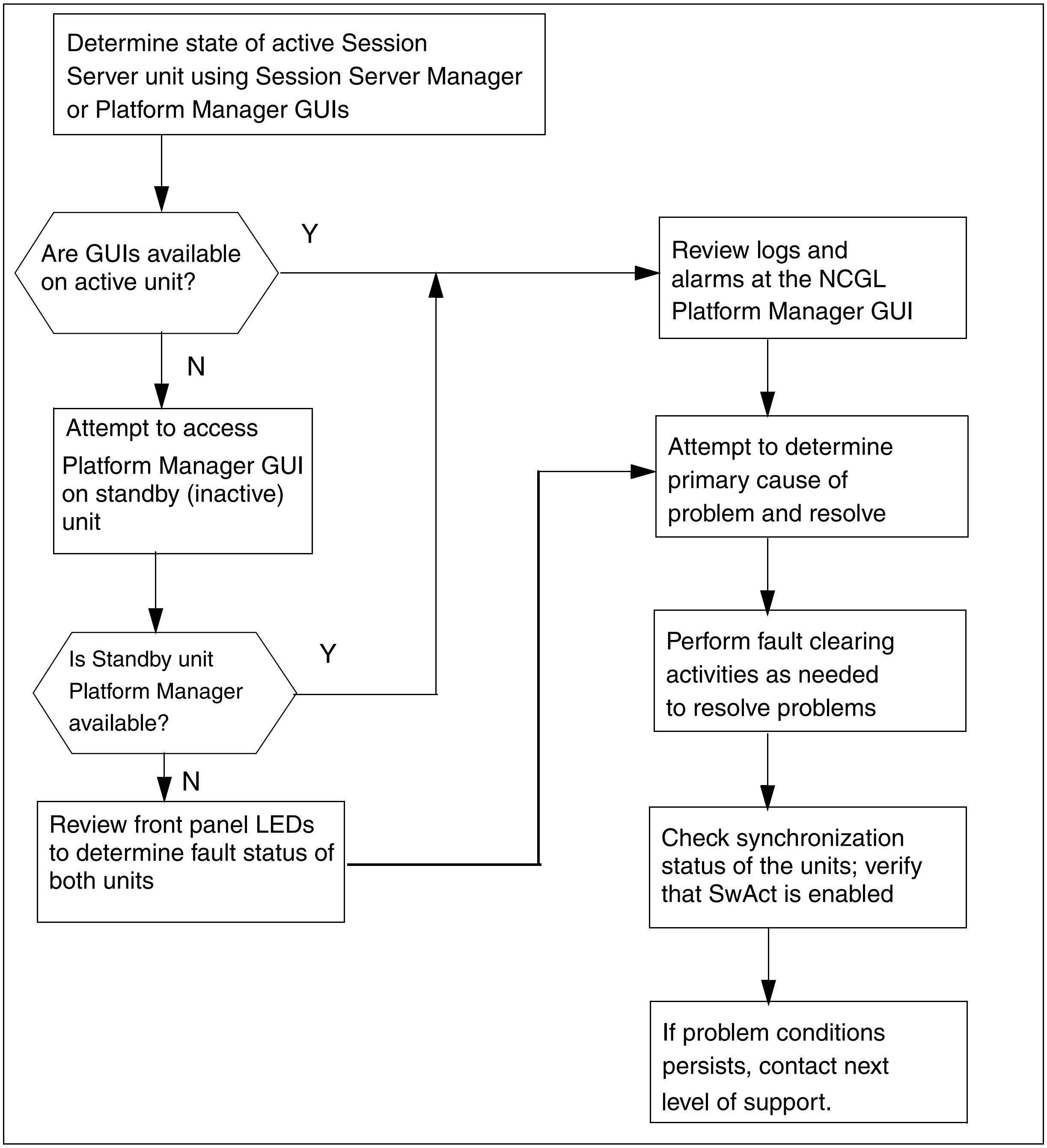
- CS 2000 NCGL Platform Manager
- CS 2000 Session Server Manager
- Session Server platform CLI (command line interface) or console

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

Fault handling and correction on the Session Server node

The following flowchart shows the overall process for performing fault handling on the Session Server platform:

Session Server fault management task flow


Determine state of active Session Server unit using Session Server Manager or Platform Manager GUIs
Are GUIs available on active unit?
Y
N
Attempt to access Platform Manager GUI on standby (inactive) unit
Is Standby unit Platform Manager available?
Y
N
Review front panel LEDs to determine fault status of both units
Review logs and alarms at the NCGL Platform Manager GUI
Attempt to determine primary cause of problem and resolve
Perform fault clearing activities as needed to resolve problems
Check synchronization status of the units; verify that SwAct is enabled
If problem conditions persists, contact next level of support.

Fault handling by the Session Server platform

The following table provides a summary of the fault handling behavior of the Session Server node (both platforms) 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.

Session Server platform fault handling-system and manual interventions

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.

Session Server platform fault handling-system and manual interventions

Fault Event	Action
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 Core

In the Core, the association of a trunk group to an access link is defined in Core 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. Since the Core has no direct communication with the Session Server, it is dependent on receiving link status information from the SIP-T GWCs (gateway controllers), that receive *Access Link Status* messages from the Session Server and pass them on to the Core.

The status of the access link on the Session Server is determined using a link auditing mechanism. Any change in a link's status detected by the Session Server is immediately propagated to each SIP-T GWC, then to the Core. As long as there is stable communication between the Core, at least one SIP-T GWC and the Session Server, the status of a SIP-T trunk in the Core should mirror that of its associated access link.

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

- On the Session Server, the access link associated with the trunk must be mapped to a Remote SIP Server.
- On the Session Server, 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 Session Server 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 Session Server 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 Session Server application administrative state must be UNLOCKED.
- On the Core, 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 Session Server 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 Core, 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 Session Server 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 Core and the Core changes the trunk group status to SYS.

If a situation occurs where there are no longer any in-service SIP-T GWCs, the Core changes the state of the trunk group to SYS. This is the only time the Core undertakes unsolicited action to remove a link from service; otherwise, link status in the Core is completely under the control of the Session Server. 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 Session Server sends an Access Link Status message to report the state change.

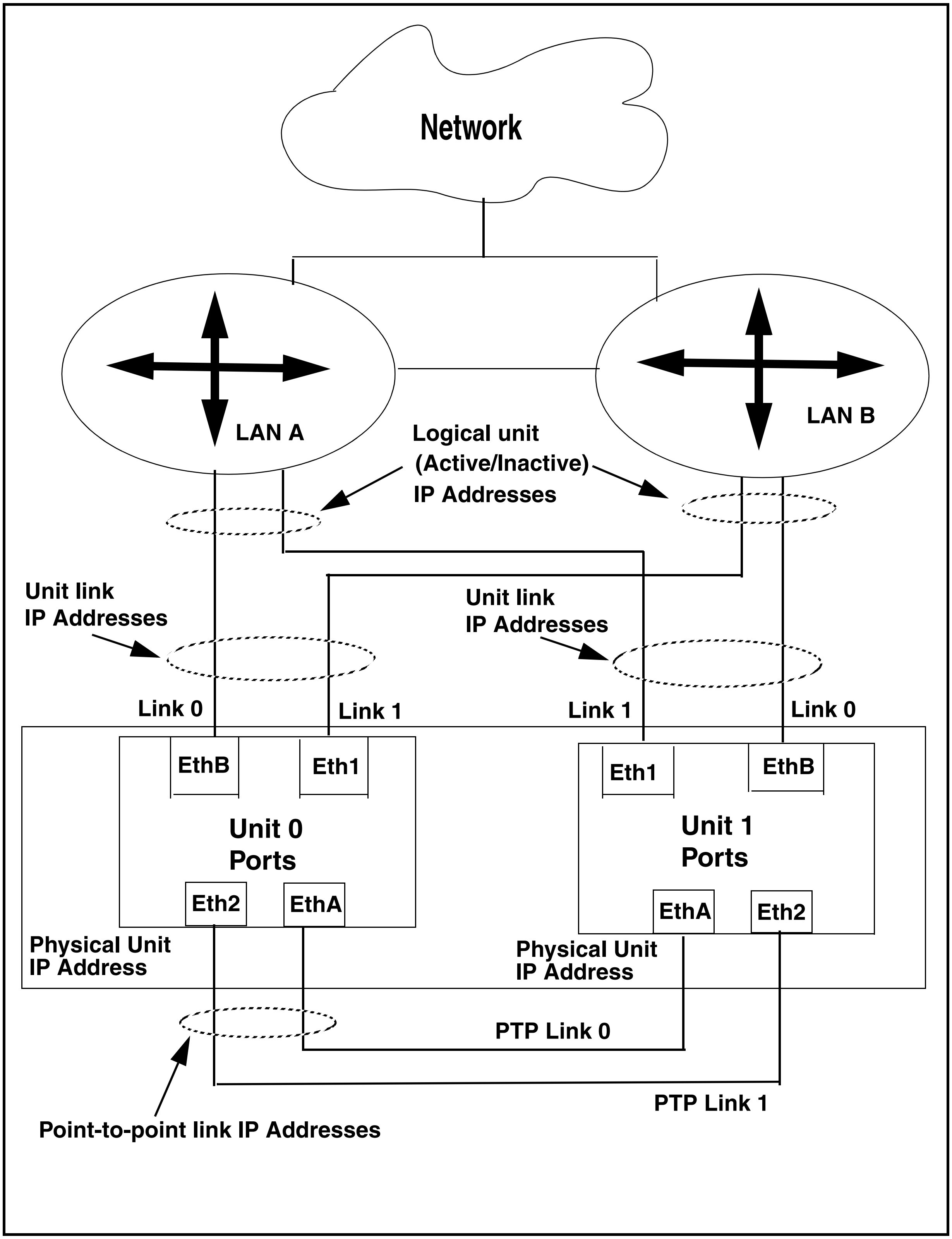
If the Session Server goes out of service due to a system failure or because of improper shutdown (which would disrupt the ability to send the Access Link Status message to the SIP-T GWCs), all in-service SIP-T trunks associated with any access links on the Session Server remain in-service.

Troubleshooting point-to-point ethernet links

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

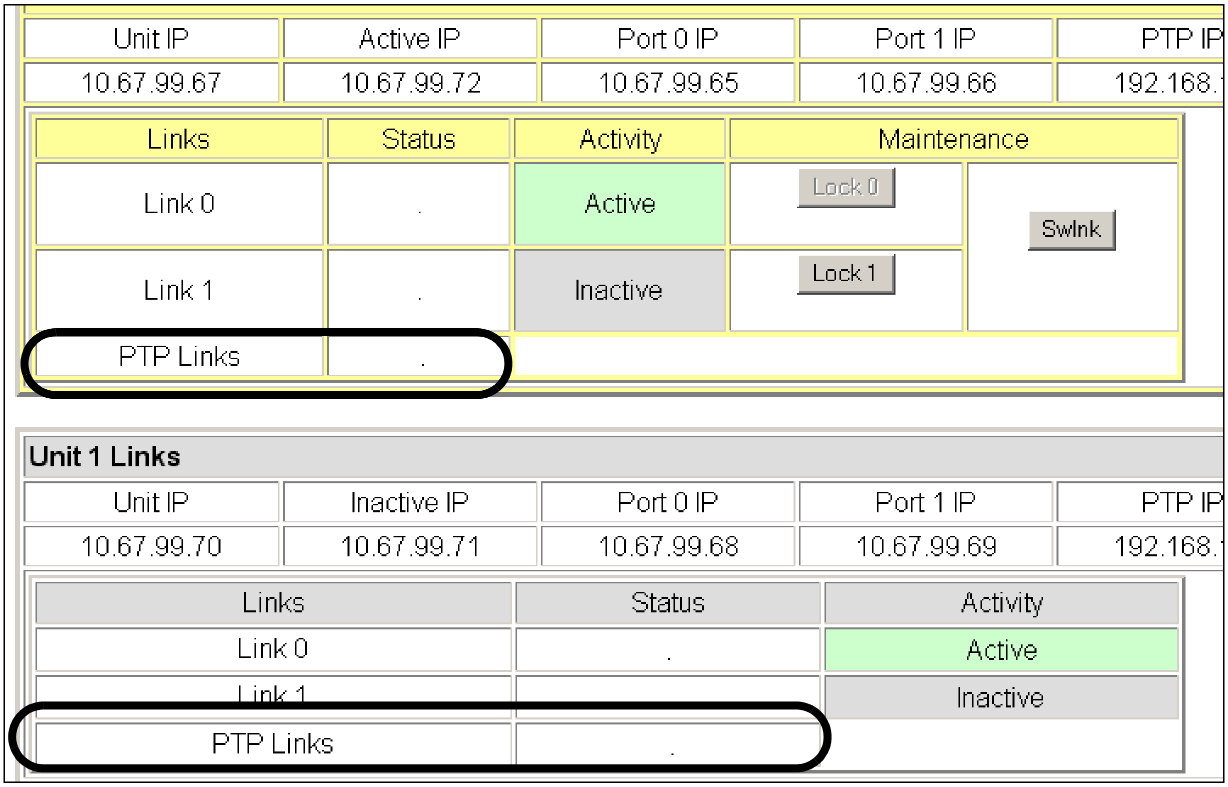
The following figure shows all port and link connections for both Session Server units. Port ethB of each unit is connected directly to a LAN switch, while port eth1 is connected to the redundant LAN switch. Ports ethA and eth2, used for the PTP links on each unit are cross-connected to the mate ports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



Unit IP	Active IP	Port 0 IP	Port 1 IP	PTP IP
10.67.99.67	10.67.99.72	10.67.99.65	10.67.99.66	192.168.1

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

Unit 1 Links

Unit IP	Inactive IP	Port 0 IP	Port 1 IP	PTP IP
10.67.99.70	10.67.99.71	10.67.99.68	10.67.99.69	192.168.1

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

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;
```

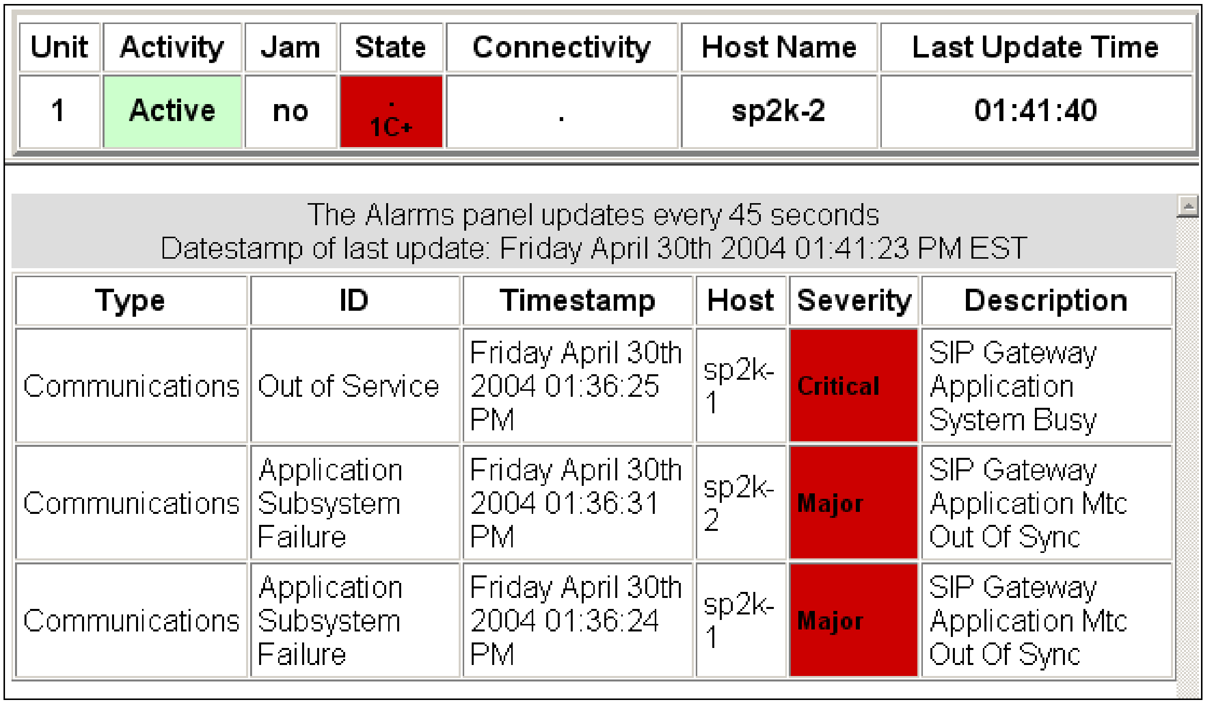
The following is an example of the alarm that is generated when both PTP links go down. The section of the alarm message in bold highlights the key difference from the alarm message raised when a single PTP link is down:

```
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;
```

Monitoring and analyzing alarms

The Session Server platform, along with the SIP Gateway application to generate alarms. These alarms can be viewed on the CS 2000 Session Server Manager's 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 Integrated EMS Alarm Manager view. Although the alarm information is organized and presented differently in the Integrated EMS Alarm Manager, the same data is made available. Refer to the Integrated EMS Fault Management NTP, NN10334-911, for information about viewing Session Server alarms

Alarms provide notification that a system hardware or software-related 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 Session Server node and its connectivity with the network. Administration of the network elements requires monitoring for alarms and checking that functions continue without interruption.

The Session Server 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 Session Server, associated GWCs, gateways or other related network components.

Alarm types

There are 5 CCITT X.733 alarm types used by the Session Server 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 seen on Session Server 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
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

Alarm IDs and descriptions

ID	General Description	ID	General Description
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[1]
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
116	Unauthorized Access Attempt	117	Unexpected Information
118	Unspecified Reason		

[1] ITU-T X.733 alarm ids from 58 to 100 are reserved - not assigned yet

Alarm timestamp

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

Alarm host

This field shows the Session Server unit 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 from Session Server to an SNMP server

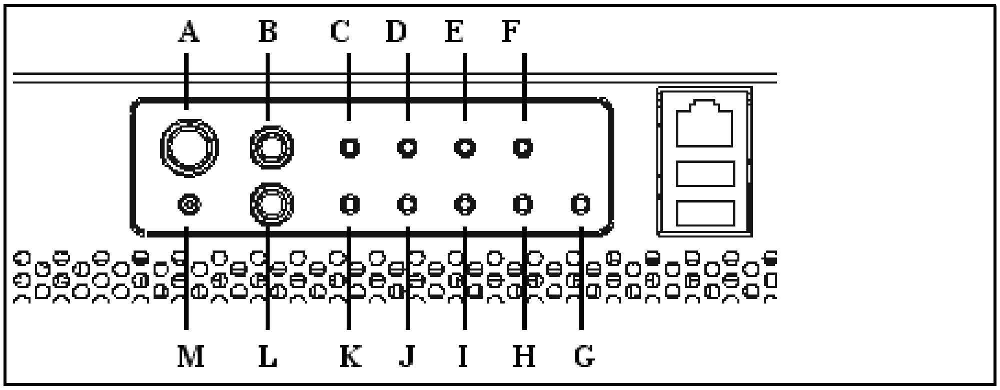
Depending on your site network configuration, Session Server alarms may be directed to an SNMP server such as the Integrated EMS server rather than to the alarms view of the Session Server GUIs. Trouble alarms must then be viewed using the available SNMP server's alarm viewing tool (like the Integrated EMS GUI).

If an SNMP server is defined (using the commish tool) for receiving alarms, then the Session Server does not display logs associated with those trouble alarms in the logs view of the Session Server GUI.

Alarms and LED fault indicators on the front panel

Along with being indicated in the Session Server GUI alarm pages, an alarm of any severity on the Session Server platform triggers an LED alarm indicator on the front panel. The alarm LED reflects the most critical alarm in the system. So, if you have a major alarm and a minor alarm, the major LED lights.

Front panel view of LED indicators and switches



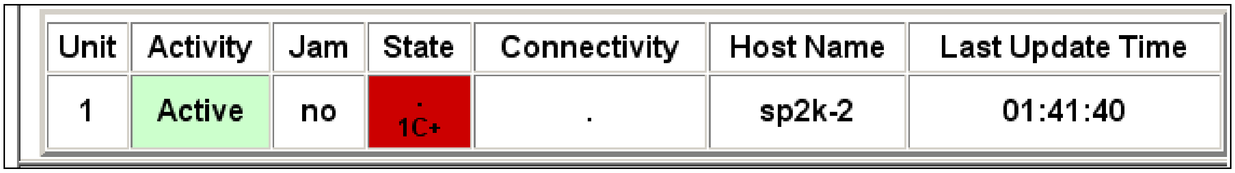
LED or Switch	Feature Indication	Description
	Front Panel Switches	
A	Power switch	Toggles the system power on the unit.
B	Reset switch	Resets the system.
L	ID switch	Toggles the system ID LED. For details, refer to the HP Carrier-Grade Server cc3310 Product Guide, HP part number: cc3310_Product
M	NMI switch	Asserts a Non-maskable interrupt to the baseboard. For details, refer to the HP Carrier-Grade Server cc3310 Product Guide, HP part number: cc3310_Product

LED or Switch	Feature Indication	Description
Front Panel Alarm LEDs		
C	Critical (amber or red)	When continuously lit, indicates the presence of a critical system fault. An example could be the loss of a large section of memory, or other corruption, that renders the system not operational.
D	Major (amber or red)	When continuously lit, indicates the presence of a major system fault. The system can continue to operate but in a degraded fashion (reduced performance or loss of fault-tolerance). An example could be the loss of one of two mirrored disks.
E	Minor (amber)	When continuously lit, indicates the presence of a minor system fault.
F	Power (amber)	When continuously lit, indicates the presence of a power system fault.
Front Panel Status LEDs		
G	Disk 0 Activity/Fault LED (green/amber or red)	Indicates disk 0 hard drive activity when green, or a disk 0 hard drive fault when amber or red.
H	Disk 1 Activity/Fault LED (green/amber or red)	Indicates disk 1 hard drive activity when green, or a disk 1 hard drive fault when amber or red.
I	Main power LED (green)	When continuously lit, indicates the presence of DC power in the server. The LED goes out when the power is turned off or the power source is disrupted.
J	NIC0/NIC1 activity LED (green)	Indicates activity on the network interface ports.
K	Server ID LED (white) controlled by LED switch	Used by maintenance personnel to identify which server unit requires fault management. LED stays full on.

Session Server unit-level alarm states and severity

The alarms page displays alarm info for each of the Session Server 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 on page 20.

Example

Two critical alarms in a particular alarm state display as a red button with “2C.”

Two critical alarms and one warning in a particular alarm state display as a red button with “2C+.”

One major alarm, one minor alarm, and one warning in a particular alarm state display as 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 Panel sort order cannot be modified. It defaults to sorting by alarms severity, then by time. The Alarms Panel also does not support filtering of alarms.
- The Alarms Panel 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 Session Server system date/time are changed after an alarm is raised, the Alarms Panel does not update its timestamps. The timestamps shown at the Alarms Panel were those current at the time that the alarms were raised.
- The Alarms Panel 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 Panel does not update its values in the description field. The threshold values shown at the Alarms Panel 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.

Auditing of call processing

The Session Server has automated callp auditing services running constantly that monitor for the following conditions:

- when contact with the database on the active Session Server 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 on the Session Server:

Procedure	Hardware platform or SIP GW application	Page
View Session Server alarms from the Session Server Manager or NCGL Platform Manager	All	35

Monitoring and analyzing logs

A log report is a record of a message that Session Server platform NCGL or the SIP Gateway application generates. Some logs are generated whenever a significant event has occurred that forces an alarm to be raised or cleared. Other logs are generated for informational purposes only.

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, time-stamp, severity, and description.

The following log types are generated on the Session Server:

- customer logs located at /var/log/custlog

Session Server has the capability for the SIP Gateway application or the NCGL platform to generate customer logs associated with alarms. Customer logs can be any of the following types: SIPC, SIPM, CRTM, SIPS, DBSE, SIPGW and XTS. Customer logs are generated to the local custlog file. Saved as ASCII-based text, in CSV format, log data can be reviewed, copied and printed. Log files can also be loaded into a spreadsheet application for further analysis.

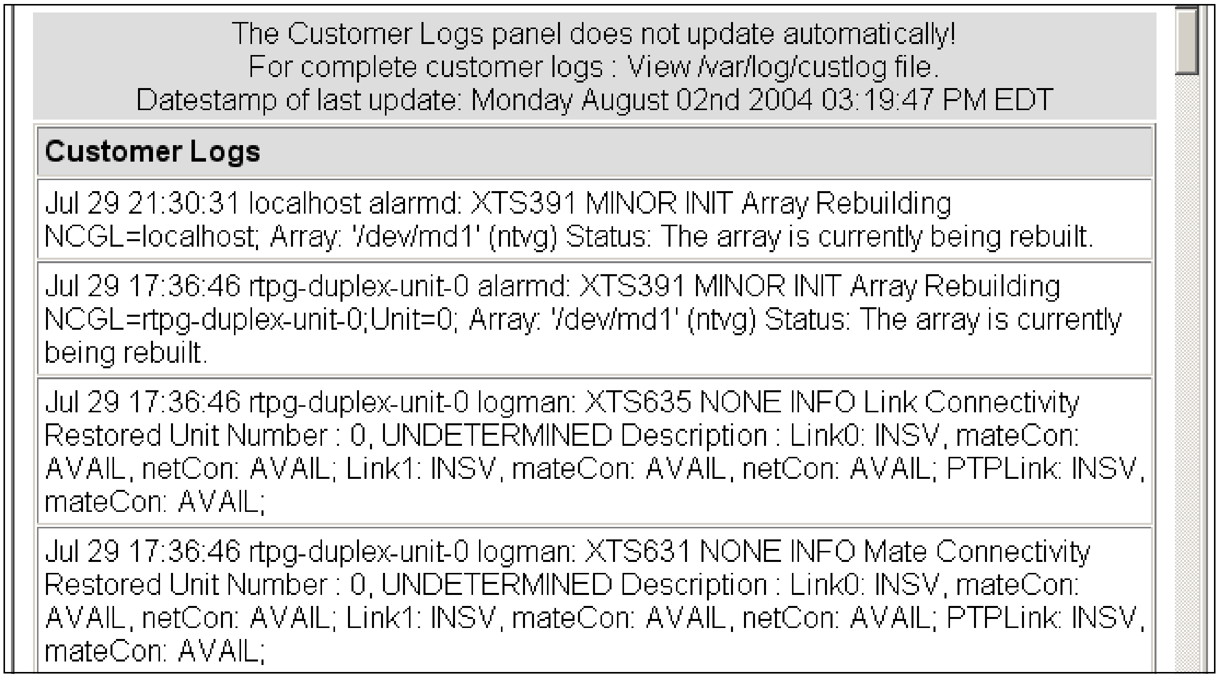
Session Server can be configured to alter what log information is written to the local custlog file by redirecting log information to a remote log server and SNMP server using the NCGL commissioning tool.

If Session Server is configured to transfer SNMP alarm traps to an OSS network, log reports related to the raising or clearing of alarms are only available on the Integrated EMS or other 3rd party OSS application, rather than on the logs view of the Session Server GUIs.

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

The following sample logs view is generated by the CS 2000 Session Server Manager. The logs view 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 GUI



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 you defined an SNMP server to receive alarms during commissioning, 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 Integrated EMS 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 local Session Server GUIs.

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 Mbytes. 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 Session Server 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 Session Server

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 Session Server, and is also forwarded to the Integrated EMS 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

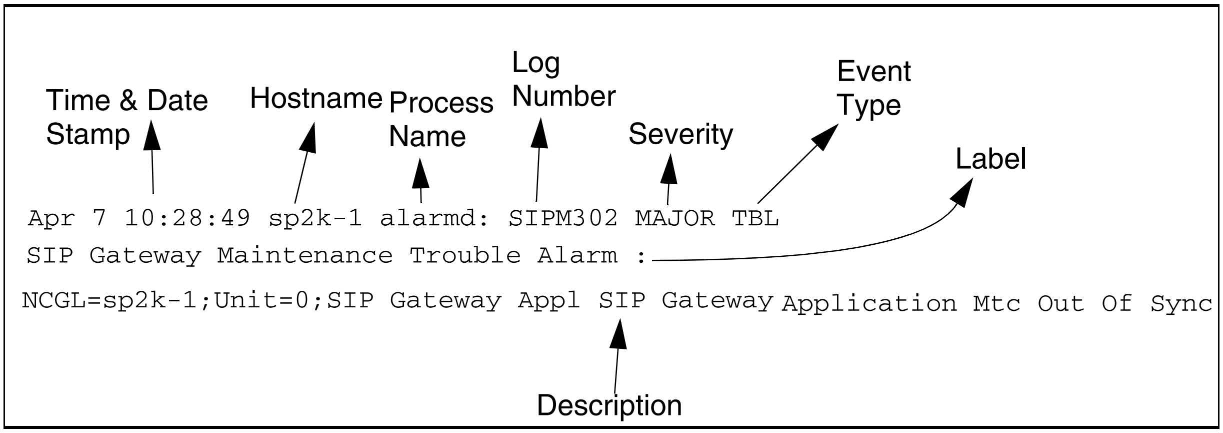
Unless alarms are redirected to an SNMP server, every alarm that is raised by the NGCL operating system has an associated XTS300-series log generated. Once the alarm condition is cleared, a complementary XTS600-series log is generated.

Customer log information is saved in ASCII based text and can be reviewed, copied or printed directly from the log files. The data can also be loaded into a spreadsheet application for analysis. The format of the syslog entry data format lends itself to parsing.

Customer log histories can be only viewed by directly accessing the custlog file using the Session Server CLI (command line interface). Log files can also be downloaded using FTP to a PC or other system capable of connecting to the Session Server 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 anatomy of a SIP Gateway application (SIPC, SIPM or DBSE) log



```
Apr 7 10:28:49 sp2k-1 alarmd: SIPM302 MAJOR TBL
SIP Gateway Maintenance Trouble Alarm :
NCGL=sp2k-1;Unit=0;SIP Gateway Appl SIP Gateway Application Mtc Out Of Sync
```

Format and anatomy 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
```

The following procedures are available for accessing logs on the Session Server:

Procedure	NCGL platform or SIP GW application	Page
View Session Server logs from the CS 2000 Session Server Manager or CS 2000 NCGL Platform Manager	All	37
View and save log files (for log reports) from the NCGL operating system	All	41

The following table displays all available customer logs that are generated by the Session Server platform hardware and the NGCL operating system.

Customer log	NCGL platform or SIP GW application	Start Page
XTS300 series logs (300-395)	NCGL	165
XTS600 series logs (600-695)	NCGL	209

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

Customer log	NCGL platform or SIP GW application	Start Page
STGW700	SIP GW Application	107
DBSE300	SIP GW Application	111
SIPC301 through SIPC750	SIP GW Application	115
SIPM300 through SIPM500	SIP GW Application	121
SIPS300 through SIPS606	SIP GW Application	139
CRTM700 and CRTM701	SIP GW Application	161

Session Server logs generated on the CS 2000

Session Server has some customer logs generated on the CS 2000 core. 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 core NGSS log group, refer to the Carrier Voice over IP Fault Management Logs Reference Manual, NTP NN10275-909.

Remove and replace a Session Server unit or component

The following Session Server components are field replaceable

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

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

Replacing an entire Session Server unit

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

Replacing hard disk drives

Each Session Server node 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 Session Server unit from the SAM-F 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 Session Server unit from the SAM-F 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 Session Server unit from the SAM-F 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 Session Server.

Procedure	Hardware, platform or SIP GW application
Replace a Session Server server unit on page 71	entire Session Server unit
Replace a Session Server hard drive on page 81	hard disk drive
Replace a Session Server power supply on page 95	power supply module
Replace a Session Server CDRW/DVD-ROM drive on page 91	CDRW/DVD-ROM drive

Routine maintenance

This section provides a list of activities used to perform routine maintenance for the Session Server. 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.

> ***Note:*** Consult your Nortel installation staff for additional maintenance practices and guidelines.

Tasks to be performed daily

Component	Task	Document	Notes
Session Server	Monitor alarms and logs	Session Server Fault Management NTP, NN10332-911	

Tasks to be performed weekly

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

Preventative maintenance

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

Tasks to be performed daily

Component	Task	Document	Notes
Session Server	Monitor alarms and logs	Session Server Fault Management NTP, NN10332-911	

Tasks to be performed daily

Component	Task	Document	Notes
GWC	Monitor GWC logs to verify connectivity has not been lost with the Session Server 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 core logs to verify that DPT trunks do not unexpectedly go out of service. Each outage should have corresponding logs in the NGSS to explain why and the lack of corresponding NGSS logs indicates a problem.	CS 2000 Fault Management, 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
Session Server	Clean the DVD drive	HP Carrier-Grade Server cc3310 Product Guide, HP part number: cc3310_Product	
Session Server	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

Tasks to be performed per office schedule

Component	Task	Document	Notes
Session Server	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.	Session Server Fault Management NTP, NN10332-911	
Session Server	Check that cables and connectors are secure at both the front and rear of the Session Server chasses. Also, inspect the integrity of all cabling to ensure there is no frayed wiring.	no formal procedure required	

Performing a dead office recovery of a Session Server node

There are no network component dependencies related to when either of the Session Server units is booted. The Session Server, Core and GWCs associated with Session Server can come back into service in any order. Once the Session Server active unit has booted and the SIP Gateway application initializes, it reads its state file and attempt 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.

Execute the procedures in the following activity to perform a restart of a Session Server node.

Step	Procedure
1	Determine which physical or logical unit you want to become active and power that unit up first by executing procedure *Power-On and boot a Session Server unit*, found in the Session Server Security and Administration NTP, NN10346-611.
2	Log onto the active unit to monitor the status of the SIP Gateway application using procedure View the operational status of the SIP Gateway application on page 44. Verify that the Administrative state of the SIP Gateway application becomes **Unlocked** and the Operational state becomes **Enabled**. If the active unit comes up in any state other than Unlocked:Enabled, refer to the Session Server Security and Administration NTP, NN10346-611 and complete one or both of the following procedures: • complete procedure *Unsuspend the SIP Gateway application* • complete procedure *Unlock the SIP Gateway application*
3	Once the active unit has begun call processing, power up the mate unit by executing procedure *Power-On and boot a Session Server unit*, found in the Session Server Security and Administration NTP, NN10346-611.

Step	Procedure
4	From the active unit, verify that the SIP Gateway application databases on the both units have synchronized using procedure Verify synchronization status of Session Server units on page 68
5	Monitor the system for an appropriate period per your site guidelines. If you experiences problems with call processing, refer to the Session Server Security and Administration NTP, NN10346-611and perform the following tasks in order: • complete procedure *Invoke a maintenance SwAct of the Session Server platform* • complete procedure *Inhibit a system SwAct (Jam)* • contact your next level of support or Nortel GNPS.

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 Session Server 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. The time of day for the backup or the content set of the backup cannot be changed by the customer; however, the customer can perform a manual backup of the database on an as-needed basis such as when an upgrade activity is scheduled. It is recommended that manual backups be performed on the active database.

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 and unlocked and the ethernet links are unjammed) and fault tolerance restored, synchronization between the standby unit's database to the active unit's database begins.

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

Database restore procedures

Procedure
Prepare for a database restore on a Session Server unit on page 102
Perform a database restore to a Session Server unit on page 106

Individual procedures

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

View Session Server 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 Session Server.

A customer log entry is generated for each alarm raised and cleared. Refer to procedures View Session Server logs on page 37 or View and save log files on page 41 to review and correlate log entries with alarms.

Limitations and restrictions

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

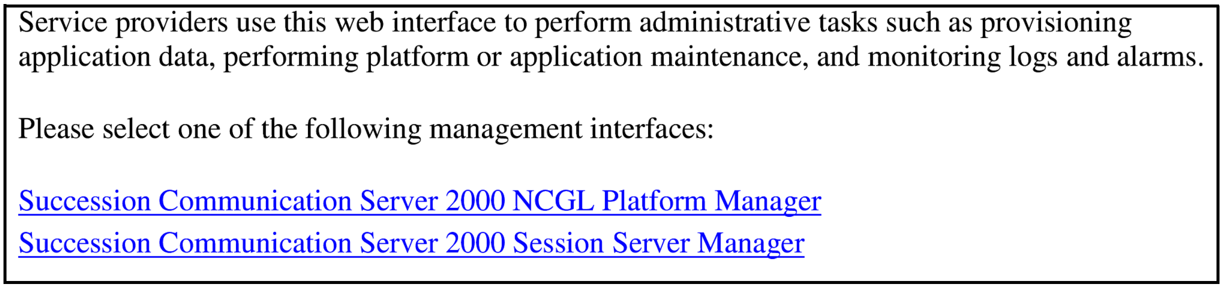
Prerequisites

This procedure has no prerequisites.

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.



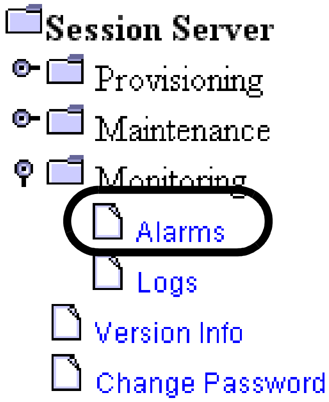
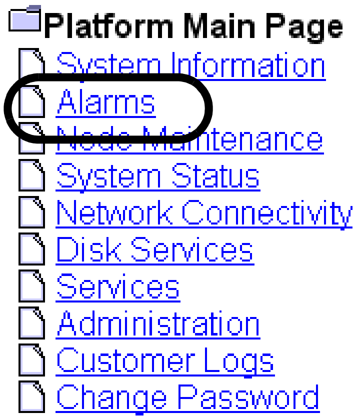
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

Succession Communication Server 2000 NCGL Platform Manager

Succession Communication Server 2000 Session Server Manager

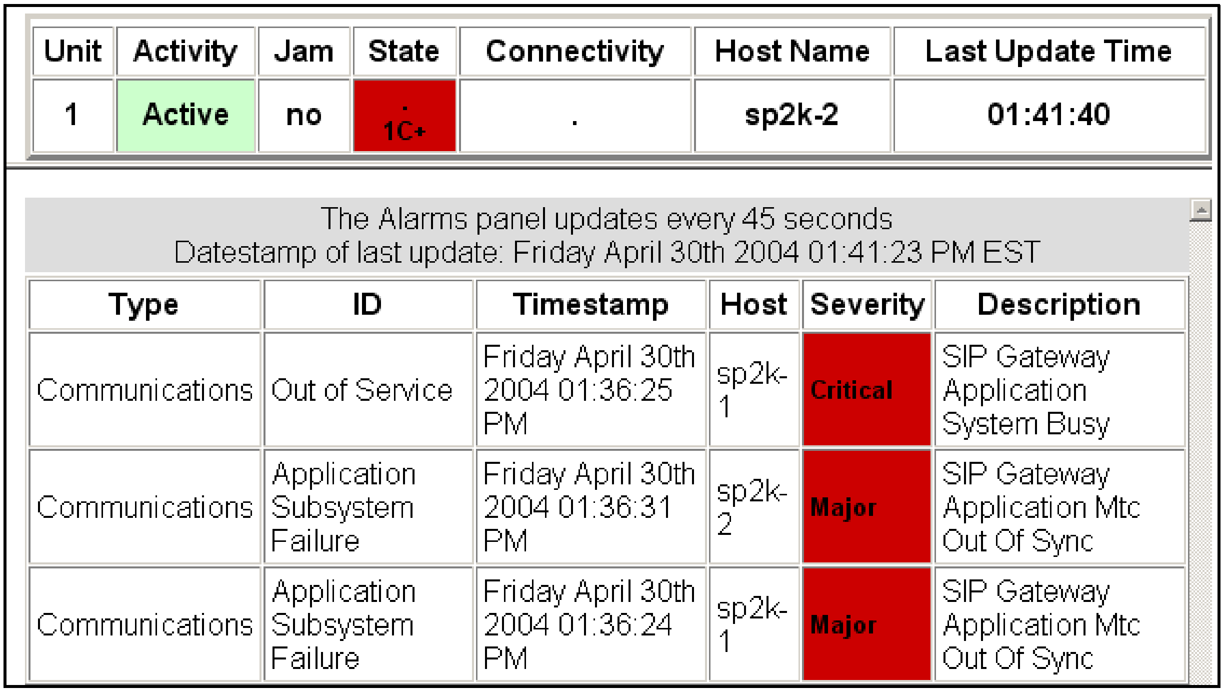
2 From either view, click the **Alarms** link.

View from the CS 2000 Session Server Manager	**View from the CS 2000 NCGL Platform Manager**
	
Session Server Provisioning Maintenance Monitoring Alarms Logs Version Info Change Password	Platform Main Page System Information Alarms Node Maintenance System Status Network Connectivity Disk Services Services Administration Customer Logs Change Password

The Alarms page is displayed.

3 Using the alarms view, refer to Monitoring and analyzing alarms on page 11 for assistance in reviewing and correlating alarms to logs and to troubleshooting activities.

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



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

4 You have completed this procedure.

View Session Server 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 Session Server.

You cannot save or print log entries or log file contents using this procedure. Instead refer to procedure View and save log files on page 41 to perform this activity.

Limitations and restrictions

Only the most recent logs generated are viewable from the GUIs using this procedure. To view log histories, refer to procedure View and save log files on page 41.

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 Integrated EMS vs. 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.

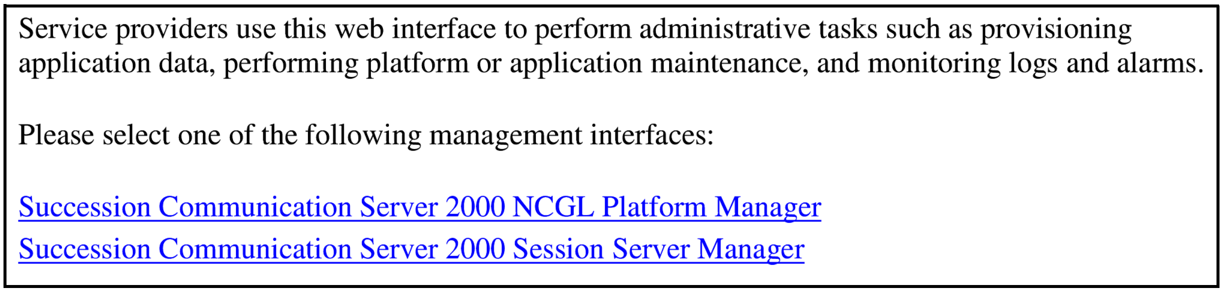
Prerequisites

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

Action

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.

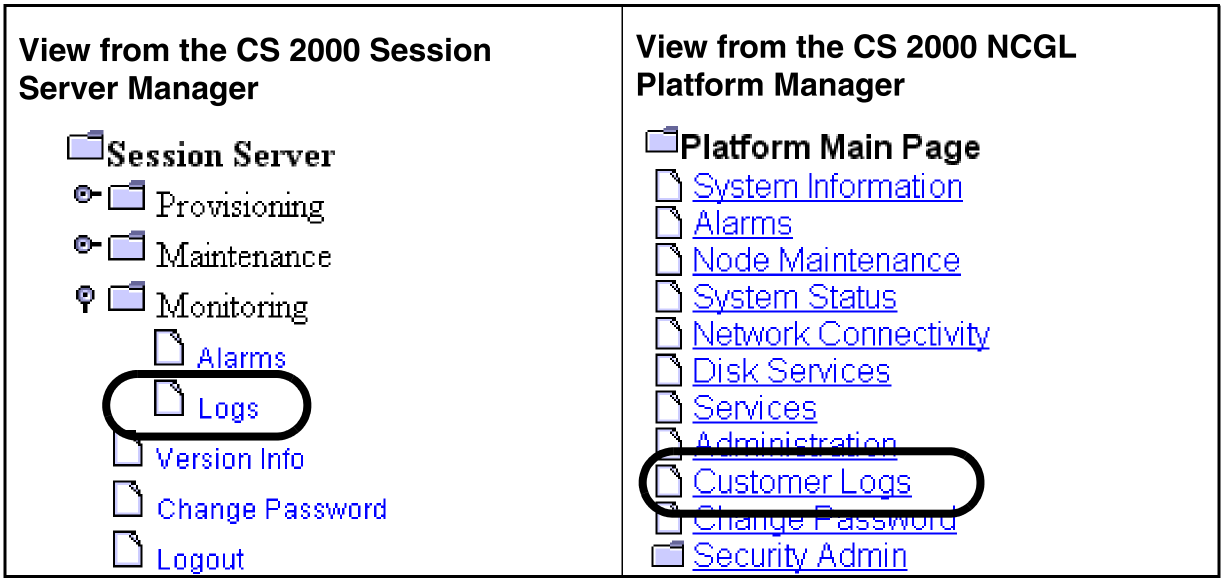


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

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

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



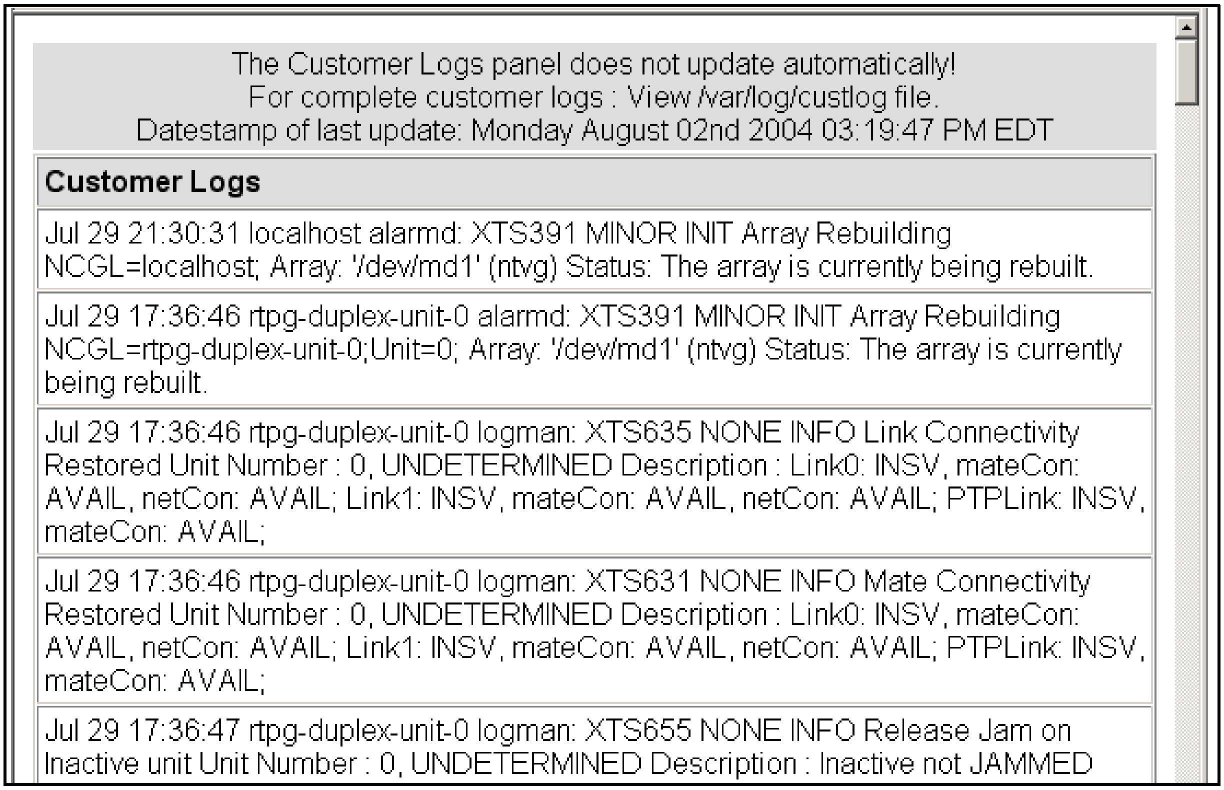
View from the CS 2000 Session Server Manager

View from the CS 2000 NCGL Platform Manager

The logs page is displayed.

3 Using the logs view, refer to Monitoring and analyzing logs on page 20 for assistance in reviewing, analyzing and correlating logs to alarm activity and to troubleshooting activities.

Logs view from Session Server GUIs; view from Integrated EMS may vary



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;
Jul 29 17:36:47 rtpg-duplex-unit-0 logman: XTS655 NONE INFO Release Jam on Inactive unit Unit Number : 0, UNDETERMINED Description : Inactive not JAMMED

4 You have completed this procedure.

View and save 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. Session Server log files are saved as ASCII text files and stored on the Session Server 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 Session Server hard drives.

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

The system log management utility checks every hour to see if the custlog file's contents exceed 5 Mbytes. 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 Session Server 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 Session Server console, either through a direct connection at the rear of the active Session Server unit or through the Integrated EMS application.

Action

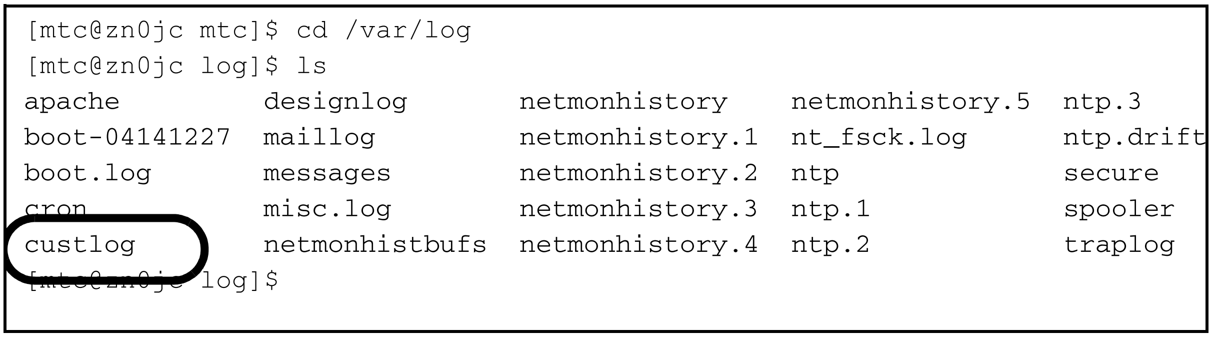
At the Session Server console

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)

6 This procedure is complete.

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

View the operational status of the SIP Gateway application

Purpose of this procedure

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

Limitations and restrictions

This procedure provides instructions for determining the service status of the SIP Gateway application software only. For instructions on determining the status of the Session Server platform, refer to procedure View the operational status of a Session Server NCGL platform on page 49.

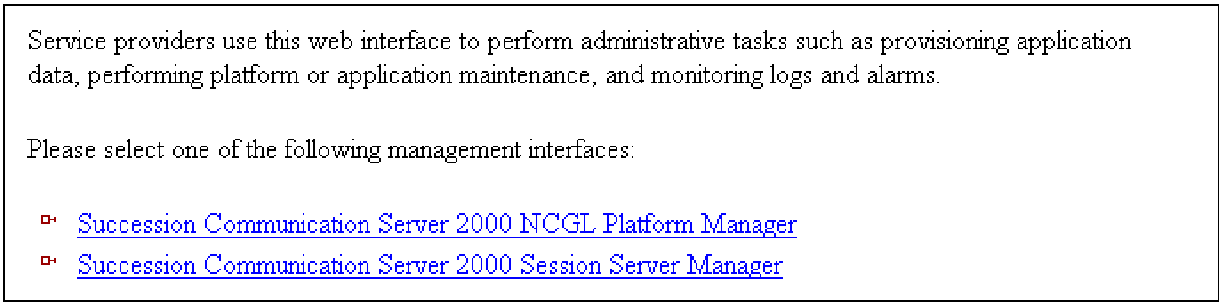
Prerequisites

There are no prerequisites for this procedure.

Action

At the Session Server GUI or Integrated EMS client

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

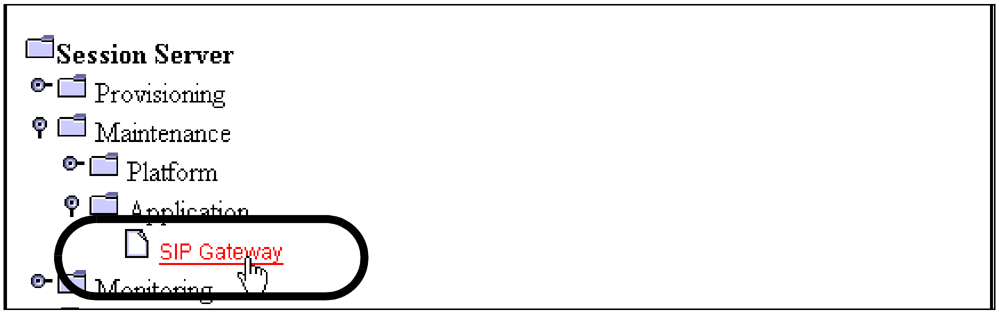


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

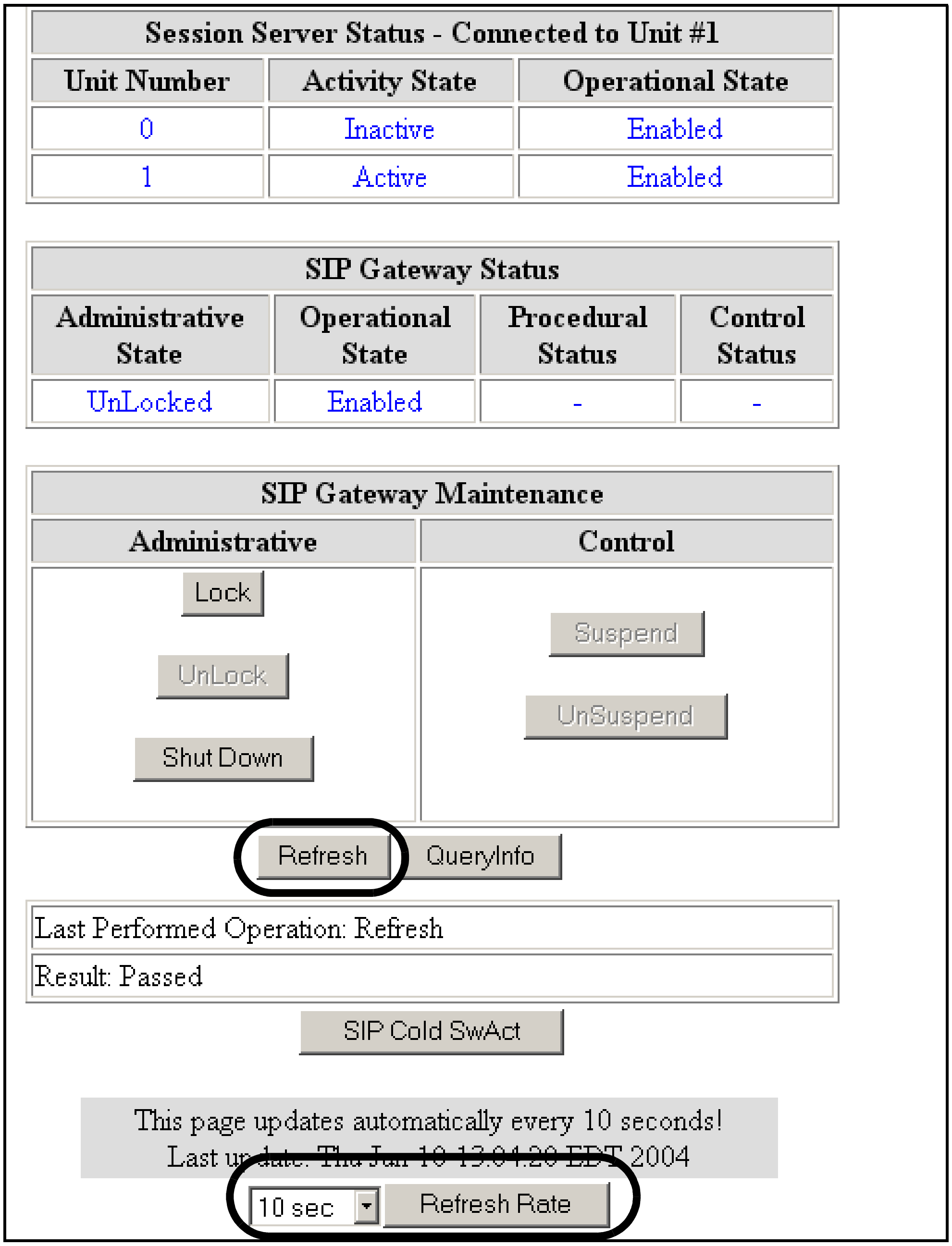
Please select one of the following management interfaces:

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

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



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



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

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

SIP Gateway Maintenance

Administrative	Control
Lock UnLock Shut Down	Suspend UnSuspend

Last Performed Operation: Refresh

Result: Passed

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

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

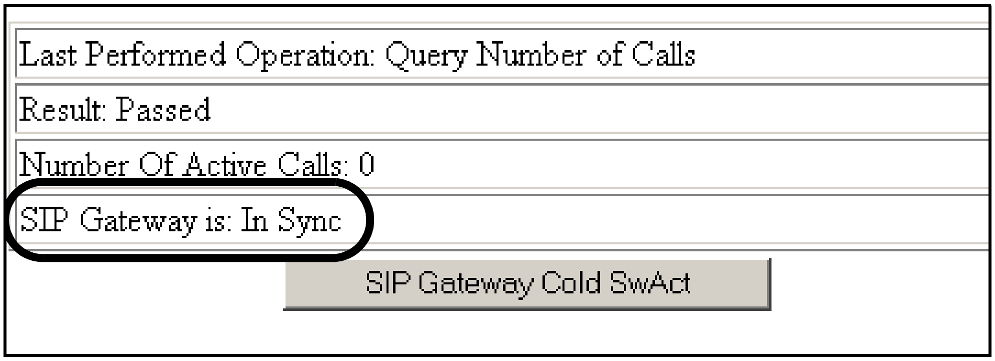
4 Refer to section Interpreting SIP Gateway application status and maintenance fields on page 47 to review the description of the various fields of this view.

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

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

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

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



Last Performed Operation: Query Number of Calls

Result: Passed

Number Of Active Calls: 0

SIP Gateway is: In Sync

7 The procedure is complete.

Interpreting SIP Gateway application status and maintenance fields

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

Session Server node status field descriptions

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

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

SIP Gateway application Status field descriptions

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

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

SIP Gateway Maintenance field descriptions and interpretation of service states

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

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

View the operational status of a Session Server NCGL platform

Purpose of this procedure

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

Limitations and restrictions

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

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

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

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

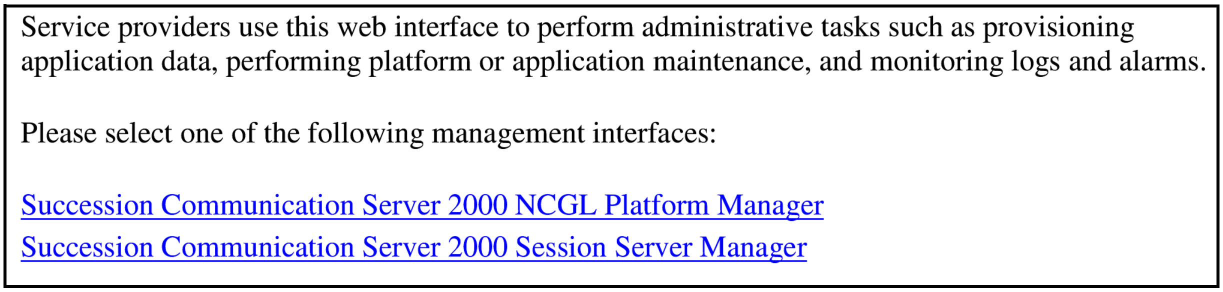
Prerequisites

There are no prerequisites for using this procedure.

Action

At the Session Server GUI or Integrated EMS client

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

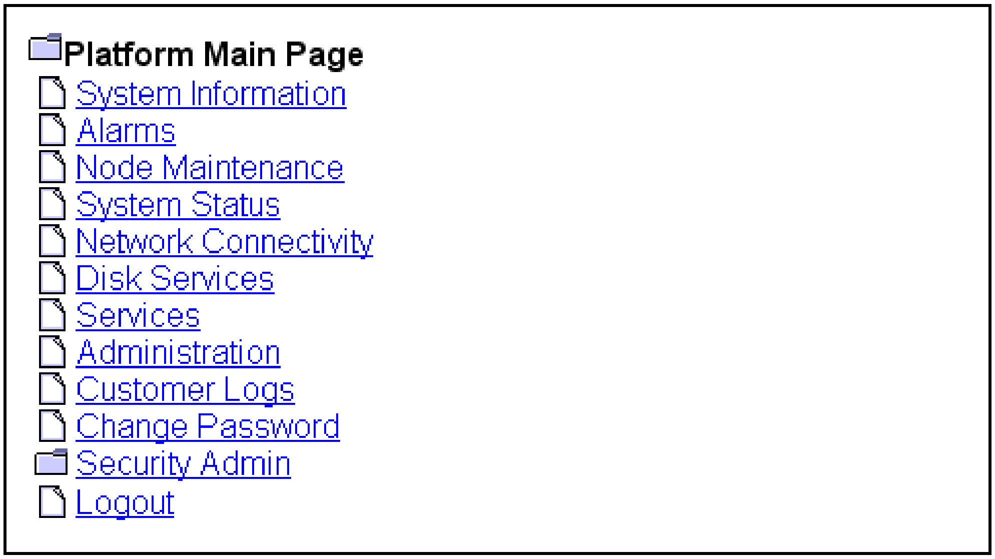


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

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

The Platform Main Page menu is displayed.



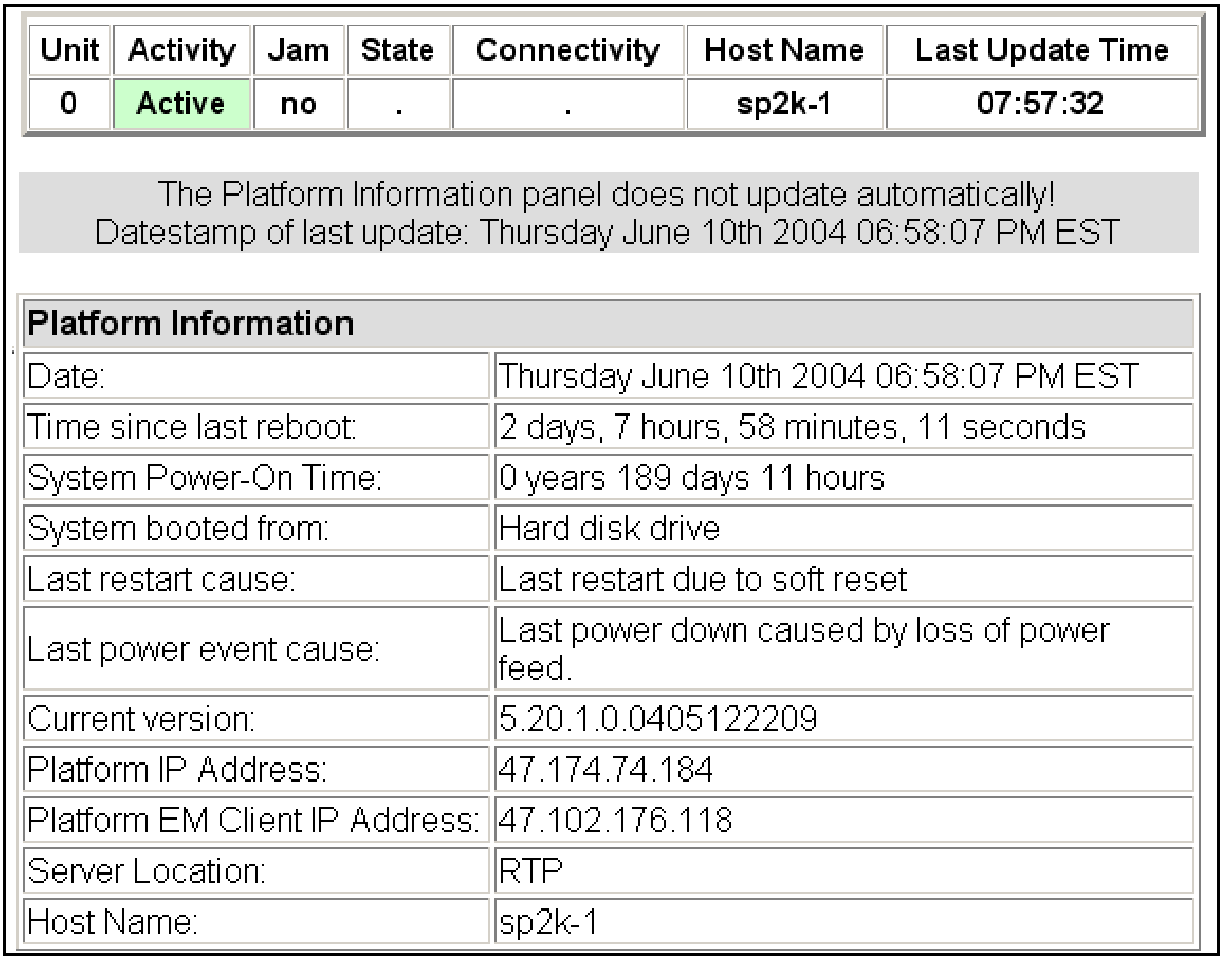
2 Use the following table to determine your next step:

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

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

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

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



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

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

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

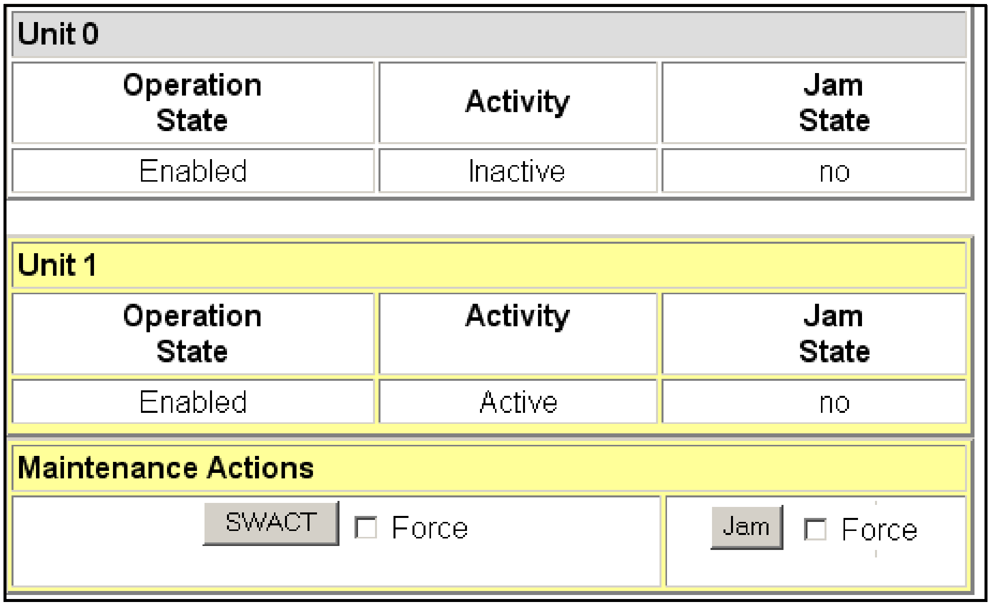
Field	Description
Unit	The unit number in the node that you are logged into.
Activity	Indicates the activity of the unit (either active or standby).
Jam	Indicates if an activity Jam has occurred on the active Session Server unit. This prevents the standby unit from becoming active, regardless of any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

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

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

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

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



Unit 0

Operation State	Activity	Jam State
Enabled	Inactive	no

Unit 1

Operation State	Activity	Jam State
Enabled	Active	no

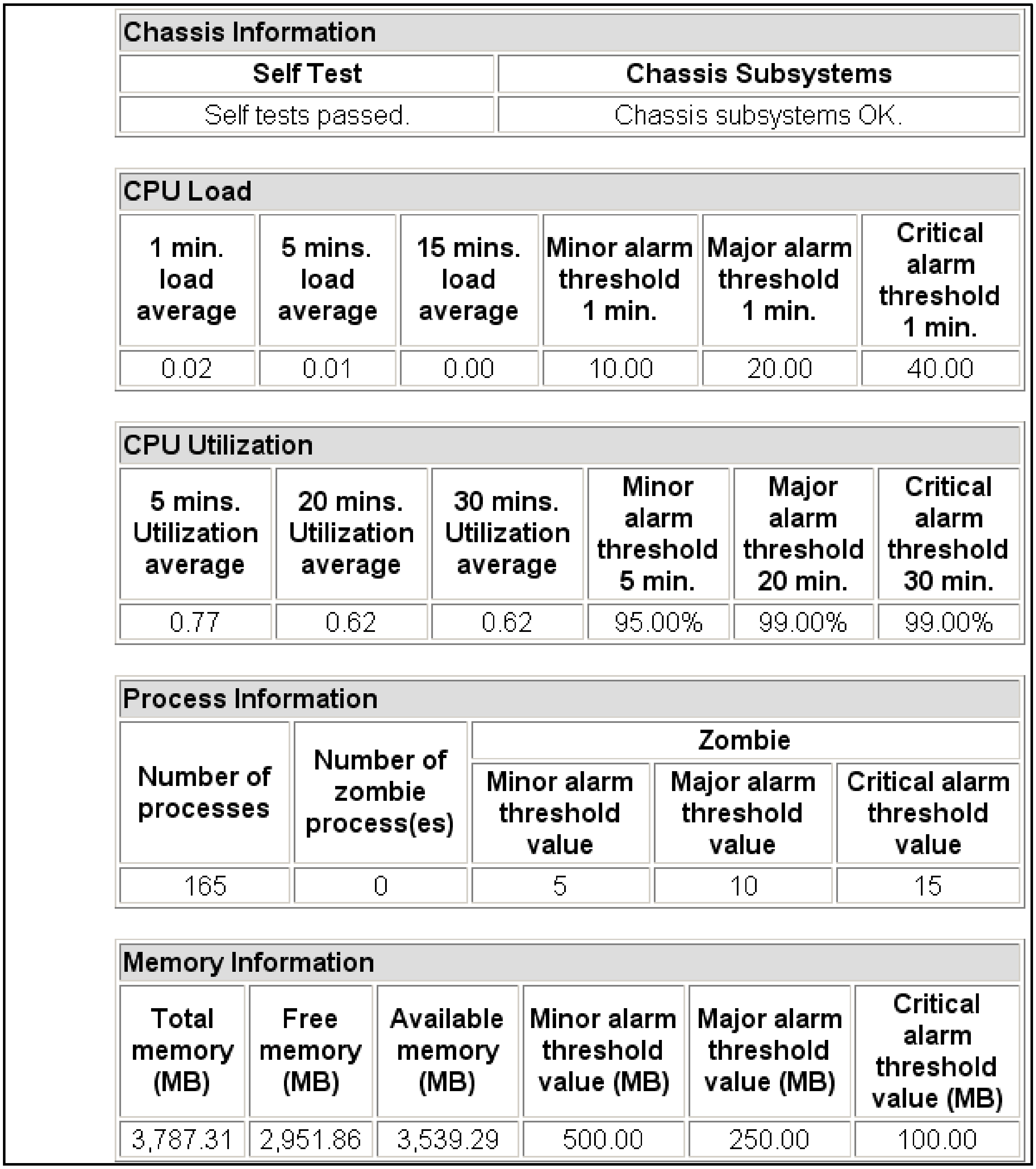
Maintenance Actions

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

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

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

> ***Note:*** The Chassis Information panel is not automatically refreshed.



Chassis Information

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

CPU Load

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

CPU Utilization

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

Process Information

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

Memory Information

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

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

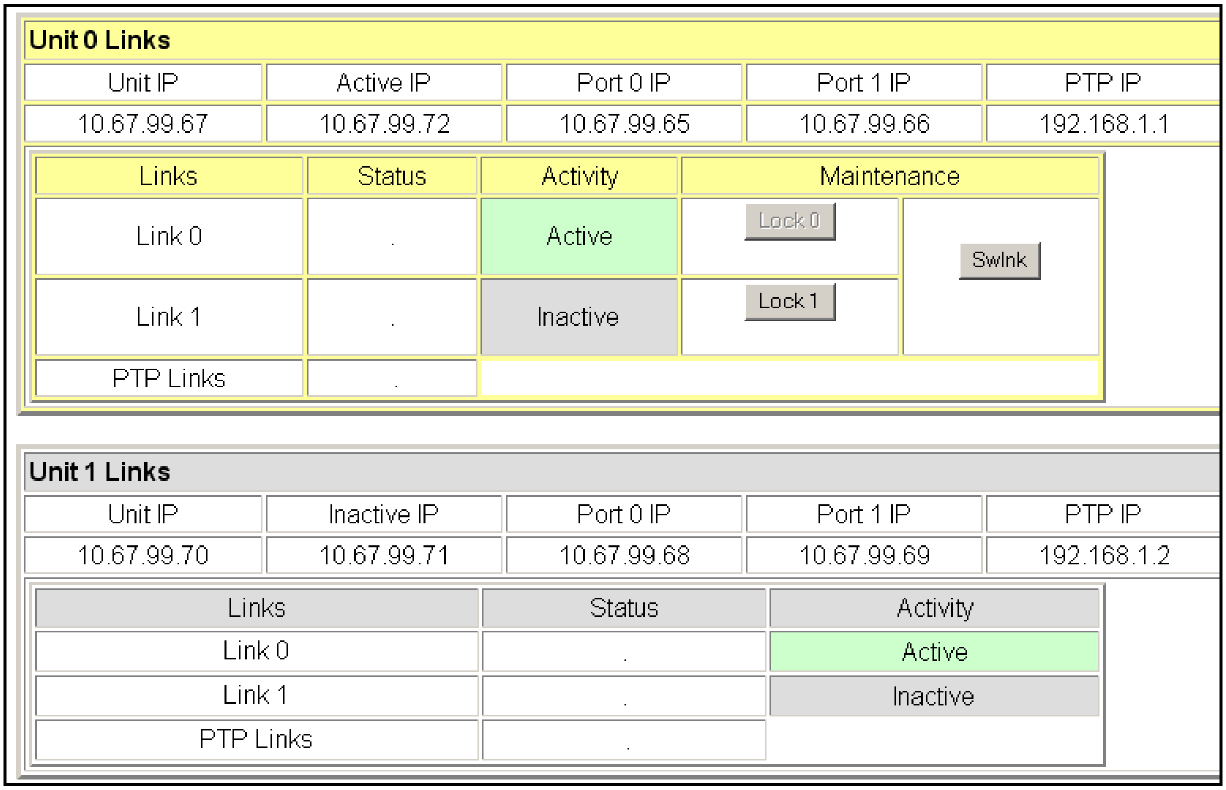
Field	Description
Process Information-zombie: major alarm threshold value	Indicates the maximum number of zombie processes allowed to be run by the CPU before a major alarm is raised indicating that the set threshold has been exceeded.
Process Information-zombie: critical alarm threshold value	Indicates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

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

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

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

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



Unit 0 Links

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

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

Unit 1 Links

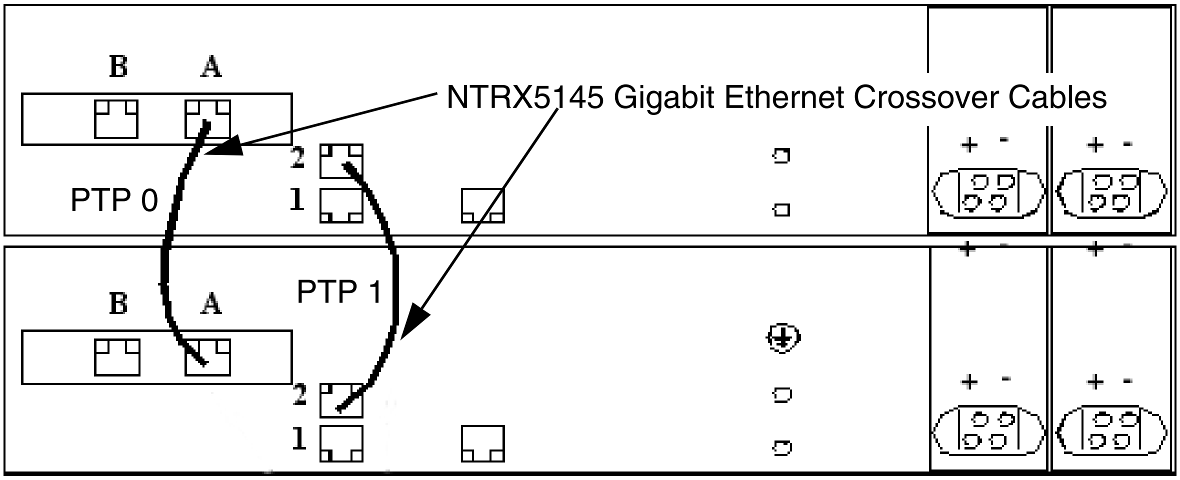
Unit IP	Inactive IP	Port 0 IP	Port 1 IP	PTP IP
10.67.99.70	10.67.99.71	10.67.99.68	10.67.99.69	192.168.1.2

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

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

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

Crossover and LAN ethernet cable connections for Session Server units



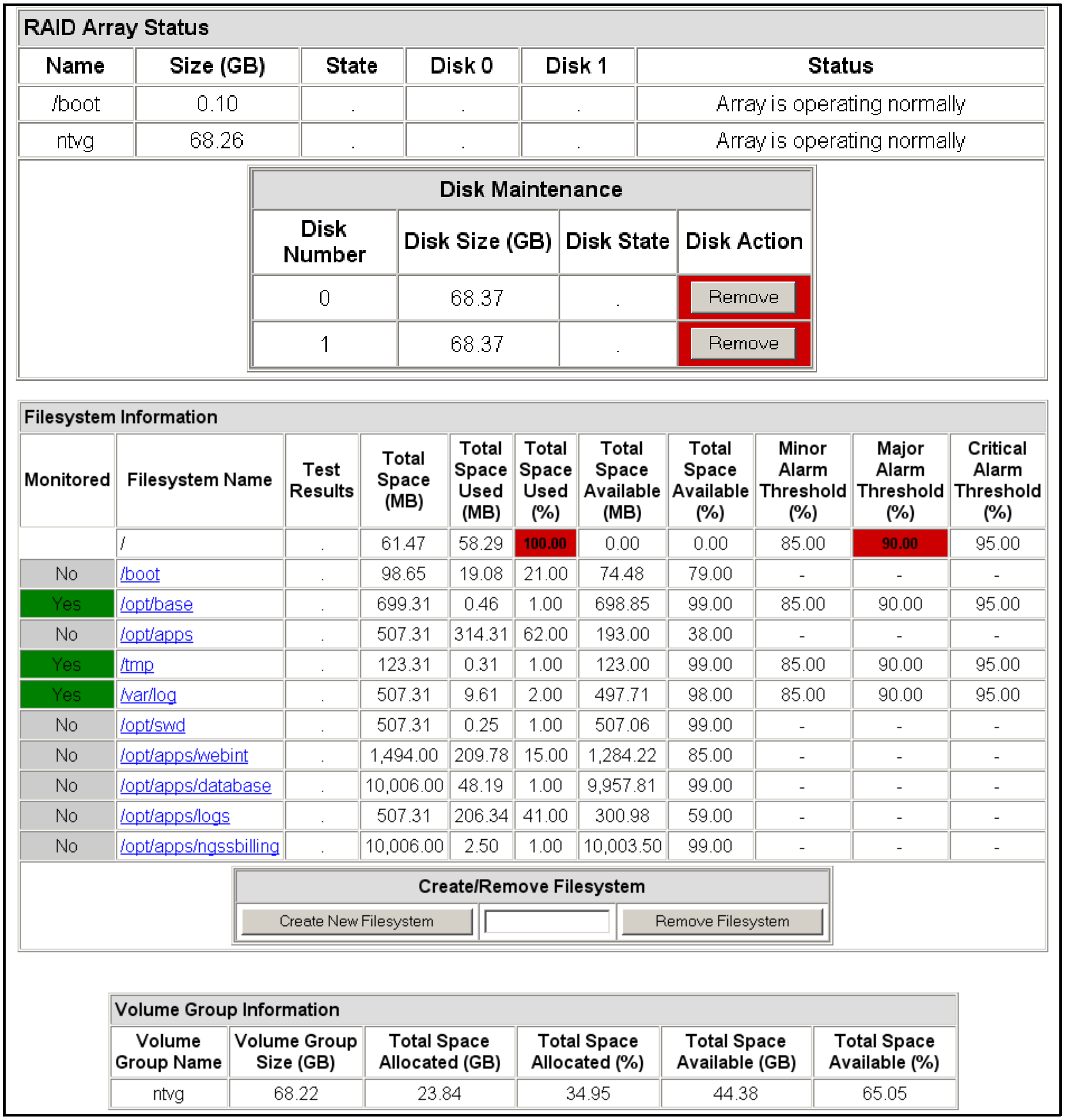
Ethernet Ports:

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

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

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

> ***Note 1:*** The Disk Services panel does not update automatically. Click the **Disk Services** link again to update it.
>
> ***Note 2:*** To create and remove file systems, refer to applicable procedures in the Session Server Configuration Management NTP, NN10338-511.



RAID Array Status

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

Disk Maintenance

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

Filesystem Information

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

Create/Remove Filesystem

Volume Group Information

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

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

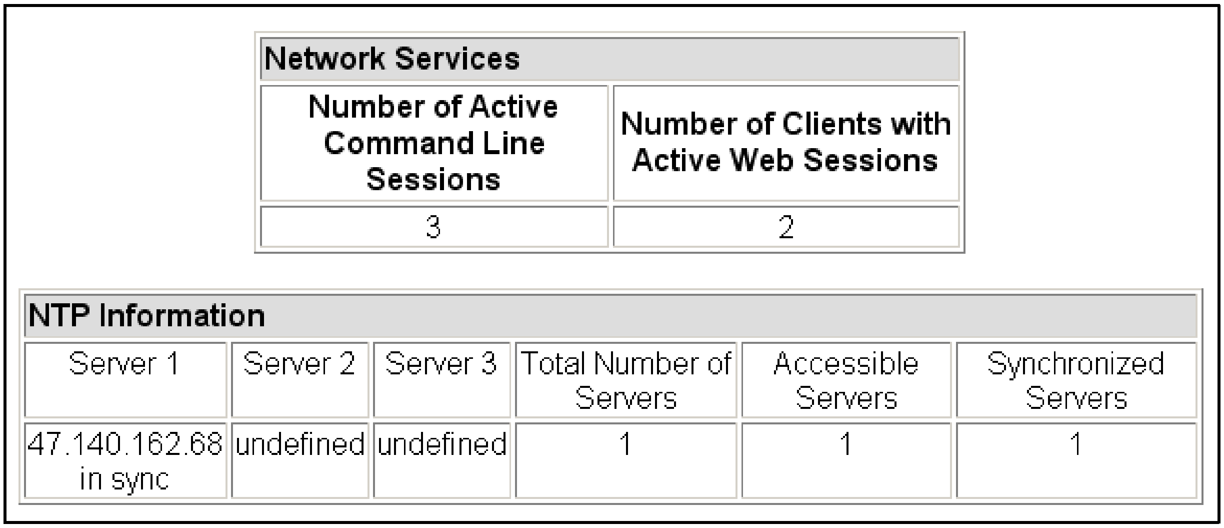
Field	Description
RAID Array Status: State	Indicates a high level state for the array: - ".": indicates the array is functioning normally. - Missing: a disk was removed from the array. - Failed: a disk in the array has failed and needs to be replaced. - Rebuilding: the array is in the process of rebuilding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

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

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

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

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



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

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

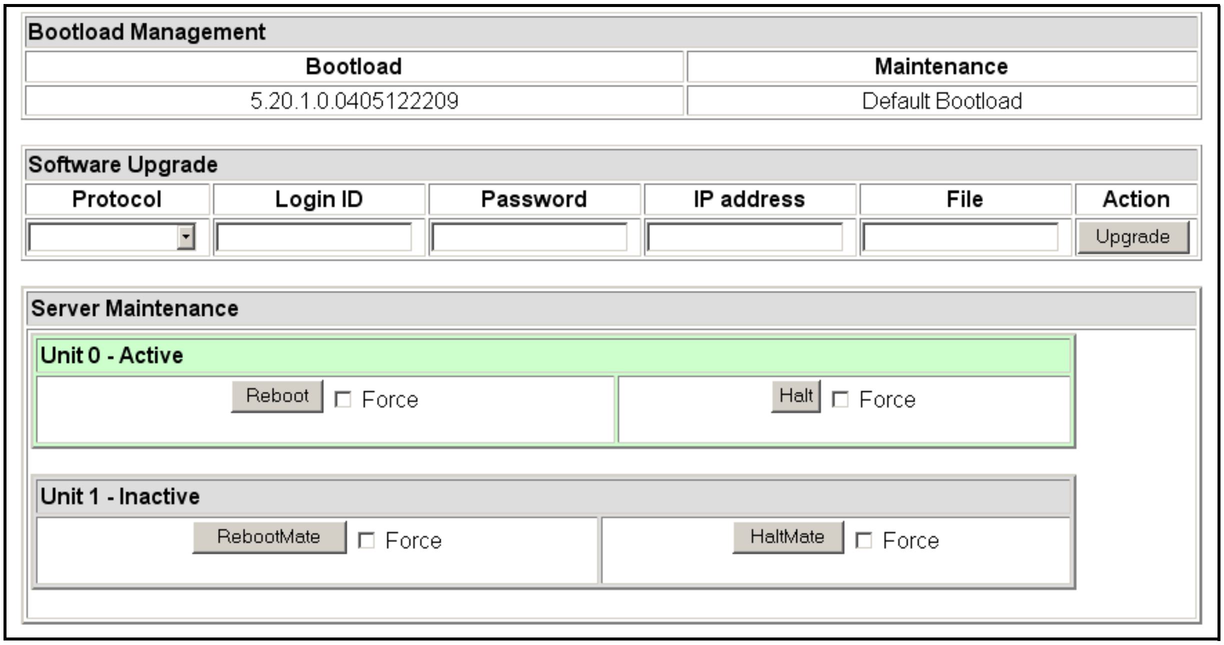
Field	Description
Network Services: Number of Active Command Line Sessions	Indicates the number of command line interface (CLI) sessions (both remote and local) on the Session Server.
Network Services: Number of Clients with Active Web Sessions	Indicates the number of clients running one or more web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

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

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

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

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



Bootload Management

Bootload	Maintenance
5.20.1.0.0405122209	Default Bootload

Software Upgrade

Protocol	Login ID	Password	IP address	File	Action
					Upgrade

Server Maintenance

Unit 0 - Active

Reboot □ Force Halt □ Force

Unit 1 - Inactive

RebootMate □ Force HaltMate □ Force

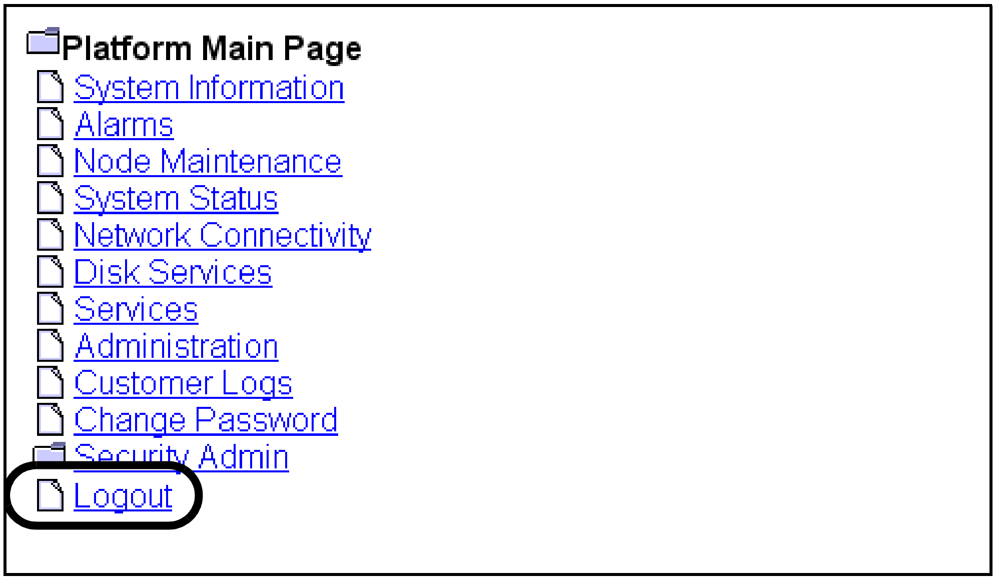
Field	Description
Bootload Management: Bootload	Indicates the load ID for the NCGL platform software load.
Bootload Management: Maintenance	Indicates whether the Bootload is the default. May also allow choosing a new default bootload if there is more than one load available. Additional loads can come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

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

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

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

You are returned to the login page



17 The procedure is complete.

Verify synchronization status of Session Server units

Purpose of this procedure

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

Limitations and restrictions

There are no restrictions for performing this procedure.

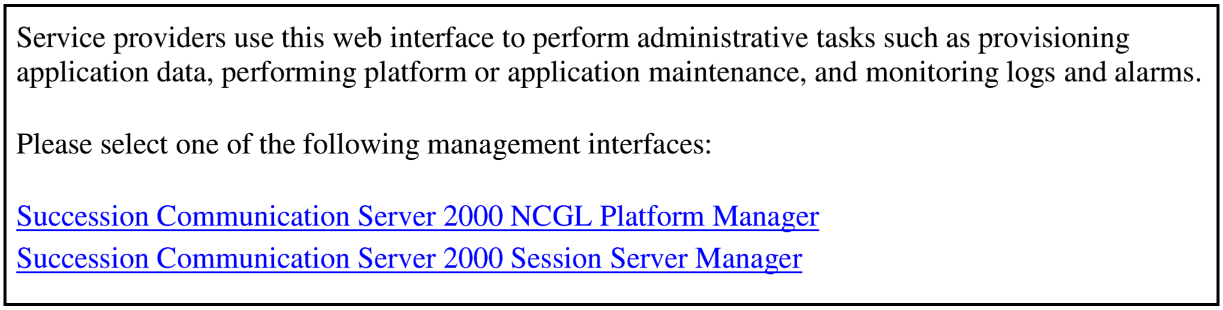
Prerequisites

There are no prerequisites for performing this procedure.

Action

At the Session Server GUI or Integrated EMS client

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

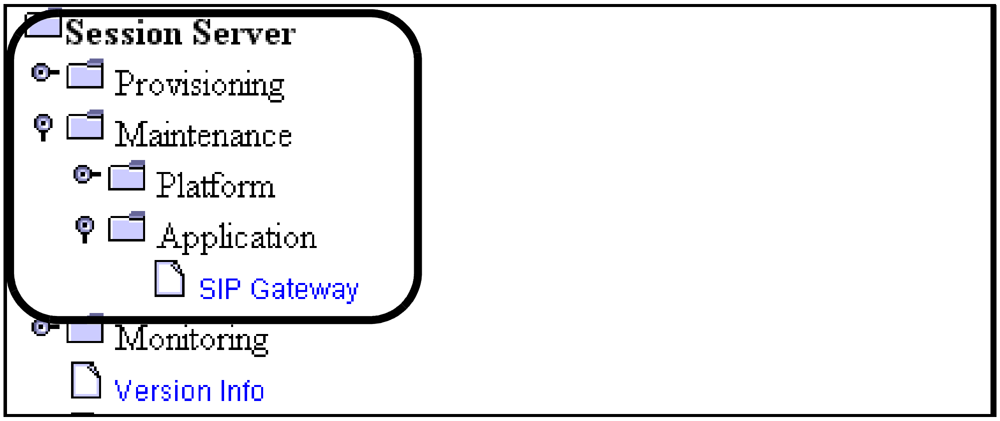


Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

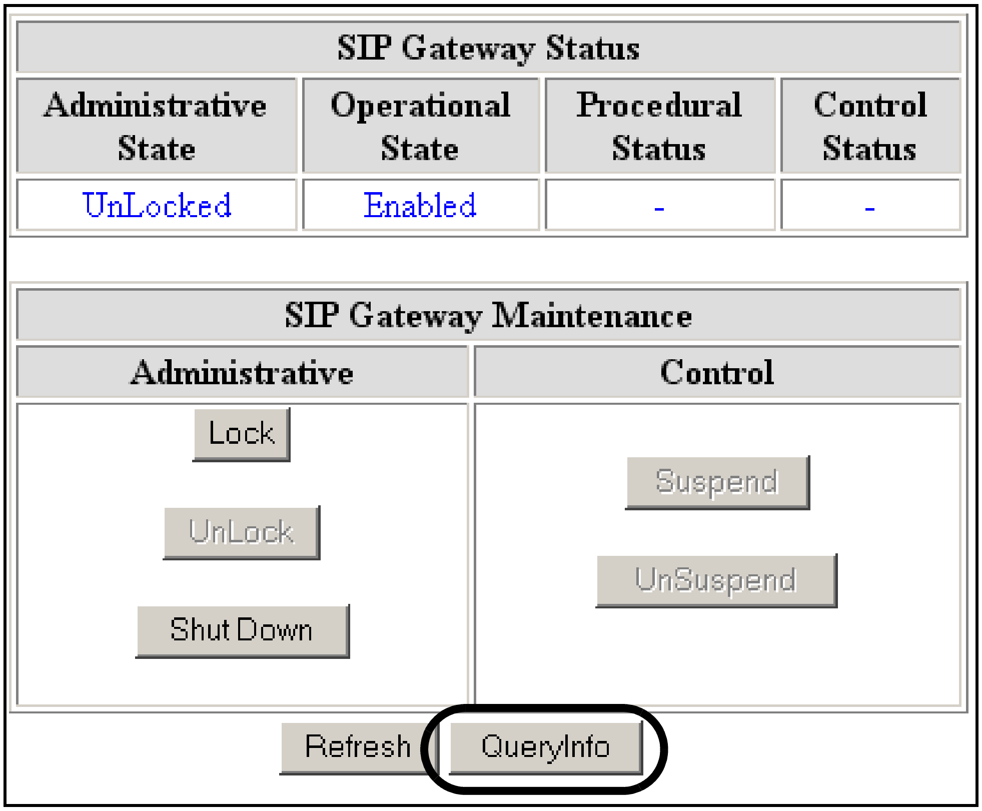
Succession Communication Server 2000 NCGL Platform Manager
Succession Communication Server 2000 Session Server Manager

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



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

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

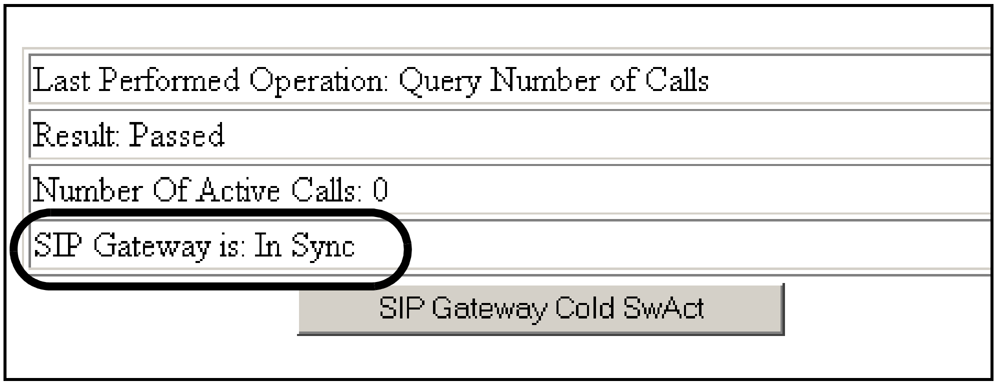


SIP Gateway Status

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

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

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



Last Performed Operation: Query Number of Calls

Result: Passed

Number Of Active Calls: 0

SIP Gateway is: In Sync

6 The procedure is complete.

Replace a Session Server server unit

Purpose of this procedure

This procedure provides the steps for removing and replacing a faulty Session Server unit with a spare. It is intended to facilitate unit replacement so that the Session Server 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 Session Server unit. If the unit you want to replace is the active unit, a system SwAct must be performed. Refer to procedure *Invoke a maintenance SwAct of the Session Server platform* in the Session Server Security and Administration NTP, NN10346-611.

This procedure does not instruct you how to install additional Session Server nodes into your network. Refer to your Nortel installation support representative for support in adding new Session Server 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 Session Server node made up of both active and inactive units, and that you are able to SwAct service and callp activity.

Action

At the CS 2000 Session Server Manager

1 Execute procedure *Inhibit a system SwAct (Jam)* found in the Session Server Security and Administration NTP, NN10346-611.

> ***Note:*** Executing this procedure generates an alarm/log XTS355.

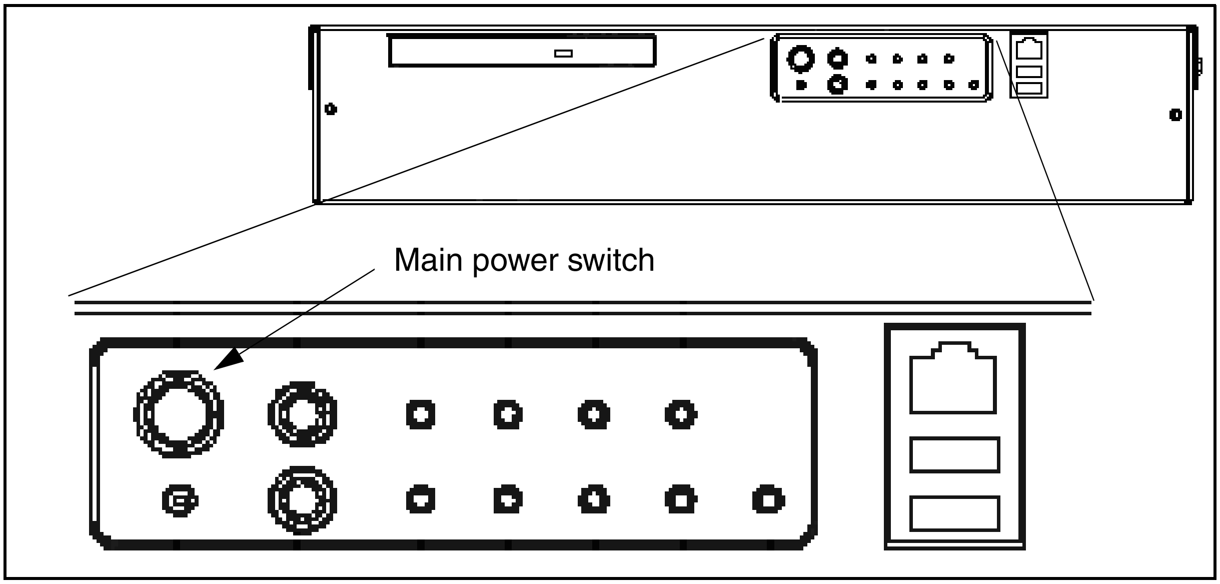
2 Determine if the Session Server unit to be replaced is still in service by executing procedure View the operational status of a Session Server NCGL platform on page 49.

3 Use the following table to determine your next step:

If	Do
the Session Server unit to be replaced is still in service,	Refer to procedure *Halt (shutdown) a Session Server unit* found in the Session Server Security and Administration NTP, NN10346-611.
the Session Server unit to be replaced is not in service,	continue with the next step

At the front panel of the Session Server chassis

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



At the rear of the Session Server chasses 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 on page 79 as needed.

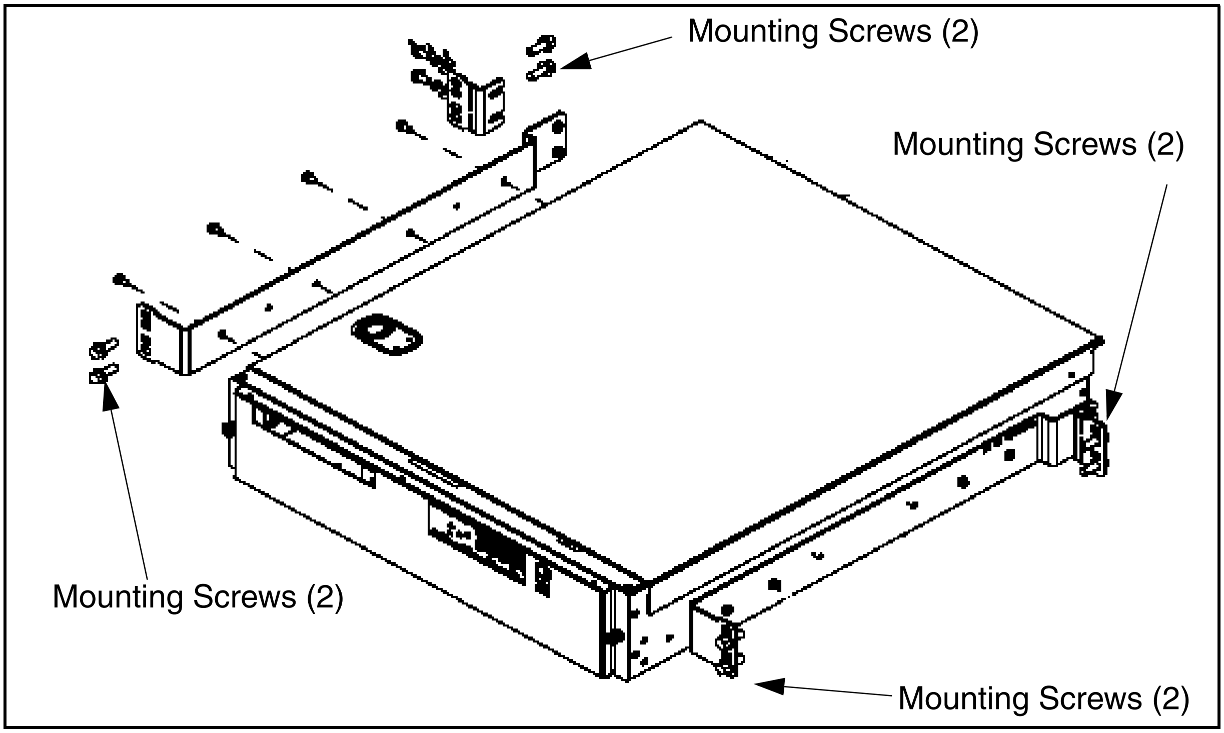
6 Label and remove the 2 ethernet crossover cables (NTRX5145) from the rear of the chassis, referring to the table of Additional installation and removal information on page 79 as needed.

7 Remove the power supply cables (NTRX5199 or NTRX5146) from the rear of the Session Server chassis, referring to the table of Additional installation and removal information on page 79.

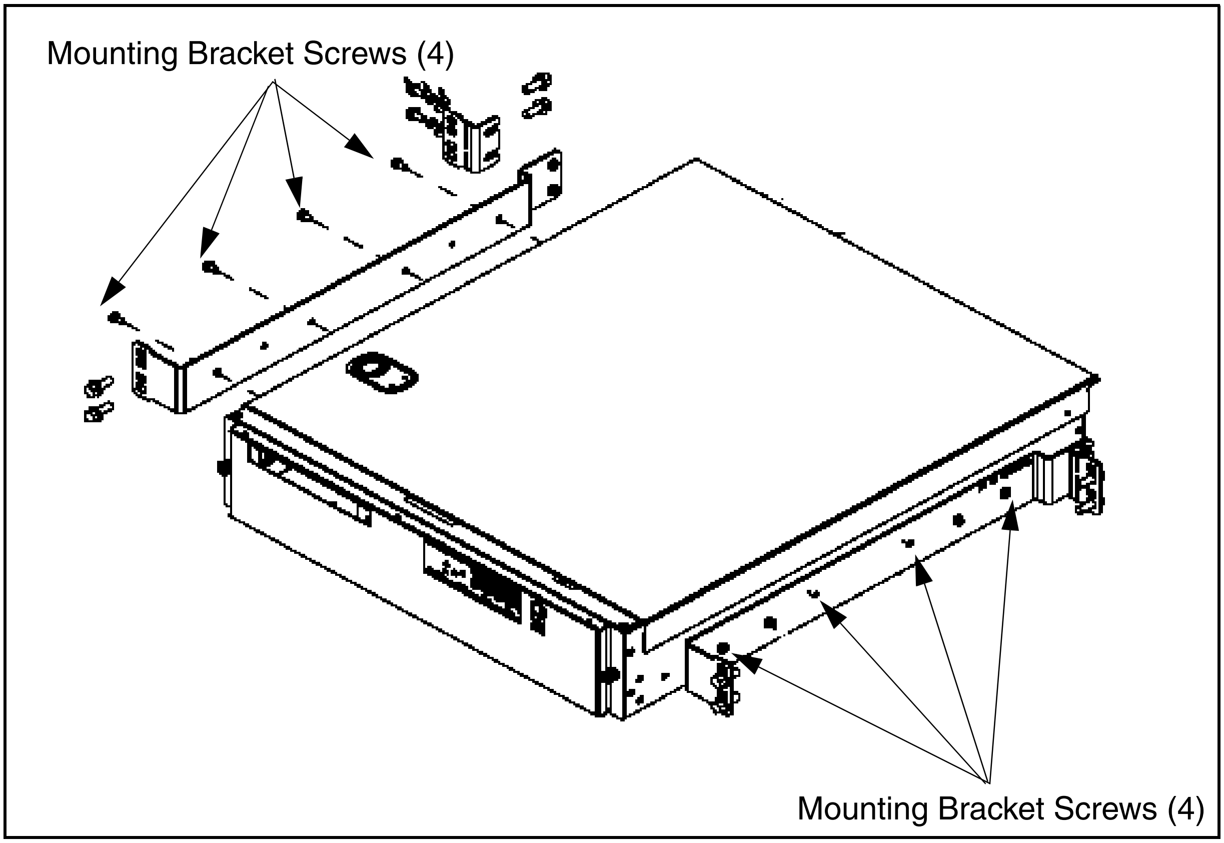
8 Remove the ground cable (NTRX5198) from the rear of the Session Server chassis as shown in figure Session Server unit rear view of ports and ground connection on page 79.

9 If the Session Server 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 on page 79 as needed.

10 Unscrew and remove the chassis mounting screws that hold the Session Server chassis in the SAM-F frame and remove the Session Server unit from the frame. There are 4 screws at the front of the chassis and 4 screws at the back of the chassis (8 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 Session Server unit chassis (8 screws total), as shown in the following figure.



12 Insert the replacement Session Server 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 Session Server 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 on page 79 as needed.

14 Connect the ground cable (NTRX5198) to the rear of the Session Server chassis at its connect point as shown in figure Session Server unit rear view of ports and ground connection on page 79.

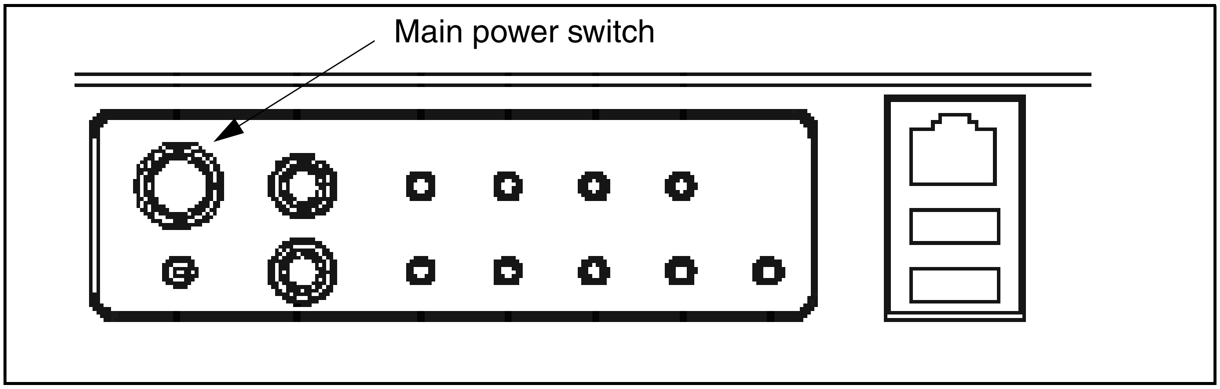
15 Attach and secure the power cables (NTRX5199 or NTRX5146) to the rear of the replacement Session Server chassis, referring to the table of Additional installation and removal information on page 79 as needed.

16 At the power supply panel, reapply power to the replacement Session Server chassis, referring to the table of Additional installation and removal information on page 79 as needed.

17 Connect the 2 ethernet crossover cables (NTRX5145) to the replacement Session Server chassis, referring to the table of Additional installation and removal information on page 79 as needed.

18 Connect the ethernet cables to the replacement Session Server chassis, referring to the table of Additional installation and removal information on page 79 as needed.

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

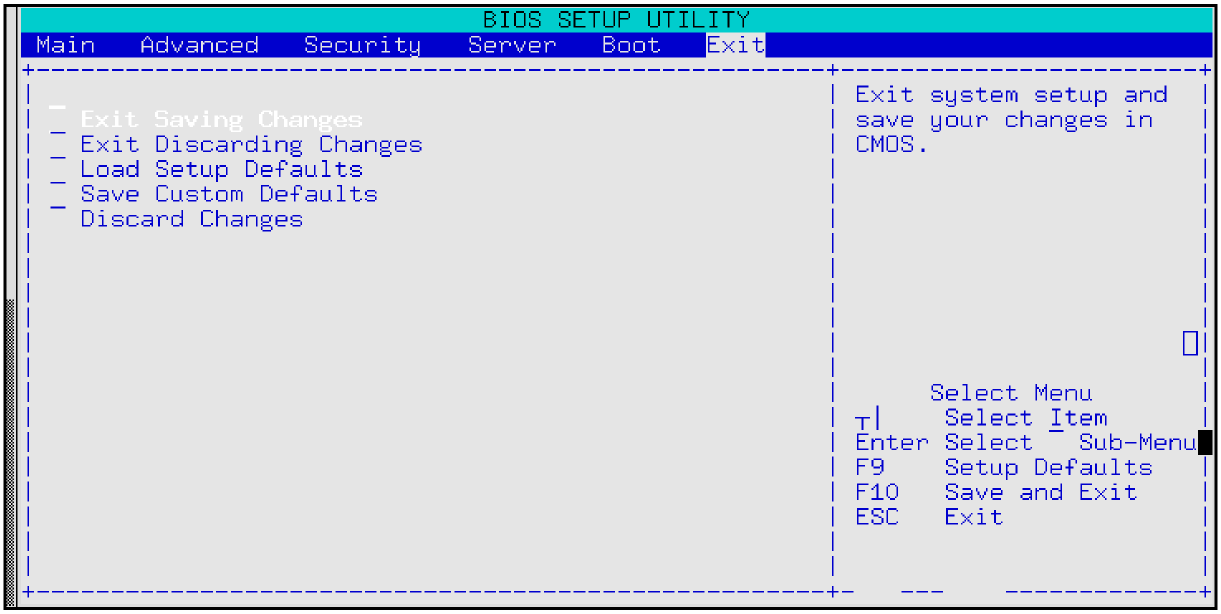


The green power LED lights and the Session Server unit boots attempts to boot from disk.

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.



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

21 Verify that the BIOS on the new unit is configured properly by completing procedure *Reconfigure the Session Server BIOS* found in the Session Server Configuration Management NTP, NN10338-511.

After this procedure is completed, the unit automatically reboots.

22 Complete procedure *Reprovision the Session Server NCGL platform software*, found in the Session Server Configuration Management NTP, NN10338-511.

23 Verify the correct configuration of the NCGL platform by using procedure *Modify NCGL platform provisioning* found in the Session Server Configuration Management NTP, NN10338-511.

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

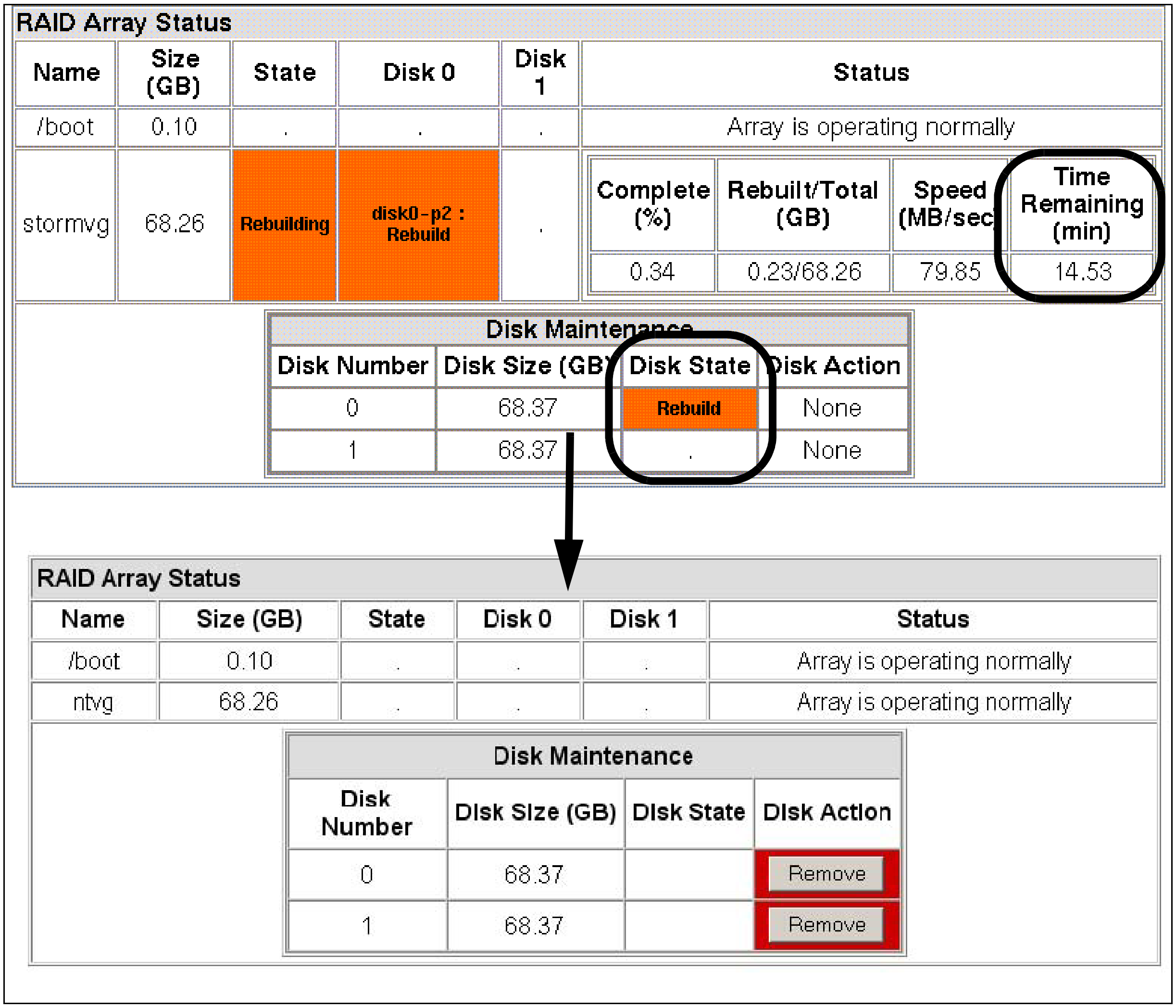
24 Complete procedure *Reinstall and reprovision the Session Server SIP Gateway application,* found in the Session Server Configuration Management NTP, NN10338-511.

At the CS 2000 Session Server Launch Point

25 Access the CS 2000 NCGL Platform Manager GUI your normal method (Integrated EMS or console interface).

26 Go to the Disk Services page using procedure View the operational status of a Session Server NCGL platform on page 49 and confirm that the newly replaced unit is rebuilding the disk drive array.

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



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 (%)	Rebuilt/Total (GB)	Speed (MB/sec	Time Remaining (min)
0.34	0.23/68.26	79.85	14.53

Disk Maintenance

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

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

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

27 Execute procedure View Session Server alarms on page 35 and ensure that all alarms raised related to this remove and replace activity are addressed and cleared.

28 After the drive array has been fully rebuilt (the array status reports that the array is operating normally) and all alarms related to the disk drive failure have been cleared, execute procedure *Verify synchronization status of Session Server units*, found in the Session Server Security and Administration NTP, NN10346-611 to verify that both units are back in sync.

29 Execute procedure *Enable a system SwAct (Unjam)* found in the Session Server Security and Administration NTP, NN10346-611.

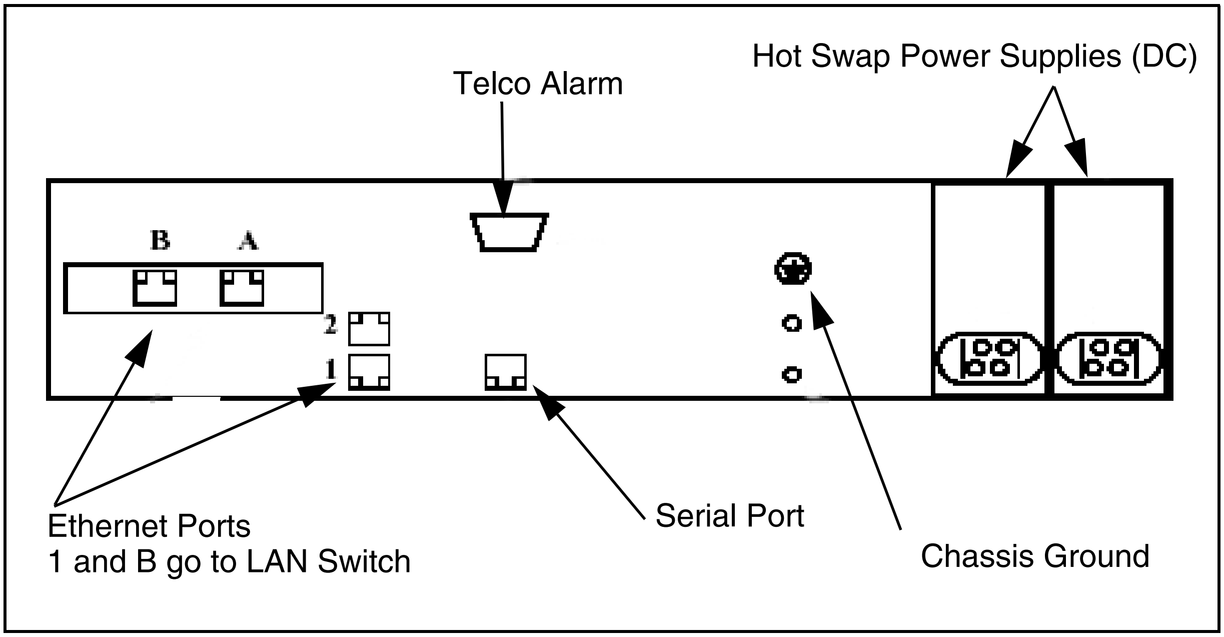
Note: Executing this procedure generates an alarm clearing log XTS655.

30 This procedure is complete.

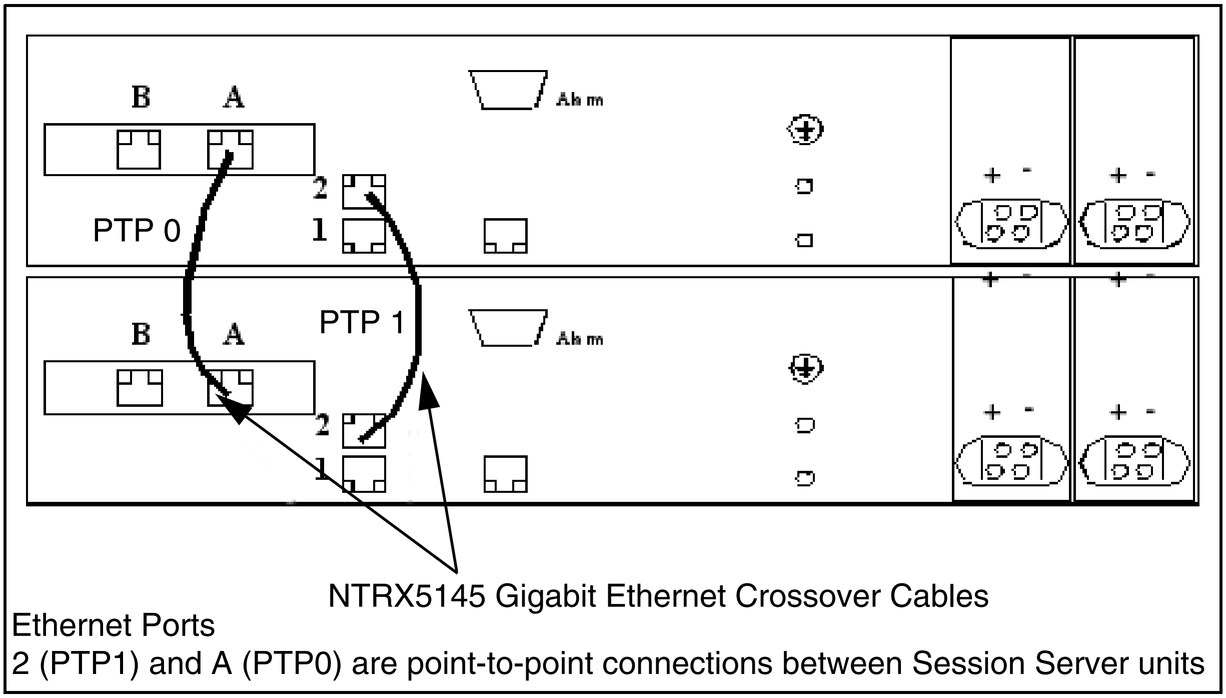
Additional installation and removal information

Use the following figures and table to assist you with removing and replacing a Session Server unit.

Session Server unit rear view of ports and ground connection



Crossover Cable connections between Session Server units


B
A
Alarm
PTP 0
2
1
+ -
PTP 1
NTRX5145 Gigabit Ethernet Crossover Cables
Ethernet Ports
2 (PTP1) and A (PTP0) are point-to-point connections between Session Server units

Session Server - 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

Replace a Session Server 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 Session Server unit.

Limitations and restrictions

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

Prerequisites

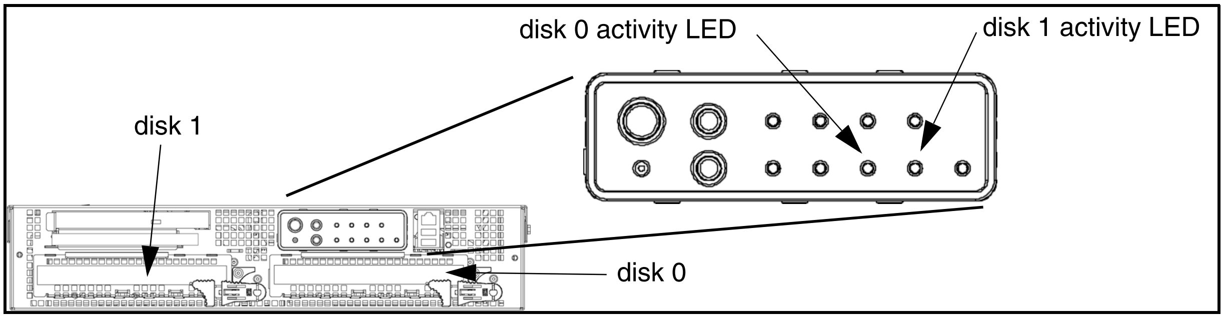
If applicable, ensure continued call processing by perform this procedure only on the standby unit. If the disk drive failure is on the active unit, perform a SwAct of the units using procedure *Invoke a maintenance SwAct of the Session Server platform* found in the Session Server Security and Administration NTP, 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 Session Server chassis for a drive is red as shown in the following diagram

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 Session Server front panel



Materials

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

Action

At the CS 2000 NCGL Platform Manager on the active unit

1 Execute procedure *Inhibit a system SwAct (Jam)* found in the Session Server Security and Administration NTP, NN10346-611.

> ***Note:*** Executing this procedure generates an alarm/log XTS355.

At the Session Server 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 on page 16 and look for a lit red LED on the Session Server chassis front panel that would indicate the ID of the failed drive.

3 Complete procedure Remove a hard drive from the NCGL operating system on page 85.

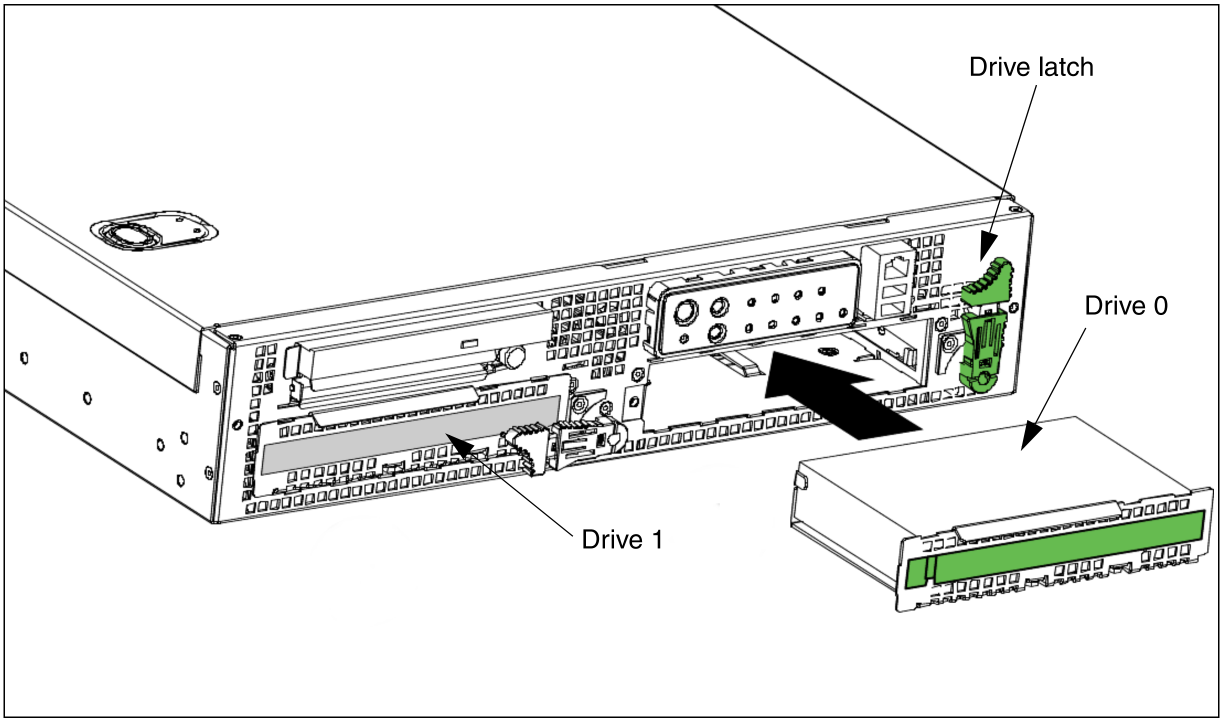
4 Put on an ESD wrist strap and fasten to a frame ground point.

> **WARNING**
> **Electrostatic discharge (ESD) damage**
> Provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground (any unpainted metal surface) on your server or frame when handling parts.

5 Remove the bezel on the face of the Session Server unit to access the disk drives.

6 Unlatch the failed disk from the chassis by turning the green latch 90 degrees, clockwise, from the horizontal position to the vertical position. Remove the failed disk from the chassis.

7 Insert the replacement drive into the chassis slot and secure the drive by engaging the green latch.



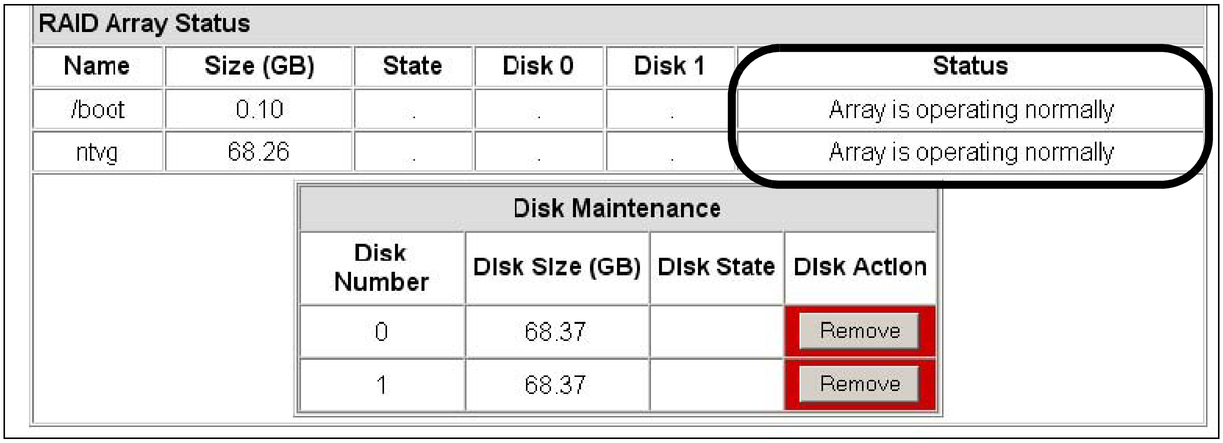
Once the disk drive is replaced, the Session Server unit immediately begins to rebuild the array. During the rebuild, the front panel LED for the disk drive alternates between red and green. If the Session Server chassis is wired to an external alarm system, a minor alarm is indicated with an amber LED.

If the disk is inserted into the Session Server 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

8 Referring to procedure View Session Server alarms on page 35, verify that all alarms related to this activity and the original disk failure condition have been cleared.

9 After the drive array has been fully rebuilt (the array status reports that the array is operating normally, as shown below) and all alarms related to the disk drive failure have been cleared, execute procedure Verify synchronization status of Session Server units on page 68 to verify that the database for both units is synchronized.



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

10 Execute procedure *Enable a system SwAct (Unjam)* found in the Session Server Security and Administration NTP, NN10346-611.

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

11 This procedure is complete.

Remove 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 Replace a Session Server hard drive on page 81.

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.

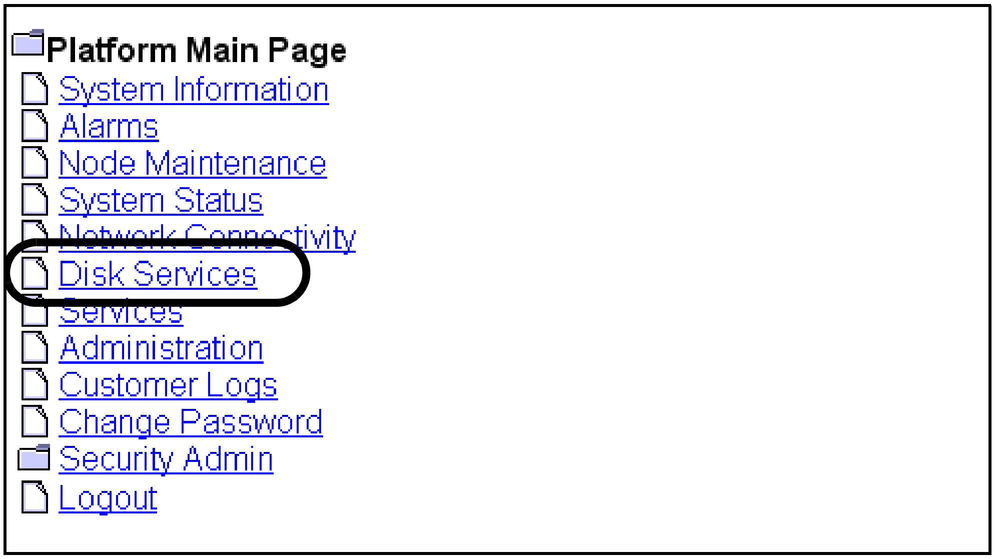
Action

At an Integrated EMS or client workstation

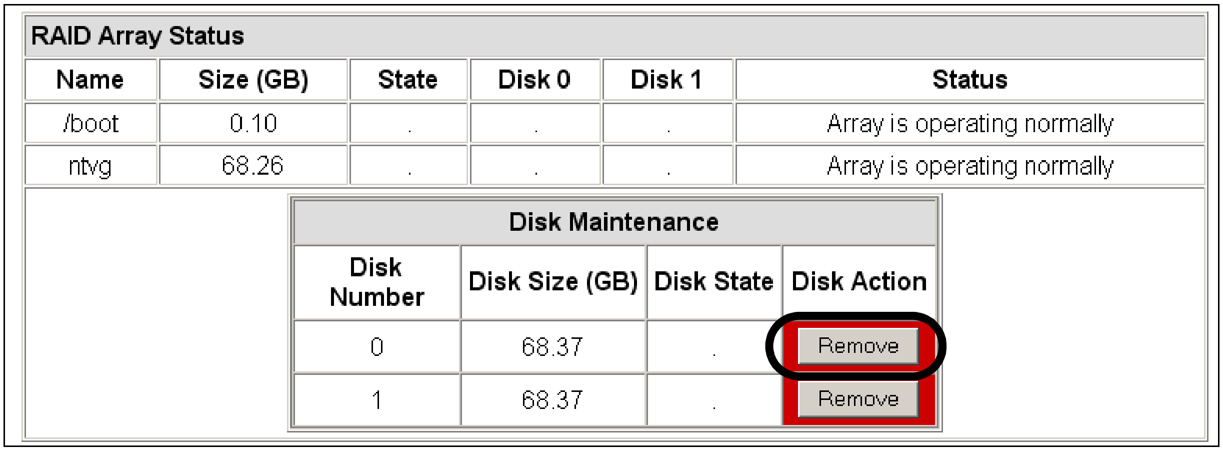
1 Log onto the inactive unit CS 2000 NCGL Platform Manager.

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.



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

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 Replace a Session Server hard drive on page 81 to physically remove the hard drive from the unit.

6 You have completed this procedure

Insert 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 Replace a Session Server hard drive on page 81.

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.

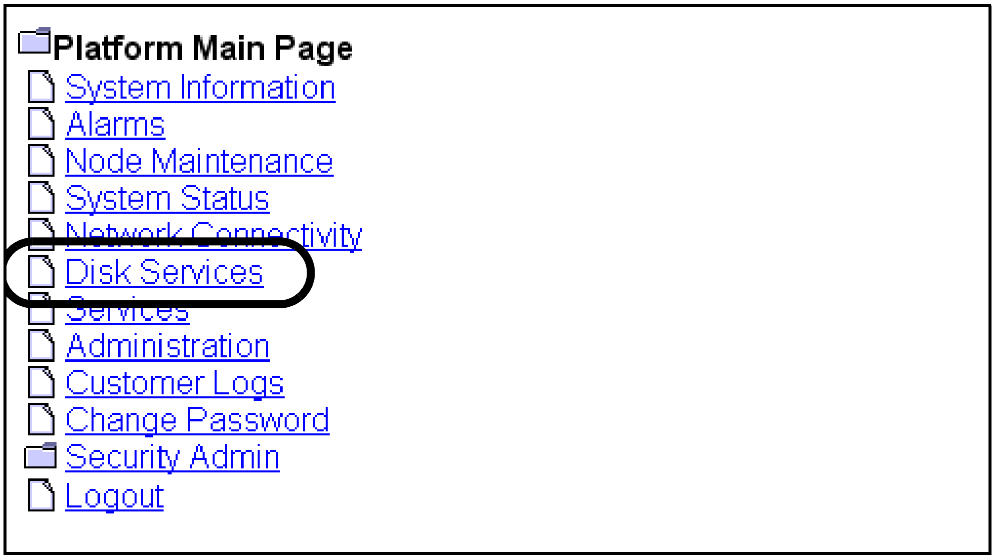
Action

At the Session Server unit chassis

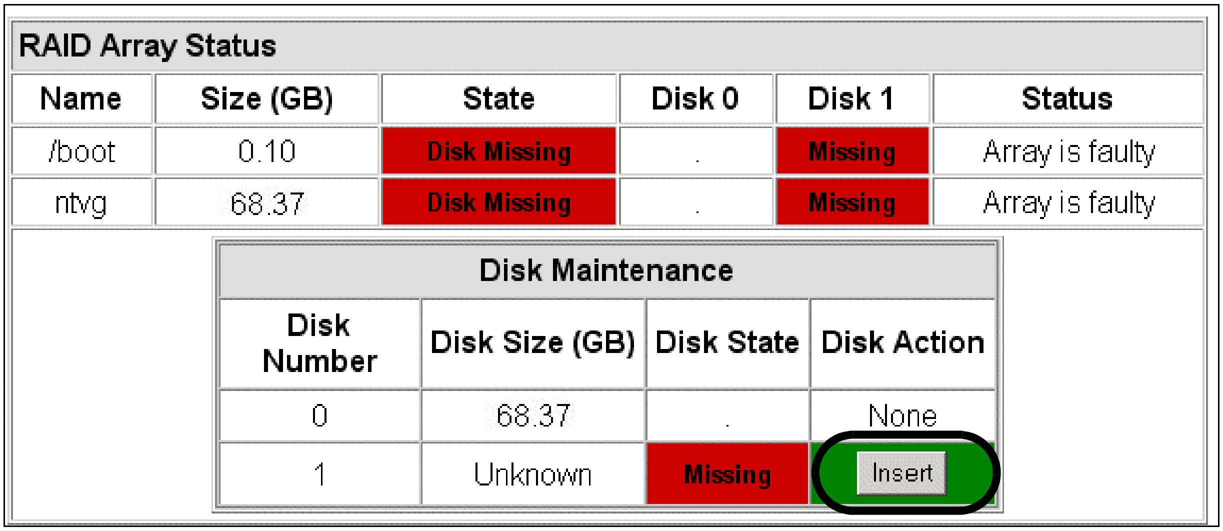
1 If applicable, log onto the inactive unit CS 2000 NCGL Platform Manager.

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.



RAID Array Status

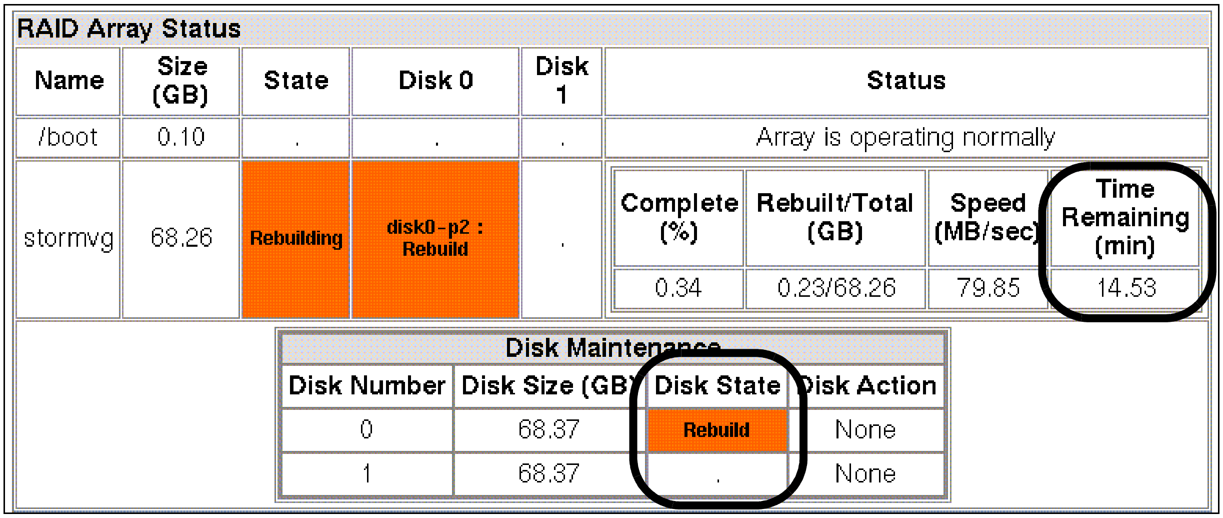
Name	Size (GB)	State	Disk 0	Disk 1	Status
/boot	0.10	Disk Missing	.	Missing	Array is faulty
ntvg	68.37	Disk Missing	.	Missing	Array is faulty

Disk Maintenance

Disk Number	Disk Size (GB)	Disk State	Disk Action
0	68.37	.	None
1	Unknown	Missing	Insert

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 (%)	Rebuilt/Total (GB)	Speed (MB/sec)	Time Remaining (min)
0.34	0.23/68.26	79.85	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 Replace a Session Server hard drive on page 81 to physically remove the hard drive from the unit.

6 This procedure is complete.

Replace a Session Server CDRW/DVD-ROM drive

Purpose of this procedure

Use this procedure to replace a damaged or failed CD+RW/DVD drive in a standby Session Server 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 Session Server unit fails to read a CDROM 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 procedure *Invoke a maintenance SwAct of the Session Server platform* found in the Session Server Security and Administration NTP, NN10346-611.

Materials

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

Action

At the CS 2000 NCGL Platform Manager

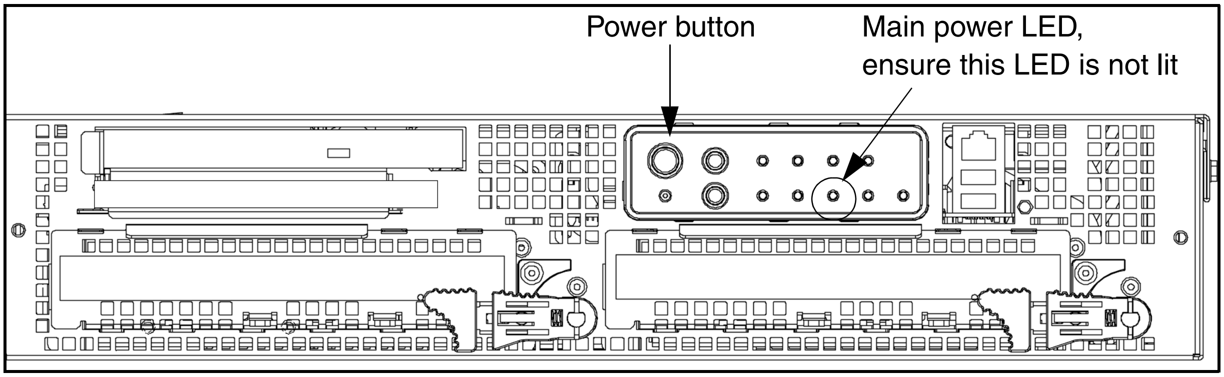
1 Execute procedure *Inhibit a system SwAct (Jam)* found in the Session Server Security and Administration NTP, NN10346-611.

> ***Note:*** Executing this procedure generates an alarm/log XTS355.

2 Shut down the standby Session Server unit by completing procedure *Halt (shutdown) a Session Server unit* found in the Session Server Security and Administration NTP, NN10346-611.

At the front panel of the Session Server chassis

3 Ensure that the chassis is powered down by examining the main power LED. Verify that the main power LED is not lit.

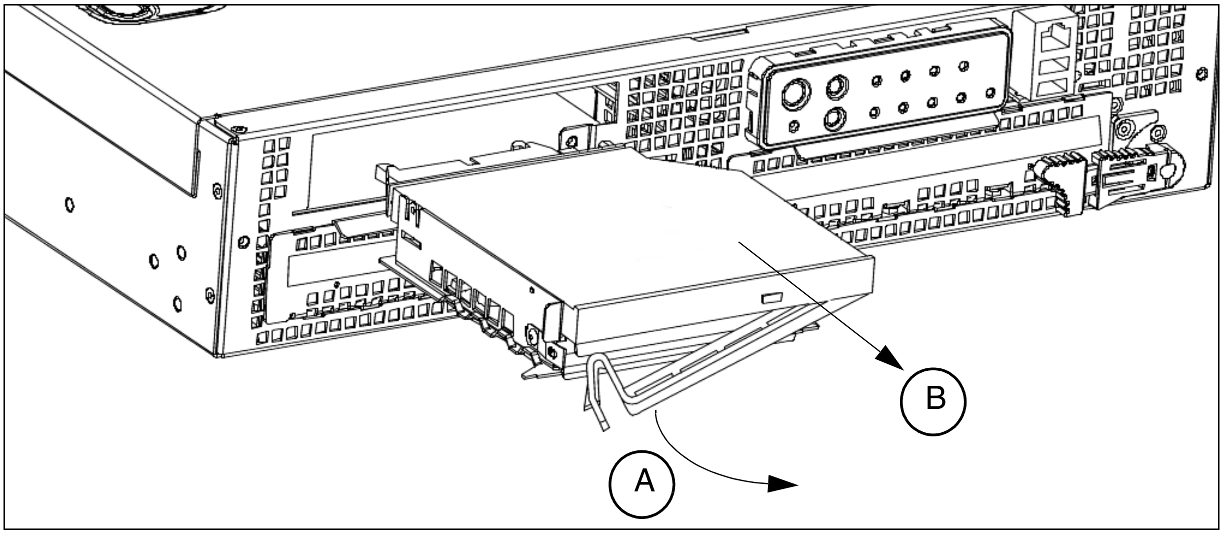


4 Put on an ESD wrist strap and fasten to a frame ground point.

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

5 Unseat the drive by pulling the blue horizontal lever on the front of the drive, as shown in view A. The lever is pulled from the left side of the drive and pivots on the right side of the drive. Refer to the figure below.

6 Slide the drive from the chassis, as shown in view B.



7 Pull the blue horizontal lever on the front of the replacement drive then slide the replacement drive into the chassis.

8 Press the blue horizontal lever on the front of the drive. The drive is fully seated when the horizontal lever is fully secured.

9 Press the power button to restore power to the chassis. Allow the unit to boot normally.

At the CS 2000 NCGL Platform Manager

10 After the unit has completed rebooting, refer to procedure View Session Server alarms on page 35,and verify that all alarms related to the drive failure condition and drive replacement have been cleared.

11 Execute procedure *Verify synchronization status of Session Server units*, found in the Session Server Security and Administration NTP, NN10346-611 to verify that both units are back in sync.

12 Execute procedure *Enable a system SwAct (Unjam)* found in the Session Server Security and Administration NTP, NN10346-611.

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

13 You have completed this procedure.

Replace a Session Server power supply

Purpose of this procedure

Use this procedure to replace an AC or DC power supply unit in a Session Server chassis. Each Session Server 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 procedure *Invoke a maintenance SwAct of the Session Server platform* found in the Session Server Security and Administration NTP, 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 section Alarms and LED fault indicators on the front panel on page 16 and
- 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

Rear power supply LED indicators

Power supply LED	Power supply condition
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
Risk of electrocution
Use caution when disconnecting power from the chassis.

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

Replacing a DC power supply

At the CS 2000 NCGL Platform Manager

1 Execute procedure *Inhibit a system SwAct (Jam)* found in the Session Server Security and Administration NTP, NN10346-611.

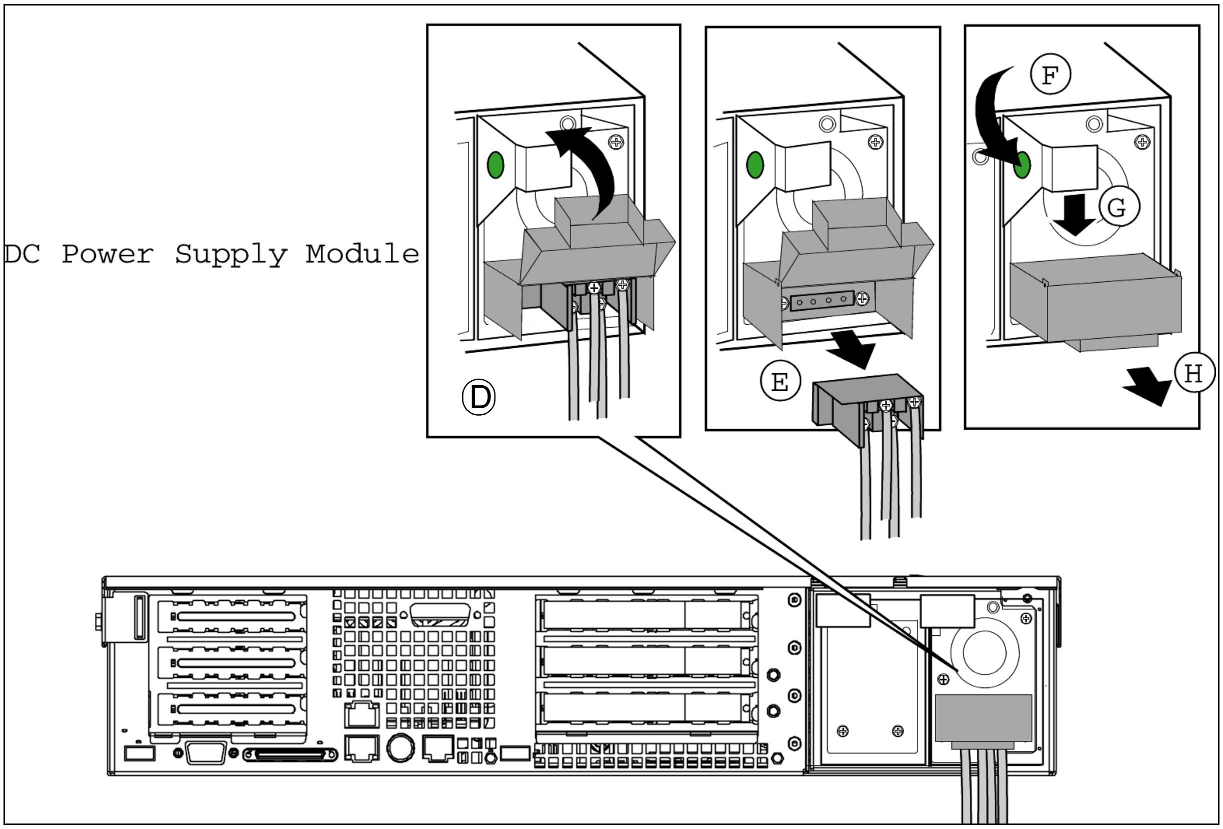
> ***Note:*** Executing this procedure generates an alarm/log XTS355.

At the Session Server chassis

2 Disconnect the power cord/cable from the DC source to remove power from the power supply.

3 Using a small flat-bladed screwdriver, unlatch the black connector cover from the connector base and flip connector cover up (refer to view D of the following illustration).

DC power supply replacement



4 Disconnect the DC power plug from power supply module by pulling the DC power plug rearward, as shown in view E of the previous illustration. Flip black connector cover down and re-latch connector cover to connector base.

5 Using a #2 Phillips screwdriver, remove the two screws that secure the terminal block to the DC power supply module.

6 Press in green button on the handle and pull the handle downward. At the same time, pull the DC power supply module out of DC power supply cage (views F, G, and H of the previous illustration).

7 When reinserting a DC power supply module, make sure the handle is in the downward position before sliding the DC power supply module into the power supply cage.

8 Secure the terminal block to the replacement power supply using two Phillips head screws.

9 For safety, ensure that the DC power supply cabling is properly and securely attached to its mount point(s).

At the CS 2000 NCGL Platform Manager

10 Referring to procedure View Session Server alarms on page 35, verify that all alarms related to this failure condition have been cleared.

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

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

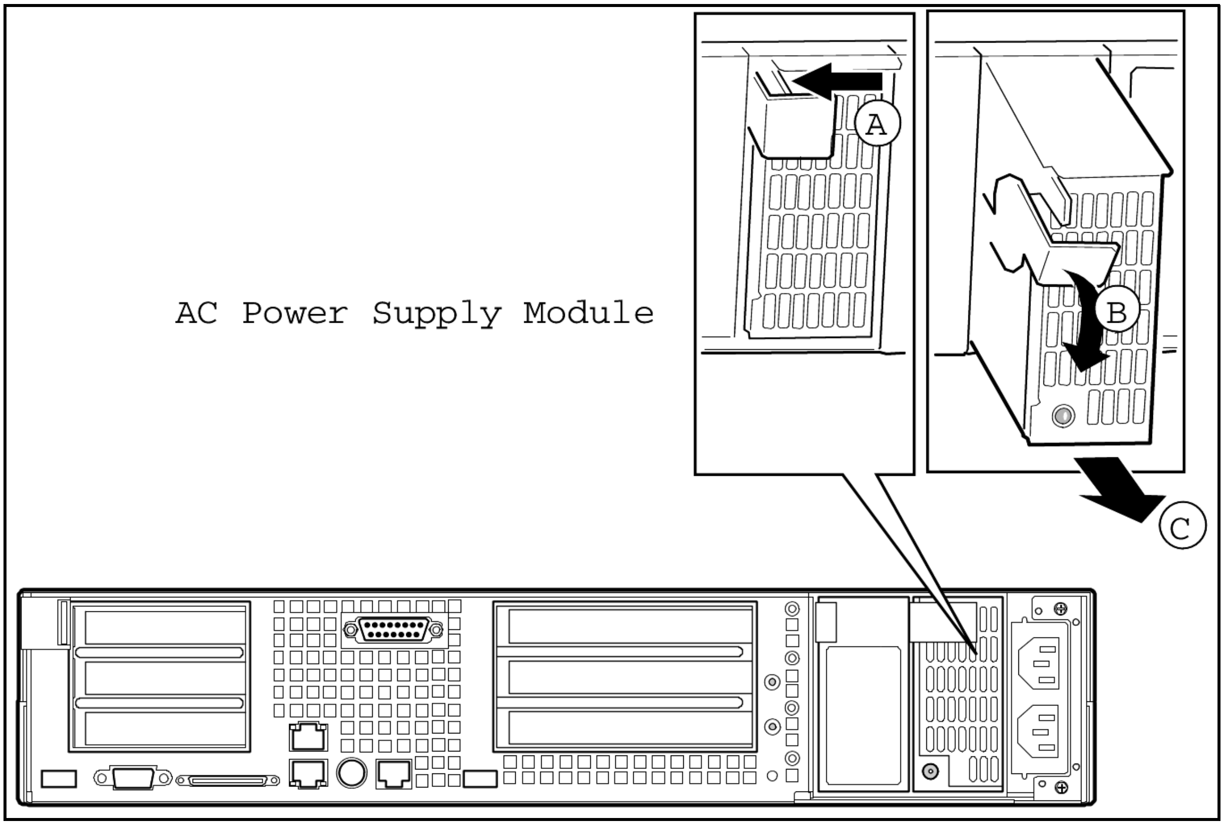
12 This procedure is complete.

Replacing an AC power supply

At the Session Server chassis

1 Press the locking tab inside of green handle inward as shown in view A of the following figure.

AC power supply replacement



2 Pull green handle slightly downward and rearward (as shown in view B), sliding the AC power supply module out of the AC power supply cage (as shown in view C).

3 When reinserting an AC power supply module, make sure the green handle (view B) is in the downward position before sliding AC power supply module into power supply cage.

4 For safety, ensure that the AC power supply cabling is properly and securely attached to its mount point(s).

At the CS 2000 NCGL Platform Manager

5 Referring to procedure View Session Server alarms on page 35, verify that all alarms related to this failure condition have been cleared.

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

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

7 This procedure is complete.

Prepare for a database restore on a Session Server unit

Purpose of this procedure

Use this procedure to prepare for a restoration of the SIP Gateway application database from a backup copy to the active unit.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of a high level upgrade activity, found in the Session Server Upgrades NTP, NN10349-461.

Limitations and Restrictions

CAUTION

Performing a restore of the SIP Gateway application database to the active unit is a service affecting activity and can cause data mismatches at the CS 2000 call server.

ATTENTION

For security reasons, you can only copy the database file from a remote server to the /users/mtc directory on the unit and you must use the secure copy command **scp** to perform this activity.

Automatic backup of the SIP Gateway application database occurs at 1:00 AM each day on both Session Server units. This configuration setting cannot be modified and does not impact the use of this procedure.

The name of the backup database file is *solid.db.* Do not modify this name.

Prerequisites

You must have secure copy (scp) access to the Session Server unit from the remote system or other server location from where the database backup file solid.db is copied.

Action

From the remote server where the backup database file is located

1 Log onto the remote server, locate and navigate to the directory where the backup copy of the database file is stored.

2 Secure copy the database file to the Session Server unit you are restoring a backup copy of the database to by typing

```
$ scp solid.db mtc@<SS_IP_address>:
```

and pressing the Enter key.

where

SS_IP_address
is the IP address of the Session Server unit

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

At the Session Server CLI or Integrated EMS client

3 Log onto the Session Server unit you are restoring a backup copy of the database to, and change to the root user.

4 Move the solid.db file you copied in step 2 from the /users/mtc directory to the /opt/apps/database/solid/backup directory by typing

```
$ mv /users/mtc/solid.db
/opt/apps/database/solid/backup
```

and pressing the Enter key.

5 Change directory to the backup database directory by typing

```
$ cd /opt/apps/database/solid/backup
```

and pressing the Enter key.

6 Verify that the correct version (based on the file date) of the solid.db database file that you want to restore is located in the directory by typing

```
$ ls -l /opt/apps/database/solid/backup
```

and pressing the Enter key.

7 Verify that the presence of files *solid.ini* and *solmsg.out* files are also in the /opt/apps/database/solid/backup directory.

> **ATTENTION**
>
> The restorebackup.sh script does not run if you do not have the solid.ini and solmsg.out files located in the correct directory.

8 If the solid.ini file is not present, copy it into the backup directory by typing

```
$ cp /opt/apps/database/solid/dbfiles/solid.ini
/opt/apps/database/solid/backup/solid.ini
```

and pressing the Enter key

9 If the solmsg.out file is not present, copy it into the backup directory by typing

```
$ cp
/opt/apps/database/solid/dbfiles/solmsg.out
/opt/apps/database/solid/backup/solmsg.out
```

and pressing the Enter key

10 Change the ownership of all files in the backup directory by typing

```
$ chown soliddb *
```

and pressing the Enter key.

11 Change the group of all files in the backup directory by typing

```
$ chgrp adm *
```

and pressing the Enter key.

12 Change the access permissions for all files in the backup directory by typing

```
$ chmod 600 *
```

and pressing the Enter key.

13 The database is now ready to be restored. You have completed this procedure. Return to the high-level activity.

Additional information

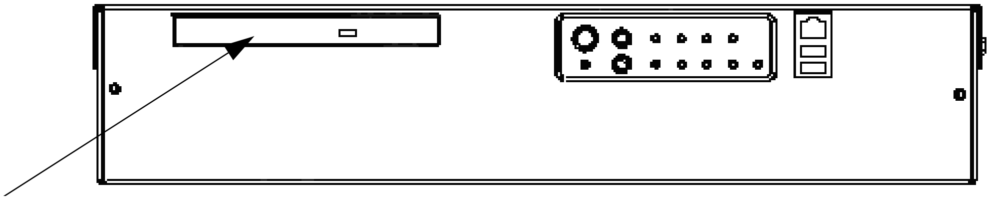
This section provides additional information regarding database restore activities.

To restore a backup database saved to a CD.

If you must restore a database backup that has been saved to a CD, you must first copy the database file from the CD to the default backup directory on the active Session Server unit. The selected backup database file must be restored to the following location:

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

To restore a backup of the database file to the backup directory, you must use a Session Server command line interface to copy the database file from a CD or CD-RW disk containing a copy of the back up database file to the opt/apps/database/solid/backup directory.



DVD/CDRW Drive location for restoring database backups

Ensure that you remove the CD disk from the DVD/CDRW drive, and store it in a safe place when you are done.

To restore a database backup saved to another system

If you must restore a database backup that has been saved to another system, you must first copy the database file from the remote system back to the default backup directory on the active Session Server unit. The selected backup database file must be restored to the following location:

/opt/apps/database/solid/backup

To restore a backup of the database to the backup directory you must use a Session Server command line interface to copy the database file solid.db from the remote system to the opt/apps/database/solid/backup directory. You may also be able to remote copy the backup database file from the remote system to the Session Server opt/apps/database/solid/backup directory. However, for security reasons, you may need to consult your site network administrator for instructions and permission to perform a remote copy.

Perform a database restore to a Session Server unit

Purpose of this procedure

Use this service impacting procedure to restore a SIP Gateway application database from a backup copy to the active Session Server units.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of a high level upgrade activity, found in the Session Server Upgrades NTP, NN10349-461.

Limitations and Restrictions

> **CAUTION**
>
> This procedure can only be executed on the active unit. Performing a restore of the SIP Gateway application database to the active unit is service affecting, and can cause data mismatches at the CS 2000 call server.

Prerequisites

You must first have completed procedure Prepare for a database restore on a Session Server unit on page 102.

Action

At the Session Server CLI or Integrated EMS client

1 Log onto the active Session Server unit you are restoring a backup copy of the database to, and change to the root user.

2 Change directories by typing

```
$ cd /opt/apps/database/solid_install
```

and pressing the Enter key.

3 Run the database restore script by typing

```
$ ./restorebackup.sh
```

and pressing the Enter key.

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

STGW700

Log report STGW700 is an information log that is generated by the SIP Gateway Call Processing Application.

This log may be generated when callp activity is interrupted or negatively impacted, such as during a Session Server upgrade.

Format

The format for log report STGW700 is as follows:

```
May 11 15:09:33 PGk-1 sipgwyappln: STGW700 NONE INFO SIPCALLP
supportedExtensionList was Null defaulted to 100rel

Aug 17 12:11:33 rtpg-duplex-unit-1 sipgwyappln: STGW700 NONE INFO SIPCALLP
No Active Server for SIP Link 5

Sep 13 15:50:59 cablab.ss.unit0 sipgwyappln: STGW700 NONE INFO LINKMTC
mgcHostName in Config Data is null

Sep 13 15:56:49 cablab.ss.unit0 sipgwyappln: STGW700 NONE INFO SIPCALLP
No Active Server for SIP Link 2

Sep 17 09:42:00 OTT2.SS0 sipgwyappln: STGW700 NONE INFO SIPCALLP
new message received with bad syntax. OTT2NGSS

Sep 17 09:42:25 OTT2.SS0 sipgwyappln: STGW700 NONE INFO SIPCALLP
new message received with bad syntax. CABLABNGSS
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPGW700	The component prefix and number of the log

Field	Value	Description
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	The type of trouble or info recorded
Label	sipcallp; linkmtc	Title label for the log
Description	LogMessage	Detailed description of the messages, refer to section Additional information.

Action

This is an information log only. No action is required. If this log persists, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

The following additional information applies to the Log Message field of the log entry:

- Failed to send SUBSCRIBE for detecting Fax Modem Tones
- AUDIT CALL FORCE RELEASE CALLID : 0022.4960-14-10-04-39.73@RALEIGH GWC 172.17.40.44 GCP State : 9
- LINKMTC mgcHostName in Config Data is null
- PostGainNotifyCallp Called on INACTIVE side
- Sync call to the standby unit failed with callid callId
- GCP NewCall received for Unsupported Agent: agentType
- No more CallDataBlocks to process CallID: callId
- Failed to add ISUP payload for call callId
- Remote SIP server not mapped for SIP LINK Index SipLinkIdx
- No Active Server for SIP Link SipLinkIdx
- HandleNewCall::Failed to Set MDB for callid callId
- No GCP Nodes to process call with callid callId
- Unauthorized Call attempt from MGC DestMgc

- HandleSipUPDATERequest::MDB Parsing for UPDATE failed for callid callId
- HandleACK::MDB Parsing for ACK failed for callid callId
- Handle200OKINVITERecvd::MDB Parsing for 200 OK INVITE failed for callid callId
- Incompatible media format received in 200 OK response to INVITE.
- Handle200OKINVITERecvd::Failed to send ACK for callid callId
- Handle200OKINVITERecvd::Failed to get Outbound Message for callid callId
- Handle200OKINVITERecvd::Failed to add 305 warning header for callid callId
- HandleReINVITE::MDB Parsing for Re INVITE failed for callid callId
- HandleSipINFORequest::MDB Parsing for INFO failed for callid callId
- HandleACKReINVITE::MDB Parsing for ACK failed for callid callId
- new message received with bad syntax start-line. msgDestName
- new message received with bad syntax. msgDestName
- Unable to Get Received Message (ACK) for callid callId
- Module:Procedure Null App Call Context
- Module:Procedure Unable to Get Received Message
- Media Error: CALLID: callId - 488 Not Acceptable Here Received
- Media Error: CALLID: callId - 606 Not Acceptable Received
- Incompatible media format, call rejected.
- Media type not available, call rejected.
- GCP Socket Open Failed
- Failed to get Active IP Address
- Bind for GCP Socket Failed
- supportedExtensionList was Null defaulted to 100rel
- NGSS Profile Data Creation Failed for Server sipServerName

DBSE300

Log report DBSE300 is generated any time a change in database connectivity is detected, specifically a loss of connectivity between the Session Server or Policy Controller provisioning watchdog program and the Solid database. It reports ‘No Solid DB Connection’ when database connectivity is lost and a critical “No Database Connection Alarm” is raised.

DBSE300 reports ‘Solid DB Connection Restored’ when database connectivity is reestablished and the critical “No Database Connection Alarm” is cleared.

Format

The format for log report DBSE300 is as follows:

```
Mar 22 21:27:48 vm0 alarmd:DBSE300 CRIT TBL No Solid DB Connection No
Database Connection

Mar 22 21:27:48 vm0 alarmd:DBSE300 CRIT TBL Solid DB Connection Restored
No Database Connection
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	DBSE300	The component prefix and number of the log
Severity	critical	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded

Field	Value	Description
Label	Alphanumeric	Title label for the log
Description	No Database Connection	Detailed description of the trouble or activity or activity

Action

Take corrective action to restore the unresponsive database.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC310

Log report SIPC310 is generated for the following alarm conditions

- indicates that “SIP CallP No Database Connection” is associated with the generation of the critical alarm due to a loss of connectivity between the SIP Gateway application database and the CallP application.
- indicates a SIP Gateway application overload condition when a call processing overload threshold is reached or when then SIP Gateway Application is no longer in an overload state. The logs are used, along with an associated major alarm to support overload control management for the Session Server.

Format

The format for log report SIPC310 is as follows:

```
Sep 13 19:20:14 cablab.ss.unit0 alarmd: SIPC310 CRIT TBL SIP CallP
NCGL=cablab.ss.unit0;Unit=0;SIPC No Database Connection

Sep 13 19:20:14 cablab.ss.unit0 alarmd: SIPC310 NONE TBL SIP CallP
NCGL=cablab.ss.unit0;Unit=0;SIPC Automatically cleared due to alarm
generator process death


Jan 12 13:26:47 RTP7-UNIT1 alarmd: SIPC310 MINOR TBL SIP CallP
NCGL=RTP7-UNIT1;Unit=1;SIPC Overload Condition Pending

Jan 12 13:27:07 RTP7-UNIT1 alarmd: SIPC310 MAJOR TBL SIP CallP
NCGL=RTP7-UNIT1;Unit=1;SIPC Overload Threshold Reached

Jan 12 13:27:17 RTP7-UNIT1 alarmd: SIPC310 NONE TBL SIP CallP
NCGL=RTP7-UNIT1;Unit=1;SIPC Overload Alarm Cleared
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log

Field	Value	Description
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPC310	The component prefix and number of the log
Severity	critical/major/minor	The log severity (may be related to alarm severity)
Event Type	Trouble	The type of trouble or info recorded
Label	SIP CallP	Title label for the log
Description	No Database Connection or Overload Threshold Reached	See a detailed description of the trouble in the log details.

Action

Reestablish connectivity between SIP Gateway application callp process and the database.

Associated OM registers

If a major alarm/log is generated, indicating an overload threshold is reached, then the associated Session Server SIPGW_CALLP OM group OVRLD_CALLS_REJECTED register is incremented. Refer to the Session Server Performance Management NTP, NN10342-711 for details and instructions for viewing this OM group.

Additional information

This log report requires no additional information.

SIPC301

Log report SIPC301 titled *All Incoming SIP Msgs Blocked* is a critical log that is generated when the SIP Gateway Call Processing Application does not receive any incoming SIP messages due to Access Control List (ACL) being enabled and no valid entries in Remote SIP server or ACL.

Format

The format for log report SIPC301 is as follows:

```
Nov 12 21:32:08 loopback sipgwyappln: SIPC301 CRIT TBL All SIP Incoming
Msgs Blocked
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPC301	The component prefix and number of the log
Severity	Critical	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	All SIP Incoming Msgs Blocked	Detailed description of the trouble or activity or activity

Action

No action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC650

Log report SIPC650, titled *IP CallP No Data Found,* is an informational log that is generated when the SIP Gateway Call Processing Application goes to get data from the database for a particular table and no data is found.

Format

The format for log report SIPC650 is as follows:

```
Nov 12 21:32:08 loopback sipgwyappln: SIPC650 NONE INFO SIP CallP No Data
Found: SIPT GWC
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPC650	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	No Data Found	Detailed description of the trouble or activity

Action

No action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC750

Log report SIPC750, titled *SIP Access Control List*, is generated when the SIP Gateway Call Processing Application drops incoming SIP messages due to Access Control List restrictions.

A Minor, Major or Critical log is generated based on the number of SIP messages dropped in last 15 minutes:

- Minor Threshold: 25 messages
- Major Threshold: 100 messages
- Critical Threshold: 500 messages

Format

The format for log report SIPC750 is as follows:

```
Nov 12 21:32:08 loopback sipgwyappln: SIPC750 CRIT TBL Incoming 600 SIP
messaged dropped
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPC750	The component prefix and number of the log
Severity	MIN/MAJ/CRIT	The log severity (may be related to alarm severity)
Event Type	INFO	The type of trouble or info recorded

Field	Value	Description
Label	Alphanumeric	Title label for the log
Description	Incoming SIP messages dropped	Detailed description of the trouble or activity

Action

No action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPM300

Log report SIPM300 is a SIP Maintenance Trouble information log. It is generated by the SIP Gateway application maintenance process for a variety of unexpected reasons or conditions which may include:

- messaging failures
- failure to set a timer
- timer expirations that should not occur
- failure to write to the “SA_State” file
- process deaths
- failure to start the callp process

The SIP Gateway application generates log report SIPM300 in addition to raising the SIPM300 alarm.

Format

The format for log report SIPM300 is as follows:

```
 Apr  6 13:24:47 RTPF-SIP0 sipgwymtc: SIPM300 NONE TBL SIP Gateway
 Maintenance Trouble
{Reason Text : SIP Gateway Application process death]
[Error Code  : -1]
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwymtc	Identifies the NGCL or application process unit that generates the report
Log Number	SIPM300	The component prefix and number of the log

Field	Value	Description
Severity	None	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded; this is an information only log
Label	SIP Gateway Maintenance Trouble	Title label for the log
Description	Reason text	Detailed description of the trouble or activity; see section Additional Information for a detail list of Trouble reasons

Action

No action is required. This is an information log only.

Associated OM registers

This log report has no associated OM registers.

Additional information

The following additional information applies to the Description field of the log entry:

- [Reason Text: <TroubleReason>]
  - — SAM to Web Server message send failure
  - — SAM to SIP CallP message send failure
  - — Been Terminating too long. Timer Expired.
  - — SAM Wait Timer Messaging Timeout
  - — SAM/SIP CallP Audit Messaging Timeout
  - — Failed to set the SIP Gateway Application state
  - — SIP Gateway Application process death
  - — Failed to start the SIP Gateway Application process
  - — Failed to set a timer
  - — SIP CallP created, but not in the requested state
  - — SIP CallP created, but failed to reply to SAM
  - — SIP CallP on the Inactive failed to respond to a request
  - — SIP CallP on the Inactive failed to get to the requested state

- — SAM failed to send a reply to a platform swact request
- — SAM failed a Swact Request due to an invalid Swact Request
- — SAM failed a Graceful Swact Request due to being marked to do a COLD Swact
- — SAM failed a Swact Precheck Request due to option = FORCE
- — SAM failed a Swact Precheck or PreSwact request due to option = NOW
- — SAM failed a Swact Request due to an invalid option
- — SAM failed a Swact Request due to an unacceptable platform status
- — SAM failed a Swact Request due to not being In-Sync
- — Swact Precheck Failed due to failure received in SIP CallP response
- — Swact Precheck Failed due to failure to notify SIP CallP
- — Swact Precheck Failed due to timeout waiting on SIP CallP response
- — Swact PreSwact Failed due to failure received in SIP CallP response
- — Swact PreSwact Failed due to failure to notify SIP CallP
- — Swact PreSwact Failed due to timeout waiting on SIP CallP response
- — Swact AbortSwact Failed due to failure received in SIP CallP response
- — Swact AbortSwact Failed due to failure to notify SIP CallP
- — Swact AbortSwact Failed due to timeout waiting on SIP CallP response
- — Swact PostSwact Failed due to failure received in SIP CallP response
- — Swact PostSwact Failed due to failure to notify SIP CallP
- — Swact PostSwact Failed due to timeout waiting on SIP CallP response
- — Disable PreCheck Failed due to failure received in SIP CallP response
- — Disable PreCheck Failed due to timeout waiting on SIP CallP response
- — Disable PreDisable Failed due to failure received in SIP CallP response

- — Disable PreDisable Failed due to timeout waiting on SIP CallP response
- — Disable AbortDisable Failed due to failure received in SIP CallP response
- — Disable AbortDisable Failed due to timeout waiting on SIP CallP response
- — Swact PreSwact Failed due to failure to notify SIP CallP
- — Disable PreDisable Failed due to failure received from the mate SAM
- — Disable PreDisable Failed due to failure to notify SIP CallP
- — Disable PreDisable Failed due to timeout waiting on mate SAM response
- — Disable AbortDisable Failed due to failure received from the mate SAM
- — Disable AbortDisable Failed due to failure to notify SIP CallP
- — Disable AbortDisable Failed due to timeout waiting on mate SAM response
- — Disable Request Failed due to Callback called with existing disable request outstanding
- — Disable Request Failed due to Callback called when platform not active and enabled
- — Disable Inactive Failed due to Callback called when platform not in duplex
- — Disable Inactive PreCheck Failed due to Callback called when SAM had a conflicting wait state
- — Disable Inactive PreDisable Failed due to Callback called when SAM had a conflicting wait state
- — Disable Inactive AbortDisable Failed due to Callback called when SAM had a conflicting wait state
- — Disable PreCheck Failed due to failure to notify SIP CallP
- — Disable PreDisable Failed due to failure to notify the Mate SAM
- — Disable AbortDisable Failed due to failure to notify the Mate SAM
- — Disable Active Failed due to Callback called when platform was in duplex
- — Disable Active Graceful Failed due to Callback called when SIP State was not suspended
- — Disable Callback called with invalid request

- — SAM received a response to a Swact request that contained an invalid request
- — SAM received a response to a Swact request that contained an invalid option
- — SAM received a response to a Swact request that contained an invalid result
- — Mate SAM failed a Prepare For COLD Swact request, reverting to a WARM swact
- — Failed to notify the Mate SAM to Prepare For COLD Swact request, reverting to a WARM swact
- — Timed out waiting on the Mate SAM to respond to a Prepare For COLD Swact request, reverting to a WARM swact
- — SAM failed to register with DataSync

- <ErrorCode>: This is an integer code used for debugging. -1 is the default value

SIPM301

Log report SIPM301 generated when its associated critical alarm is raised because the SIP Gateway Application has transitioned to a state that indicates it should be in-service, but is actually not, while the active Session Server unit running the SIP Gateway application is in an enabled operational state. This “system busied” (SYSB) state is represented by state values as follows:

- Administrative State = Unlocked
- Operational State = Disabled
- Procedural Status = “-” or Not Terminating
- Control Status = “-” or Not Suspended

Call processing cannot occur while the SIP Gateway application is in this state.

The SIP Gateway application generates log report SIPM301 in addition to raising or clearing the alarm.

Format

The format for log report SIPM301 is as follows:

```
Apr  6 14:39:00 RTPF-SIP0 alarmd: SIPM301 CRIT TBL  SIP Gateway Maintenance
Trouble Alarm :
NCGL=RTPF-SIP0;Unit=0; SIP Gateway Application System Busy


Apr  6 14:39:01 RTPF-SIP0 alarmd: SIPM301 NONE TBL  SIP Gateway Maintenance
Trouble Alarm:
NCGL=RTPF-SIP0;Unit=0; SIP Gateway Application System Busy - Alarm Cleared
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log

Field	Value	Description
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPM301	The component prefix and number of the log
Severity	Critical or None	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded
Label	SIP Gateway Maintenance Trouble Alarm	Title label for the log
DeviceInfo	Alphanumeric	Info that specifies the device to which the alarm pertains
AlarmRaiseLowerText	Alphanumeric	Text indicating whether the SIP Gateway Application System Busy alarm has been raised or cleared

Action

When the SIP Gateway Application transitions out of this state (automatically or manually), this alarm is lowered. It is also lowered if the Session Server unit the application is running on leaves the enabled operational state.

When this alarm is raised, the system attempts recovery immediately. If immediate recovery is not successful, reattempts are made automatically every 30 seconds.

A manual method to attempt recovery from this alarm condition can be performed by executing the following procedures in order, found in the *Session Server Security and Administration NTP, NN10346-611*:

- Perform procedure *Lock the SIP Gateway application*
- Perform procedure *Unsuspend the SIP Gateway application*
- Perform procedure *Unlock the SIP Gateway application*

If the alarm condition persists, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPM302

Log SIPM302 is generated by a major alarm that is raised when the Session Server - Trunks platform that the SIP Gateway Application is running on is in a duplex configuration with both units in an enabled operational state, and the SIP Gateway application state goes out of sync between the two Session Server - Trunks units.

This alarm is cleared if the SIP Gateway application state becomes sync'ed between the two Session Server - Trunks units and the alarm is cleared.

Format

The format for log report SIPM302 is as follows:

```
Apr 13 09:13:15 RTPF-SIP0 alarmd: SIPM302 MAJOR TBL
SIP Gateway Maintenance Sync Trouble Alarm : NCGL=RTPF-SIP0;Unit=0; SIP
Gateway Application Mtc Out Of Sync

Apr 13 09:13:45 RTPF-SIP0 alarmd: SIPM302 NONE TBL
SIP Gateway Maintenance Sync Trouble Alarm : NCGL=RTPF-SIP0;Unit=0; SIP
Gateway Application Mtc Out Of Sync - Alarm Cleared
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPM302	The component prefix and number of the log
Severity	Major or None	The log severity (may be related to alarm severity)
Event Type	TBL (trouble)	The type of trouble or info recorded

Field	Value	Description
Label	SIP Gateway Maintenance Trouble Alarm	Title label for the log
DeviceInfo	Alphanumeric	Info that specifies the device to which the alarm pertains
AlarmRaiseLowerText	Alphanumeric	Text indicating whether the SIP Gateway Application Mtc Out Of Sync alarm has been raised or cleared

Action

The certificates must be provisioned on both the active and inactive units. If the certificates are only provisioned on the active unit, the CallP application will (under default behavior) fail to start on the inactive unit, and the active unit will report the out-of-sync alarm.

Check that the certificates are in /opt/base/share/ssl on the inactive unit.

- If the certificates aren't in /opt/base/share/ssl, perform the *Copy security certificates to the mate unit* procedure found in the *Session Server - Trunks Security and Administration NTP, NN10346-611*.
- If the certificates are in /opt/base/share/ssl, and the alarm persists, then proceed to lock/suspend/unsuspend/unlock the SST as described below.

The SIP Gateway application should attempt to sync itself automatically every 30 seconds. If there are repeated sync failures, a manual method to attempt recovery from this alarm condition can be performed by executing the following procedures in order, found in the *Session Server - Trunks Security and Administration NTP, NN10346-611*.

- Perform procedure *Lock the SIP Gateway application*
- Perform procedure *Suspend the SIP Gateway application*
- Perform procedure *Unsuspend the SIP Gateway application*
- Perform procedure *Unlock the SIP Gateway application*

If the alarm condition persists, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPM500

Log report SIPM500 is a SIP Maintenance State Change information log. The state of the SIP Application is actually updated by the callp process, but, the SIP Application maintenance message handler process thread keeps track of the last known state. When a message is received from callp, the SIP application maintenance process, running on the Session Server, checks to see if the current state matches the last known state. If it does not, then a state change log is generated. If the SIP application maintenance process updates the state, it also generates a state change log at the same time.

The SIP Gateway application generates log report SIPM500 in addition to raising the associated alarm.

State change logs include content indicated the FROM and TO states in external format, an indication of whether a user requested the change (if it was not system generated), a reason for the change, and a userid of the user that requested the change.

Format

The format for log report SIPM500 is as follows:

```
Apr 12 10:45:06 RTPF-SIP0 sipgwymtc: SIPM500 NONE INFO SIP Gateway
       Maintenance State Change
        [Administrative : Locked          -> Unlocked]
        [Operational    : Enabled         -> Enabled]
        [Control        : Not Suspended   -> Not Suspended]
        [Procedural     : Not Terminating -> Not Terminating]
        [User Requested : Yes]
        [Reason         : Unlock command issued]
        [Web User ID    : mtc]
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID or device name	Alphanumeric	The hostname or host id of the unit that generated the log

Field	Value	Description
Process Name	sipgwymtc	Identifies the NGCL or application process unit that generates the report
Log Number	SIPM500	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	SIP Maintenance State Change	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity; see section: Additional information on page 137

Action

No action is required. This is an information log only.

Associated OM registers

This log report has no associated OM registers.

Additional information

The following additional information applies to the Description field of the log entry:

- [Administrative: <AdminFrom> -> <AdminTo>]
  - Locked
  - Unlocked
  - Shutting down
- [Operational: <OperFrom> -> <OperTo>]
  - Enabled
  - Disabled
- [Control: <CtrlFrom> -> <CtrlTo>]
  - Suspended
  - Not Suspended
- [Procedural: <ProcFrom> -> <ProcTo>]
  - Terminating
  - Not Terminating
- [User Requested: <Yes|No>]
  - Yes
  - No
- [Reason: <StateChangeReason>]
  - Unsuspend command issued
  - Suspend command issued
  - Lock command issued
  - Lock command in progress
  - Lock operation complete
  - Unlock command issued
  - Shut Down command issued
  - Shut Down operation complete
  - System originated change of state
  - Timeout waiting to terminate call processing
  - Audit Failure
  - Timer Problem
  - Data corruption detected

- [Web User ID: <webuserid>]
  - If applicable, this is the web interface login ID of the user performing the maintenance that caused the state transition. If not applicable, this value is left blank. Refer to the *Overview* section of the *Session Server Security and Administration NTP, NN10346-611* for information about login IDs and user IDs and authorization categories

SIPS300

Log report SIPS300, titled T*LS dropped number of requests over time*, is generated during the alarming of dropped connection requests. This can occur either due to the connection request threshold being crossed, or due to the SIP Gateway application attempting to use TLS when TLS has not been enabled. The severity of the alarm indicates the threshold that was crossed: 10 dropped connection requests within a minute generates a minor alarm, 50 dropped requests generates a major alarm, and 100 or more dropped requests generates a critical alarm. The following message descriptions are generated:

- Dropped <number> Connections requests
- Automatically cleared due to alarm generator process death

The alarm is raised for a minimum of 30 minutes and clears on its own if the problem does not recur. Associated log SIPS600 may also be generated with this log.

Format

The format for log report SIPS300 is as follows:

```
Oct  6 20:19:53 comit.ngss.unit1 alarmd: SIPS300 MINOR TBL TLS
Dropped Connection
Request NCGL=comit.ngss.unit1;Unit=1;SIPS Dropped 10 Connections requests
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln, alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS300	The component prefix and number of the log

Field	Value	Description
Severity	None, Minor, Major, Critical	The log severity (may be related to alarm severity)
Event Type	Trouble	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see bullet list above	Detailed description of the trouble or activity

Action

Monitor incrementing (pegging) of the OM register TLS_CONNECTION_REQUESTS_DROPPED in Session Server OM group SIPGW_TLS and ensure that the event doesn't continuously recur. If it does recur, use the Session Server Configuration Management NTP, NN10338-511, to check the threshold values for the TLS connections. Consider setting the TLS connections value to a higher number, based on the number of connections expected in the given time period. If the TLS connections value is adequate, check to ensure the integrity of the central office LAN. Determine if an intruder has compromised network security. The log/alarm will be raised at least 30 minutes, and if the problem has ceased, a clear alarm log will be generated.

Associated OM registers

Refer to the Session Server Performance Management NTP, NN10342-711 for details and instructions for viewing registers in the SIPGW_TLS OM group.

Additional information

The associated log SIPS600 may also be generated with this log.

SIPS301

Log report SIPS301, titled *TLS failed certificate authentications over time*, is generated by authentication failure events. This information log indicates the reason for the authentication failures and the level of trouble. A critical alarm indicates a very serious problem while a minor alarm can indicate transient failures or the beginning of a series of authentication failures.

The following message descriptions are generated:

- Failed <number> certificate authentications:
  which indicates the number of times this event occurred in the last minute before the alarm was raised.
- Automatically cleared due to alarm generator process death

Format

The format for log report SIPS301 is as follows:

```
Feb 9 13:03:50 comit.ngss.unit1 alarmd: SIPS301 CRIT TBL TLS Failed Authentication
NCGL=comit.ngss.unit1;Unit=0;SIPS Failed 28 certificate authentications

Feb 9 13:08:10 comit.ngss.unit1 alarmd: SIPS301 NONE TBL TLS Failed Authentication
NCGL=comit.ngss.unit1;Unit=0;SIPS Automatically cleared due to alarm
generator process death
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS301	The component prefix and number of the log

Field	Value	Description
Severity	None, Minor, Major, or Critical	The log severity (may be related to alarm severity)
Event Type	Info, Trouble	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see the bullet list above	Detailed description of the trouble or activity

Action

On a major or critical severity log, check to ensure that the security certificate and key provided to the SIP Gateway application are in the correct directory (as pointed to by the database entry). Then ensure that the certificate and key files are not corrupted or altered. Use the Certificate Management Tool to ensure that the certificate and key files are meant to be used together. Contact your next level of support or Nortel GNPS for support with these activities.

Associated OM registers

Monitor incrementation of the OM registers TLS_CONNECTION_ REQUESTS_FAILED and TLS_HANDSHAKE_AUTHENTICATION_ FAILED in Session Server OM group SIPGW_TLS. Refer to the Session Server Performance Management NTP, NN10342-711 for details and instructions on viewing registers in the SIPGW_TLS OM group.

Additional information

This log report has no additional information.

SIPS302

Log report SIPS302, titled TLS Local certificate is expiring soon, is generated as a result of regular alarm process checks to ensure the local server certificate continues to be valid. The expiration date contained in the certificate is checked on a daily basis. As the expiration date of the certificate approaches, an alarm is raised and log generated within 31 days (minor alarm), 15 days (major alarm), or 5 days (critical alarm) of the expiration date. For certificates that have already expired, a critical alarm and log are generated, and authentication failures (log SIPS601) will be generated for any connections that are attempted.

Format

The format for log report SIPS302 is as follows:

```
Oct 8 13:14:17 comit.ngss.unit0 alarmd: SIPS302 MINOR TBL TLS
Local Certificate is Expiring Soon
NCGL=comit.ngss.unit0;Unit=0;SIPS TLS Local Certificate is Expiring Soon
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS302	The component prefix and number of the log
Severity	None, Minor, Major, or Critical	The log severity (may be related to alarm severity)
Event Type	Info, Trouble	The type of trouble or info recorded

Field	Value	Description
Label	TLS	Title label for the log
Description	Local Certificate is Expiring Soon	Detailed description of the trouble or activity

Action

Use the Certificate Management Tool to create a new self-signed certificate (if using self-signed certificates) or to generate a certificate signing request (for creating CA-signed certificates). Refer to the Session Server Security and Administration NTP, NN10346-611, for procedures on creating new CA-signed or self-signed security certificates. Add the new certificate to the system using procedures in the Session Server Configuration Management NTP, NN10338-511.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SIPS305

Log report SIPS305, titled *TLS initialization logs*, is generated during the initialization (unlock) of the SIP Gateway application. It indicates that there is a problem with the initialization of the application. The following message descriptions may be generated:

- TLS Local Key and Certificate do not match
- TLS Failed client init
- TLS Failed Server init
- TLS Failed to load Certificate
- TLS Failed to load Key
- TLS Failed to Init
- TLS Failed to get pointer
- TLS Failed to create thread

Format

The format for log report SIPS305 is as follows:

```
Feb 9 13:11:39 comit.ngss.unit1 sipgwyappln: SIPS305 CRIT INIT TLS
TLS Failed to load Key
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS305	The component prefix and number of the log
Severity	Critical	The log severity (may be related to alarm severity)

Field	Value	Description
Event Type	Initialization	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see details above for the description	Detailed description of the trouble or activity

Action

Perform the following activities in the order listed:

- Check to ensure that the certificate and key files provided to the SIP Gateway application are in the correct directory (as pointed to by the database entry).
- Ensure that the certificate and key files themselves are not corrupted or altered.
- Ensure that the certificate and key files are meant to be together (by running the Certificate Management Tool). If necessary, contact your next level of support or Nortel GNPS for assistance with this activity.
- Once the problem is resolved, and the SIP Gateway application is initialized (unlocked) again, there will be 3 logs indicating problem resolution: SIPM500, SIPS605, SIPS604.

Associated OM registers

This log report has no associated OM registers.

Additional information

Normally, the Certificate Management Tool will provision the certificate and key files properly. If this tool has not been used to successfully set up security certificates prior to attempting to bring the SIP Gateway application into service, unexpected results could occur. Extra information as to the cause of the problem will likely reside in the SIP Gateway application initialization trace logs provided in the /opt/apps/logs directory. Look for entries labeled: siptrace.<date>.server.<pid>.

SIPS600

Log report SIPS600, titled *TLS connection request dropped*, is generated during the connection setup of SIP Gateway application callp processes. This is an information log only and is not associated with an alarm. The following message descriptions are generated:

- Dropped TLS Handshake request, monitor OMs
- Dropped TLS Handshake request, TLS is not enabled

Format

The format for log report SIPS600 is as follows:

```
Oct 8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS600 MINOR INFO TLS
Dropped TLS Handshake request, monitor OMs
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS600	The component prefix and number of the log
Severity	Minor	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see bullet list above	Detailed description of the trouble or activity

Action

If the message “Dropped TLS Handshake request, monitor OMs” is displayed only once or twice, there is likely a transient connection problem. Monitor incrementing of the OM register TLS_CONNECTION_REQUESTS_DROPPED in Session Server OM group SIPGW_TLS and ensure that the event doesn’t continuously recur. If it does recur, use the Session Server Configuration NTP, NN10338-511, to check the threshold values for the TLS connections. Consider setting the TLS connections value to a higher number, based on the number of connections expected in the given time period. If the TLS connections value is adequate, check to ensure the integrity of the central office LAN. Determine if an intruder has compromised network security.

If the message “TLS is not enabled” is displayed, refer to other available logs and ensure that the SIP Gateway application initialized properly.

Associated OM registers

Refer to the Session Server Performance Management NTP, NN10342-711 for details and instructions for viewing registers in the SIPGW_TLS OM group.

Additional information

This log report has no additional information.

SIPS601

Log report SIPS601, titled *TLS authentication failure <reason>*, is generated from TLS authentication failure events. This information log indicates the reason for the authentication failures. Refer to the Additional information section for log message details.

Format

The format for log report SIPS601 is as follows:

```
Oct  8 16:36:56 comit.ngss.unit1 sipgwyappln: SIPS601 MINOR INFO TLS
common name: 47.129.118.195, reason: certificate has expired
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS601	The component prefix and number of the log
Severity	Minor	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	TLS	Title label for the log

Field	Value	Description
Common Name	The common name in the security certificate that the remote SIP server uses.	The common name in the X.509 security certificate that the remote SIP server is presenting to the Session Server.
Description	Refer to Additional information	Detailed description of the trouble or activity

Action

This information log report requires no action; however, an excessive amount of authentication failures may have associated alarms. Check for additional alarms or associated OMs.

Associated OM registers

Monitor incrementation of the OM registers TLS_CONNECTION_REQUESTS_FAILED and TLS_HANDSHAKE_AUTHENTICATION_FAILED in Session Server OM group SIPGW_TLS. Refer to the Session Server Performance Management NTP, NN10342-711 for details and instructions for viewing registers in the SIPGW_TLS OM group.

Additional information

One or more of the following detailed reasons may be part of the information log:

- unable to get issuer certificate
- unable to get certificate CRL
- unable to decrypt certificate’s signature
- unable to decrypt CRL’s signature
- unable to decode issuer public key
- certificate signature failure
- CRL signature failure
- certificate is not yet valid
- CRL is not yet valid
- certificate has expired
- CRL has expired

- format error in certificate’s notBefore field
- format error in certificate’s notAfter field
- format error in CRL’s lastUpdate field
- format error in CRL’s nextUpdate field
- out of memory
- self signed certificate
- self signed certificate in certificate chain
- unable to get local issuer certificate
- unable to verify the first certificate
- certificate chain too long
- certificate revoked
- invalid CA certificate
- path length constraint exceeded
- unsupported certificate purpose
- certificate not trusted
- certificate rejected
- application verification failure
- subject issuer mismatch
- authority and subject key identifier mismatch
- authority and issuer serial number mismatch
- key usage does not include certificate signing
- unable to get CRL issuer certificate
- unhandled critical extension
- key usage does not include CRL signing
- unhandled critical CRL extension

SIPS604

Log report SIPS604, titled *TLS initialization logs*, is generated during initialization (unlock) of the SIP Gateway application, indicating when the current local certificate will expire, using the format Year=<YYYY>, Month = <MM>, Day = <DD>. This is an information log only and is not directly associated with an alarm.

Format

The format for log report SIPS604 is as follows:

```
Oct 8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS604 NONE INFO TLS
Local Certificate Expires: Year=2005, Month = 10, Day = 8
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS604	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see details above for the description	Detailed description of the trouble or activity

Action

No action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

No additional information is currently available.

SIPS605

Log report SIPS605,titled *TLS initialization logs*, is generated during initialization (unlock) of the SIP Gateway application, indicating that TLS Security is enabled. This is an information log only and is not directly associated with an alarm. A SIPS604 log may be generated with this log.

Format

The format for log report SIPS605 is as follows:

```
Oct 8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS605 NONE INFO TLS
TLS Security Enabled
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS605	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see details above for the description	Detailed description of the trouble or activity

Action

No action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

No additional information is currently available.

SIPS606

Log report SIPS606, titled *TLS attempt to add trusted certificate failed*, is generated when there is a problem importing the trusted certificate provisioned into the database using the CS 2000 Session Server Manager. This is an information log only and is not associated with an alarm. The following message descriptions are generated:

- Failed to add Trusted CA name server
- Failed to add Trusted CA name <name>

Format

The format for log report SIPS606 is as follows:

```
Oct 8 13:41:47 comit.ngss.unit1 sipgwyappln: SIPS606 NONE INFO TLS
Failed to add Trusted CA name <servername>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS606	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	see bullet list above	Detailed description of the trouble or activity

Action

The security certificate being used is not correct or has become corrupted, and is unable to be loaded by the SIP Gateway application. Try to reprovision the certificate (using a different name) or delete the certificate, then re-add it. Refer to the *Session Server - Trunks Configuration Management*, NN10338-511, for procedures on provisioning existing security certificates. Refer to the *Session Server - Trunks Security and Administration*, NN10346-611, for procedures on creating new CA-signed or self-signed security certificates.

If the certificate identified in the log report is this server’s own certificate, then delete the entry from the list of Remote Trusted Certificates. Because the certificate is for this server and is not used by the running SIP Gateway application, it is not necessary to restart the SIP Gateway application.

Associated OM registers

This log report has no associated OM registers.

Additional information

If log SIPS606 is generated along with authentication log SIPS301, it is likely due to the failure to properly provision the trusted certificate for the remote server. Retrieve the remote server’s public self-signed certificate and add it to the database.

Log SIPS606 can be generated when restarting the SIP Gateway if the server's own certificate is added to the remote trusted certs list. The log may appear twice indicating a failure to add the trusted CA. However, TLS is enabled and callp functions properly. Check to see if the server's own certificate was added to the remote trusted certs list, and if so, remove it from the list.

SIPS607

Log report SIPS607, titled *TLS Connection Request Failed*, is generated to provide details into which remote server is not able to connect with the local server (SIP Gateway application running on the Session Server). This log supplements log SIPS601 and is an information log only and is not directly associated with an alarm.

Format

The format for log report SIPS607 is as follows:

```
Feb 16 09:53:44 comit.ngss.unit1 sipgwyappln: SIPS607 NONE INFO TLS
Connection Request Failed: Server: AURUM, IP Address: 47.129.118.195
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPS607	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	TLS	Title label for the log
Description	Connection Request Failed	Detailed description of the trouble or activity

Field	Value	Description
Server:	Refer to the Additional information section	Name of the remote SIP server as it is provisioned in the Session Server database. This value corresponds to the name of the remote SIP server.
IP Address	IP address of the remote server unable to connect with the Session Server	The IP address of the remote SIP server.

Action

This information log report requires no action; however, if there are an excessive number of SIPS607 logs, check for additional alarms, related SIPS601 logs and associated OMs.

Associated OM registers

Monitor incrementation the OM registers TLS_CONNECTION_REQUESTS_FAILED in Session Server OM group SIPGW_TLS. Refer to the Session Server Performance Management NTP, NN10342-711 for details and instructions for viewing registers in the SIPGW_TLS OM group.

Additional information

If the value of the server name is NULL, this log, together with the SIPS601 log, indicates that the remote SIP server is not provisioned in the Session Server database

If the value of the server name is not NULL, the SIPS607 log, together with the SIPS601 log, indicates which remote server is not able to connect with the Session Server, and the reason why the remote server is not able to connect. Verify provisioning of the security certificates on the remote SIP server and on the local Session Server.

CRTM700

Log report CRTM700, titled *New private key requested*, is generated during the execution of the Certificate Management Tool , when either option 1 (generate a self-signed certificate) or option 2 (generate a certificate signing request) is used. Using either option 1 or 2 backs up the existing private key within the /opt/base/share/ssl directory and any new private key generated is placed in file /opt/base/share/ssl/server.key. This is an information log only and is not associated with an alarm.

Format

The format for log report CRTM700 is as follows:

```
Nov 11 14:12:14 ngss.unit0 cert_mgnt: CRTM700 NONE INFO CERT_MGNT
User requested new private key.
Existing key moved to /opt/base/share/ssl/server.key.1412_11112004
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	cert_mgnt	Identifies the NGCL or application process unit that generates the report
Log Number	CRTM700	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	The type of trouble or info recorded
Label	cert_mgnt	Title label for the log
Description	User requested new private key	Detailed description of the trouble or activity

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Use the Certificate Management Tool screen output and TLS initialization logs to ensure that the new key and certificate were provisioned properly.

CRTM701

Log report CRTM701, titled, *Self signed certificate requested*, is generated during the execution of the Certificate Management Tool, option 1, (generate a self-signed certificate). Self-signed certificates carry a security risk because they are not signed by a trusted certificate authority (CA) and therefore cannot be authenticated by a certificate authority. This information log is a notification that the user accepted the disclaimer regarding the risks associated with using self-signed certificates. No alarms are associated with this log.

Format

The format for log report CRTM701 is as follows:

```
Nov 12 09:54:50 comit.ngss.unit0 cert_mgnt: CRTM701 NONE INFO CERT_MGNT
User accepted disclaimer for generating self-signed certificates
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	cert_mgnt	Identifies the NGCL or application process unit that generates the report
Log Number	CRTM701	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	The type of trouble or info recorded

Field	Value	Description
Label	CERT_MGNT	Title label for the log
Description	User accepted disclaimer for generating self-signed certificates	Detailed description of the trouble or activity

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Use the Certificate Management Tool screen output and TLS initialization logs to ensure that the new key and certificate were provisioned properly.

XTS300

Log report XTS300 indicates that system random access memory (RAM) resources are low.

The NCGL operating system generates a log report whenever a minor, major or critical XTS300 OutofMemory alarm is raised or if the existing alarm is escalated. This is a quality of service alarm indicating that memory resources are low or near exhaustion. Memory resource limitation could impact the quality of service of the Session Server or Policy Controller, leading to partial loss of service.

Format

The format for log report XTS300 is as follows:

```
APR17 07:46:06 ngss-1 XTS300 minor FLT Memory
Unit Number : 0, ACTIVE
Available memory is between 125MB and 150MB;
              minor threshold reached.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	N/A	Identifies the NGCL or application process unit that generates the report
Log Number	XTS300	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded

Field	Value	Description
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911 for a description of how to monitor the connectivity and network status for both Session Server units. Refer to *Policy Controller Fault Management,* NN10438-911 for a description of how to monitor the connectivity and network status for both Policy Controller units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS301

Log report XTS301 indicates that the CPU load average for one or more time segments has exceeded a preset threshold.

The Session Server or Policy Controller platform generates log report XTS301 in addition to the alarm.

Format

The format for log report XTS301 is as follows:

```
APR17 07:46:06 ngss-1 XTS301 minor FLT CPU Load
Unit Number : 0, ACTIVE
1 minute load average is between 10.00 and 20.
00; minor threshold reached.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	N/A	Identifies the NGCL or application process unit that generates the report
Log Number	XTS301	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (Fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of CPU and memory related resources for the active unit.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS303

Log report XTS303 indicates that at least one software process has terminated abnormally and may retain system resources such as memory space or CPU usage (zombie process).

The Session Server - Trunks or Policy Controller platform generates log report XTS303 in addition to the alarm.

Format

The format for log report XTS303 is as follows:

```
APR17 08:06:23 ngss-1 XTS303 minor FLT  Zombie Process
Unit Number : 0, ACTIVE
Number of zombie processes is between 5 and 10;
              minor threshold reached.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	N/A	Identifies the NGCL or application process unit that generates the report
Log Number	XTS303	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server - Trunks Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of zombie processes for the active unit.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS304

Log report XTS304 indicates one or more of the Network File System (NFS) mounted file systems is inaccessible. Each unit mounts a file system from the mate unit. This log report is expected during upgrades or any time the mate unit is unavailable.

The unit generates log report XTS604 when the alarm clears.

Format

The format for log report XTS304 is as follows:

```
May  6 17:25:30 ngss-1 alarmd: XTS304 MINOR FLT  NFS Mount
Not Accessible NCGL=ngss-1;Unit=0 Number of accessible
NFS mounts is equal to 0; minor threshold reached
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS304	The component prefix and number of the log
Severity	minor	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm is raised in addition to more severe alarms such as Mate is unavailable and point to point (PTP) failure. If connectivity to the mate is lost or if the mate unit is offline, then this alarm clears when communication with the mate is restored.

If the mate unit is available, clear connectivity related alarms. Connectivity to the mate over the PTP link, physically provided by the crossover cables, is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

XTS305

Log report XTS305 indicates that the platform software lost time synchronization to one or more Network Time Protocol (NTP) servers, or the drift is excessive.

The Session Server or Policy Controller platform generates log report XTS305 in addition to the alarm.

Format

The format for log report XTS305 is as follows:

```
Feb 13 10:42:05 rtpsngss1unit1 alarmd: XTS305 MAJOR FLT
NTP Error NCGL=rtpsngss1unit1;Unit=1 Host is not communicating
with any NTP server(s);
No. of configured server(s): 1; No. of accessible server(s): 0.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS305	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	NTP Error	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own; however, if the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS306

Log report XTS306 indicates that CPU utilization has exceeded a preset threshold.

The Session Server or Policy Controller platform generates log report XTS306 in addition to the alarm.

Format

The format for log report XTS306 is as follows:

```
May 25 10:13:05 yin alarmd: XTS306 MINOR FLT CPU Utilization NCGL=yin;
Unit=0 5 minute percent idle cpu utilization is below 5.00,
minor threshold reached.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS306	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of CPU and memory related resources for the active unit.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS309

Log report XTS309 indicates that a peripheral hardware component (such as an ethernet card) has a Peripheral Component Interconnect (PCI) bus fault, Error Checking and Correction (ECC) memory fault, or a parity error.

The Session Server or Policy Controller platform generates log report XTS309 in addition to the alarm.

Format

The format for log report XTS309 is as follows:

```
AUG6 08:13:22 ngss-1 XTS309 critical FLT  Hardware Fault
Unit Number : 1, INACTIVE
Data parity critical threshold is reached;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS309	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. If the alarm persists, refer to procedure *Reboot a Session Server unit* in the Session Server Security and Administration NTP, NN10346-611 or *Reboot a Policy Controller unit* in the Policy Controller Security and Administration NTP, NN10434-611, for a description how to reboot the affected unit. After the reboot, check the resulting system status in *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911.

If the alarm persists, consider replacing the unit.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS314

Log report XTS314 is generated with an alarm when application memory resources are running low. A minor alarm is generated when application memory resources are reduced to 48MB. A major alarm is generated when application memory resources are reduced to 32MB.

Format

The format for log report XTS314 is as follows:

```
OCT21 11:22:10 ngss-1 XTS314 critical FLT Application Memory Unit Number:1,
ACTIVE Major memory alarm threshold of 32MB reached
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd, logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS314	The component prefix and number of the log
Severity	Minor, Major, Critical	The log severity (may be related to alarm severity)
Event Type	Fault	The type of trouble recorded
Label	Application Memory	Title label for the log

Field	Value	Description
Unit	Unit Number 0, Unit Number 1 (active)	The Session Server unit impacted or to which the alarm applies. Also may indicate if the unit is active.
Description	Major memory alarm threshold of 32MB reached	Detailed description of the trouble. This field indicates if the major threshold of 32MB was reached or if the minor threshold of 48MB was reached.

Action

Refer to procedure View the operational status of a Session Server NCGL platform on page 49 to monitor the status of CPU and memory related resources for the active Session Server unit.

Contact Nortel Networks support personnel or your next level of support immediately.

For minor severity alarms, no new datafill should be performed to the application until the problem is understood and a plan is in place to resolve the problem. Proceeding with further datafill will further reduce the amount of memory available and the alarm will progress to a major.

For major and critical severity alarms, stop all datafill and use of system tools. Limit system activities to critical issues only. Contact Nortel Networks support personnel immediately as a future upgrade is at risk of failure.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS315

Log report XTS315 is generated when the inactive unit becomes disabled and is not available.

The Session Server or Policy Controller platform generates log report XTS315 in addition to the alarm.

Format

The format for log report XTS315 is as follows:

```
Sep 13 15:00:24 cablab.ss.unit1 alarmd: XTS315 MAJOR FLT  Simplex Node
NCGL=cablab.ss.unit1;Unit=1 The state is Standby Disabled.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS315	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of the application on both units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS316

Log report XTS316 indicates that the standby call processing application on the inactive Session Server or Policy Controller is out of service and the node is not operation in a fault-tolerant mode.

The Session Server or Policy Controller platform generates log report XTS316 in addition to the alarm.

Format

The format for log report XTS316 is as follows:

```
APR7 08:16:22 ngss-1 XTS316 major FLT Application Out-of-Serv
Unit Number : 0, ACTIVE
The application state has changed from In
Service to Out Of Service.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS316	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of the application on both units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS331

Log report XTS331 indicates that the Session Server or Policy Controller active unit cannot communicate to the mate unit through the ethernet connections.

The Session Server or Policy Controller platform generates log report XTS331 in addition to the alarm.

Format

The format for log report XTS331 is as follows:

```
Oct 25 09:53:18 cablab.ss.unit1 alarmd: XTS331 MAJOR FLT
Mate Connectivity NCGL=cablab.ss.unit1;Unit=1 Link0:
INSV, mateCon: UNAVAIL, netCon: AVAIL; Link1: INSV,
mateCon: UNAVAIL, netCon: AVAIL;  PTPLink: INSV, mateCon: UNAVAIL;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS331	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the connectivity and network status for both units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS335

Log report XTS335 is generated in response to a Communications Subsystem Failure alarm when one or both PTP links is down.

The Session Server or Policy Controller platform generates log report XTS335 in addition to the alarm.

Format

The format for log report XTS335 is as follows:

```
Jul 22 09:43:04 cablab alarmd: XTS335 MAJOR FLT Link Connectivity ss.unit1;
Unit=1 Link0:INSV, mateCon: AVAIL, netCon: AVAIL;Link1:INSV, mateCon: AVAIL,
netCon: AVAIL; PTPLink: PTP0-SYSB, mateCon: AVAIL;



Jul 22 10:32:33 cablab alarmd: XTS335 MAJOR FLT Link Connectivity ss.unit1;
Unit=1 Link0: INSV, mateCon: AVAIL, netCon: AVAIL; Link1:INSV, mateCon: AVAIL,
netCon: AVAIL; PTPLink: BOTH_SYSB, mateCon: AVAIL;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS335	The component prefix and log number
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded

Field	Value	Description
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the connectivity and network status for both units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS336

Log report XTS336 indicates that one or more ethernet links are unable to communicate with the network.

The Session Server or Policy Controller platform generates log report XTS336 in addition to the alarm.

Format

The format for log report XTS336 is as follows:

```
Sep 21 09:17:26 cablab.ss.unit1 alarmd: XTS336 MAJOR FLT Network
Connectivity NCGL=cablab.ss.unit1;Unit=1 Link0: INSV, mateCon: AVAIL,
netCon: UNAVAIL; Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink:
INSV, mateCon: AVAIL;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS336	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the connectivity and network status for both units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS351

Log report XTS351 indicates a response to several CON and APL alarms because the mate Session Server or Policy Controller unit is unavailable or status information for the mate unit is unavailable at the maintenance interface.

The Session Server or Policy Controller platform generates log report XTS351 in addition to the alarm.

Format

The format for log report XTS351 is as follows:

```
Sep 21 09:27:14 cablab.ss.unit0 alarmd: XTS351 MAJOR FLT No Mate
Communication (simplex) NCGL=cablab.ss.unit0;Unit=0 Mate unit is
unavailable.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS351	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the connectivity status for the active and standby units.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS355

Log report XTS355 indicates the inactive unit is jammed to prevent a Switch of Activity (SwAct).

The Session Server or Policy Controller platform generates log report XTS355 in addition to the alarm.

Format

The format for log report XTS355 is as follows:

```
Sep 20 12:46:23 cablab.ss.unit0 alarmd: XTS355 MINOR FLT  Jam Inactive Unit
NCGL=cablab.ss.unit0;Unit=0 Inactive JAMMED
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS355	The component prefix and number of the log
Severity	minor	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This alarm may clear on its own. Refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of CPU and memory related resources for the active unit.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS391

Log report XTS391 indicates that a disk drive:

- has failed (major) or has been removed from the system chassis (critical)
- has been removed from the NCGL for maintenance or upgrade but is still installed in the chassis (major)
- is having its filesystem rebuilt and its performance is degraded (minor)

The Session Server or Policy Controller platform generates log report XTS391 in addition to the alarm. When the alarm condition is cleared, a log XTS691 is generated.

Format

The format for log report XTS391 is as follows:

```
Sep 20 15:37:47 cablab.ss.unit1 alarmd: XTS391 MAJOR UNEQ Disk Missing
NCGL=cablab.ss.unit1;Unit=1; Array:
'/dev/md1
' (ntvg) Status: A physical
disk has been removed from the array.

Sep 20 15:38:22 cablab.ss.unit1 alarmd: XTS391 MINOR INIT Array Rebuilding
NCGL=cablab.ss.unit1;Unit=1; Array:
'/dev/md0
' (/boot) Status: The array
is currently being rebuilt.

Sep 20 15:38:22 cablab.ss.unit1 alarmd: XTS391 MINOR INIT Array Rebuilding
NCGL=cablab.ss.unit1;Unit=1; Array:
'/dev/md1
' (ntvg) Status: The array is
currently being rebuilt.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	Alphanumeric	Identifies the NGCL or application process unit that generates the report
Log Number	XTS391	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

Determine the cause of the alarm and refer to *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911, for a description how to monitor the status of Disk Storage resources for the affected unit.

Replace the failed disk drive. Refer to the procedure in *Session Server Fault Management*, NN10332-911, or *Policy Controller Fault Management,* NN10438-911.

If the alarm persists at the major or critical level, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS392

Log report XTS392 indicates a error result has been returned from regularly occurring NGCL audit testing for any of the following conditions:

- Magneto Hardware Chassis Fault (equipment malfunction or failure)
- Self Test Unavailable (NCGL malfunction or process failure)
- Self Test Hardware Error (equipment malfunction or failure)
- Self Test Query Error (equipment malfunction or failure)
- Self Test Corrupted Error (equipment malfunction or failure)
- Self Test Device Failure (equipment malfunction or failure)

The severity level of the alarm is determined by the conditions listed above.

The Session Server or Policy Controller platform generates log report XTS392 in addition to the alarm. When the alarm condition is cleared, a log XTS692 is generated.

Format

The format for log report XTS392 is as follows:

```
May 19 10:31:33 loopback alarmd: XTS392 MAJOR FLT  Self Test
NCGL=localhost; Unable to communicate with BMC to get results. cc=0

May 19 11:40:44 unit0 alarmd: XTS392 MAJOR FLT  Self Test NCGL=unit0;
Unable to communicate with BMC to get results. cc=0

May 19 12:36:27 yin alarmd: XTS392 MAJOR FAIL Chassis Fault NCGL=yin;Unit=0;
Power overload detected.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log

Field	Value	Description
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS392	The component prefix and number of the log
Severity	minor, major	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This log report requires no action. If the alarm persists, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS395

Log report XTS395 indicates a error result has been returned from regularly occurring NCGL file system audit tests:

- Self Test Device Filesystem Threshold Exceeded; this is a quality of service alarm indicating that memory resources are low
- Filesystem Test Failure (minor) due to low disk space
- Filesystem Test Failure (critical) due to test failure

The Session Server or Policy Controller platform generates log report XTS395 in addition to the alarm. When the alarm condition is cleared, a log XTS695 is generated.

Format

The format for log report XTS395 is as follows:

```
May  4 13:02:58 fred alarmd: XTS395 MINOR FLT
Filesystem Error NCGL=fred;Unit=0 Status: Alarm raised.
Filesystem is < /boot >. Test results: Stat(Success) CreateDir(Success)
CreateFile(Success) WriteFile(No space left on device) ReadFile(Success)
RemoveFile(Success) RemoveDir(Success)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS395	The component prefix and number of the log
Severity	minor, major, critical	The log severity (may be related to alarm severity)
Event Type	FLT (fault)	The type of trouble or info recorded

Field	Value	Description
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity

Action

This log report requires no action. If the alarm persists, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS600

Log report XTS600 is written by the NCGL operating system when the conditions which raised alarm XTS300 have been cleared.

Format

The format for log report XTS600 is as follows:

```
Apr 7 14:11:45 sp2k-1 logman: XTS600 NONE INFO Memory Alarm Cleared
Unit Number : 0, UNDETERMINED
Description : Available memory is greater than the minor threshold
value of 150MB
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS600	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Memory Alarm Cleared	Title label for the log
Description	Refer to originating XTS300 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS601

Log report XTS601 is written by the NCGL operating system when the conditions which raised alarm XTS301 have been cleared.

Format

The format for log report XTS601 is as follows:

```
Apr 7 14:11:45 sp2k-1 logman: XTS601 NONE INFO CPU Alarm
Cleared Unit Number : 0, UNDETERMINED
Description : 1 minute load average is less than 10.00; no threshold reached
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS601	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	CPU Alarm	Title label for the log
Description	Refer to originating XTS301 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS602

Log report XTS602 is written by the NCGL operating system when the conditions which raised alarm XTS302 have been cleared.

Format

The format for log report XTS602 is as follows:

```
Apr 29 14:11:39 yang logman: XTS602 NONE INFO Disk Alarm Cleared
Unit Number : 1, ACTIVE
Description : Percentage of root free disk space is greater than 15.00.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS602	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Memory Alarm Cleared	Title label for the log
Description	Refer to originating XTS302 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS603

Log report XTS603 is written by the NCGL operating system when the conditions which raised alarm XTS303 have been cleared.

Format

The format for log report XTS603 is as follows:

```
Apr 7 14:11:46 sp2k-1 logman: XTS603 NONE INFO Zombie Process Alarm Cleared
Unit Number : 0, UNDETERMINED
Description : Number of zombie processes is less than 5.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS603	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Memory Alarm Cleared	Title label for the log
Description	Refer to originating XTS303 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS604

Log report XTS604 is written by the NCGL operating system when the conditions which raised alarm XTS304 have been cleared.

Format

The format for log report XTS604 is as follows:

```
May  6 18:50:22 ngss-1 logman: XTS604 NONE INFO NFS Mounts Accessible
Unit Number : 0, ACTIVE         Description : Number of accessible
NFS mounts is greater than 0.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS604	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	NFS Mounts Accessible	Title label for the log
Description	Refer to originating XTS304 alarm for details	Detailed description of the trouble or activity

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS605

Log report XTS605 is written by the NCGL operating system when the conditions which raised alarm XTS305 have been cleared.

Format

The format for log report XTS605 is as follows:

```
Sep 13 15:04:20 cablab.ss.unit1 alarmd: XTS605 NONE INFO NTP
Error NCGL=cablab.ss.unit1;Unit=1 Host is not communicating with any NTP
server(s); No. of configured server(s): 3; No. of accessible server(s): 0.

Sep 13 15:04:40 cablab.ss.unit1 alarmd: XTS605 NONE INFO NTP
Error NCGL=cablab.ss.unit1;Unit=1 Host is not synchronized to any NTP
server(s); No. of configured server(s): 3; No. of accessible server(s): 3.

Sep 13 15:07:50 cablab.ss.unit1 alarmd: XTS605 NONE INFO NTP
Error NCGL=cablab.ss.unit1;Unit=1 Host lost synchronization to one or more
NTP servers; No. of configured server(s): 3; No. of accessible server(s):
3; Host synchronized to: 2 server(s).

Sep 13 15:20:22 cablab.ss.unit1 alarmd: XTS605 NONE INFO NTP
Error NCGL=cablab.ss.unit1;Unit=1 Time offset is greater than the defined
threshold; Offset from NTP server 10.65.96.13: 61ms; Threshold: (+/-)50ms.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS605	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded

Field	Value	Description
Label	NTP Alarm Cleared or NTP Error	Title label for the log
Description	Refer to originating XTS305 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS606

Log report XTS606 is written by the NCGL operating system when the conditions which raised alarm XTS306 have been cleared.

Format

The format for log report XTS606 is as follows:

```
Apr 29 14:11:39 yang logman: XTS606 NONE INFO CPU Utilization Cleared
Unit Number : 1, ACTIVE
Description : 5 minute percent idle cpu utilization is above 5.00,
no threshold reached.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS606	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	CPU Utilization Cleared	Title label for the log
Description	Refer to originating XTS306 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS609

Log report XTS609 is written by the NCGL operating system when the conditions which raised alarm XTS309 have been cleared.

Format

The format for log report XTS609 is as follows:

```
Nov 4 11:00:58 OTT2.SS0 logman: XTS609 NONE INFO
Hardware Fault Cleared Unit Number : 0, ACTIVE Description :
HWMON Fault Inserted through debug tool
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS609	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Hardware Fault Cleared	Title label for the log
Description	Refer to originating XTS309 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS614

Log report XTS614 is generated when all the conditions which raised alarm XTS314 are cleared.

Format

The format for log report XTS614 is as follows:

```
Apr 29 10:16:51 ngss-1 logman: XTS614 NONE INFO
Application Memory Alarm Cleared Unit Number : 1
UNDETERMINED Description : Memory alarm cleared on application manager
initialization
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd, logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS614	The component prefix and number of the log
Severity	NONE	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble recorded
Label	Application Memory Alarm Cleared	Title label for the log

Field	Value	Description
Unit	Unit Number 0, Unit Number 1 (active)	The unit impacted or to which the alarm applies. Also may indicate if the unit is active.
Description	Memory alarm cleared on application manager initialization	Detailed description of the trouble or resolution.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS615

Log report XTS615 is written by the NCGL operating system when the conditions which raised alarm XTS315 have been cleared.

> ***Note:*** When a SwAct occurs, the SIP Gateway application database loses synchronization. An alarm and SIPM302 log are generated, indicating loss of synchronization. After the SwAct has completed, the SIP Gateway application database returns to a synchronized state, and a follow-up SIPM-302 log is generated, indicating that the alarm has cleared.

Format

The format for log report XTS615 is as follows:

```
Apr 7 09:17:04 sp2k-1 alarmd: XTS615 NONE INFO Duplex Node NCGL=sp2k-1;
Unit=0 State has changed from Standby Disabled to Standby Enabled.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS615	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Duplex Node	Title label for the log
Description	Refer to the originating XTS315 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS616

Log report XTS616 is written by the NCGL operating system when the conditions which raised alarm XTS316 have been cleared.

Format

The format for log report XTS616 is as follows:

```
Apr 7 09:37:32 sp2k-1 logman: XTS616 NONE INFO Application In-Service
Unit Number : 0, UNDETERMINED
Description : The state is Running.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS616	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Application In-service	Title label for the log
Description	Refer to originating XTS316 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

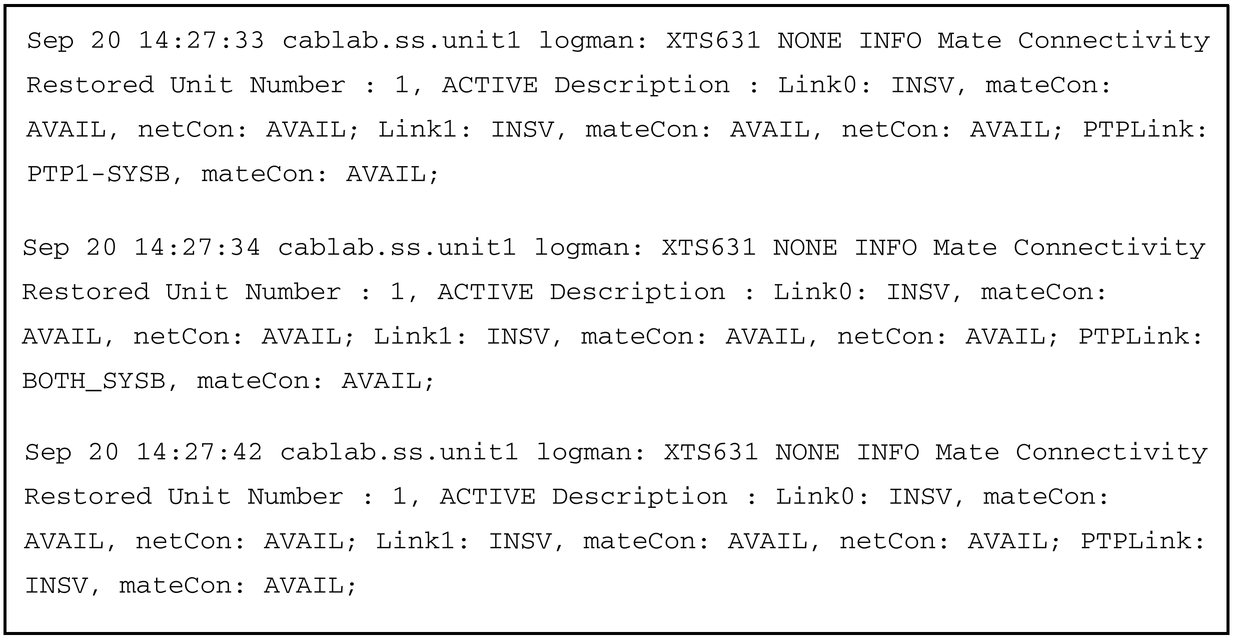
Refer to the originating alarm/log for description details.

XTS631

Log report XTS631 is written by the NCGL operating system when the conditions which raised alarm XTS331 have been cleared.

Format

The format for log report XTS631 is as follows:



```
Sep 20 14:27:33 cablab.ss.unit1 logman: XTS631 NONE INFO Mate Connectivity
Restored Unit Number : 1, ACTIVE Description : Link0: INSV, mateCon:
AVAIL, netCon: AVAIL; Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink:
PTP1-SYSB, mateCon: AVAIL;

Sep 20 14:27:34 cablab.ss.unit1 logman: XTS631 NONE INFO Mate Connectivity
Restored Unit Number : 1, ACTIVE Description : Link0: INSV, mateCon:
AVAIL, netCon: AVAIL; Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink:
BOTH_SYSB, mateCon: AVAIL;

Sep 20 14:27:42 cablab.ss.unit1 logman: XTS631 NONE INFO Mate Connectivity
Restored Unit Number : 1, ACTIVE Description : Link0: INSV, mateCon:
AVAIL, netCon: AVAIL; Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink:
INSV, mateCon: AVAIL;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS631	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)

Field	Value	Description
Event Type	Info	The type of trouble or info recorded
Label	Mate Connectivity Restored	Title label for the log
Description	Refer to originating XTS331 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS635

Log report XTS635 is written by the NCGL operating system when the conditions which raised alarm XTS335 have been cleared.

Format

The format for log report XTS635 is as follows:

```
 Apr 29 10:21:53 yang alarmd: XTS635 NONE INFO Link Connectivity Restored
NCGL=yang;Unit=1 Link0: INSV, mateCon: AVAIL, netCon: AVAIL;
Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink: INSV, mateCon: AVAIL
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman; alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS635	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Link Connectivity Restored	Title label for the log
Description	Refer to originating XTS335 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS636

Log report XTS636 is written by the NCGL operating system when the conditions which raised alarm XTS336 have been cleared.

Format

The format for log report XTS636 is as follows:

```
May 11 09:52:00 cablab alarmd: XTS636 NONE INFO Network Connectivity
Restored NCGL=cablab.ss.unit1;Unit=1 Link0: INSV, mateCon: AVAIL, netCon:
AVAIL;Link1: INSV, mateCon: AVAIL, netCon: AVAIL;  PTPLink: INSV, mateCon:
AVAIL
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS636	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Network Connectivity Restored	Title label for the log
Description	Refer to originating XTS336 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS651

Log report XTS651 is written by the NCGL operating system when the conditions which raised alarm XTS351 have been cleared.

Format

The format for log report XTS651 is as follows:

```
Sep 21 09:31:02 cablab.ss.unit0 alarmd: XTS651 NONE INFO Mate
Communication Restored NCGL=cablab.ss.unit0;Unit=0 Mate unit is available.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman; alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS651	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Mate Communication Restored	Title label for the log
Description	Refer to originating XTS351 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS655

Log report XTS655 is written by the NCGL operating system when the conditions which raised alarm XTS355 have been cleared.

Format

The format for log report XTS655 is as follows:

```
Apr 29 14:11:38 yang logman: XTS655 NONE INFO Release Jam on Inactive unit
Unit Number : 1, UNDETERMINED
Description : Inactive not JAMMED
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS655	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Release Jam on Inactive unit	Title label for the log
Description	Refer to originating XTS355 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS670

Log report XTS670 is written by the NCGL operating system when a SwAct of the system has been initiated.

Format

The format for log report XTS670 is as follows:

```
Apr 8 09:19:33 sp2k-1 logman: XTS670 NONE INFO SWACT Failover Started
Unit Number : 0, ACTIVE
Description : SWACT failover has been initiated. Initiator: Manual
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS670	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	SWACT Failover Started	Title label for the log
Description	SWACT failover has been initiated. Initiator: Manual	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS671

Log report XTS671 is written by the NCGL operating system when a SwAct of the system has been completed.

Format

The format for log report XTS671 is as follows:

```
Apr 8 09:19:33 sp2k-1 logman: XTS671 NONE INFO SWACT Failover Finished
Unit Number : 0, INACTIVE
Description : Result: Passed, Initiator: Manual
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS671	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	SWACT Failover Finished	Title label for the log
Description	Result: Passed, Initiator: Manual	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

XTS691

Log report XTS691 is written by the NCGL operating system when the conditions which raised alarm XTS391 have been cleared.

Format

The format for log report XTS691 is as follows:

```
Apr 29 10:55:48 yang alarmd: XTS691 NONE INIT Array Rebuilt
NCGL=yang;Unit=1; Array: '/dev/md1' (ntvg) The array has been rebuilt.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS691	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Array Rebuilt	Title label for the log
Description	Refer to originating XTS391 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS692

Log report XTS692 is written by the NCGL operating system when the conditions which raised alarm XTS392 have been cleared.

Format

The format for log report XTS692 is as follows:

```
Apr 29 10:55:48 yang alarmd: XTS692 NONE INIT Self Test Device Clear

Apr 29 12:36:39 yin alarmd: XTS692 NONE FAIL Chassis OK NCGL=yin;Unit=0;
Power overload detected.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	XTS692	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Self Test Device Clear	Title label for the log
Description	Refer to originating XTS392 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.

XTS695

Log report XTS695 is written by the NCGL operating system when the conditions which raised alarm XTS395 have been cleared.

Format

The format for log report XTS695 is as follows:

```
May 11 09:56:39 yin alarmd: XTS695 NONE THR Threshold exceeded
or Filesystem Error
NCGL=yin;Unit=0; Status: Alarm cleared.
Filesystem is < /tmp >. Used filesystem percentage is 0.50.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Time and Date Stamp	Alphanumeric	The time and date the log was generated
Hostname or Host ID	Alphanumeric	The hostname or host id of the unit that generated the log
Process Name	logman	Identifies the NGCL or application process unit that generates the report
Log Number	XTS695	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	Info	The type of trouble or info recorded
Label	Memory Alarm Cleared	Title label for the log
Description	Refer to originating XTS395 alarm for details	Detailed description of the trouble or activity.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Refer to the originating alarm/log for description details.