



Carrier Voice over IP Fault Management Logs Reference Volume 3

ATTENTION

The Carrier Voice over IP Fault Management Logs Reference document uses seven volumes to describe logs that Carrier VoIP Portfolio components can generate. Not all components apply to every solution.

A log report is a message about an important conditions or events related to Carrier VoIP portfolio component(s) performance. Log reports include, but are not restricted to, the following information:

- state and activity reports
- changes in state
- hardware or software errors
- test results
- other events or conditions that affect performance

Note: Both system actions and manual overrides can generate log reports.

New in this release

The following changes were made for this release:

- CPUM 300, 399 (new)
- EMJS351 (new)
- IEMS616 (new)
- NAM300 (new)
- NCAS325 (new); added NCAS501, NCAS502, NCAS601 (modified)
- PKM300 to 306 (new)
- SIPS310 (new)
- XTS382, 383, 638, 676 to 679, 682, 683 (new)
- regrouped QUA logs into QoS Collector Application group
- moved all NODEXXX, SDMXXX, SDMBXXX and SPMXXX logs to Volume 2
- M3UA101 to M3UA108 (new)
- USM300, 301, 303, 305, 600, 601, 602, 603, 604, 605 (new)
- SIPC350, 361, 370, 371, 372, 550, 625 plus 10 variants of STGW700, and STGW800 (new)

Log formats

The log formats shown in this volume display in either NT or SCC2 standard formats. Not every format that generates from the core appears in a log report. Consult the latest software load that accompanies your product for a complete list of log formats.

In this volume

Volume 3 contains the following Carrier VoIP logs by component:

- [Border Control Point](#)
- [Integrated Element Manager Server](#)
- [Media Server 2000](#)
- [Policy Controller](#)
- [QoS Collector Application group](#)
- [Session Server](#)
- [Universal Signaling Point](#)

The tables in this volume identifies and briefly describes the logs they use. Double-click on the log identifier to see the log details.

Border Control Point

The following table lists the individual logs that the Border Control Point generates.

Border Control Point logs (Sheet 1 of 3)

Log ID	Description
RTP101	Indicates that difficulties are encountered when attempting initial communication to setup the Media Blade specified by Blade Name (\$1)
RTP102	Indicates when an OutOfServiceAlarm is raised.
RTP103	Indicates when a timer-driven event checks the percentage of the configured media ports that are in use and then determines that the current usage level exceeds a configured threshold.
RTP104	Indicates when a timer-driven event detects a failed status on one of the available host network interfaces.
RTP105	Indicates a lost connection with the Last Border Control Point
RTP106	Indicates when communication problems (for example, network difficulties) are encountered when attempting to communicate with the Media Blade specified by Blade Name (\$1)
RTP107	Indicates when link issues (for example, carrier sense fails) are encountered when attempting to communicate over a problem interface (specified by Interface Name \$2) on the identified Media Blade (specified by Blade Name \$1)
RTP108	Indicates when a Session Manager does not receive responses to requests made to the only available Border Control Point in its media resource pool
RTP109	Indicates when a Session Manager does not receive responses to requests made to an available Border Control Point in its media resource pool
RTP110	Indicates a recovery of the Border Control Point Host application upon discovery of pre-existing media sessions on a Media Blade

Border Control Point logs (Sheet 2 of 3)

Log ID	Description
RTP111	Indicates that the Host was able to re-establish communication with a subtending Media Blade. This log also reports the number of connections over which the Host was able to restore control
RTP112	Indicates the start of the Border Control Point Host application recovery process
RTP113	Indicates the number of connections recovered on a specific Media Blade
RTP114	Indicates the number of Media Blades with which the Host failed to establish communications
RTP118	Indicates when an attempt to dispatch an outgoing signal fails
RTP200	Indicates when the Border Control Point initializes in a state in which no Media Blade information has been configured
RTP201	Indicates when a request for reboot of the Border Control Point fails due to a software exception
RTP202	Indicates when a request for service is made from an unknown proxy - one which is not configured for this Border Control Point
RTP203	Indicates an attempt to send a registration message to one of the configured proxies fails
RTP204	Indicates that an audit is performed over the Connection Map and a particular connection is not found on the corresponding Media Blade
RTP205	Indicates that an audit is performed over the Connection Map and a particular connection is unexpectedly found to be idle on the corresponding Media Blade
RTP206	Indicates when an audit is performed over the Connection Map and a particular connection is found on the corresponding Media Blade which exceeds the Long Idle Duration threshold

Border Control Point logs (Sheet 3 of 3)

Log ID	Description
RTP207	Indicates when an audit is performed over the Connection Map and a particular connection is found on the corresponding Media Blade which exceeds the Long Call Duration threshold
RTP208	Indicates a failed attempt to access the interface status file (establish a file handle, read from it, or it does not exist)
RTP300	Indicates when it is necessary for the Border Control Point to autonomously increase in the size of the Hash Map used to store connection information
RTP301	Indicates a denied request for an increase in the size of the Hash Map
RTP302	Indicates a request for an increase in the size of the Hash Map fails due to some unforeseen software issue
RTP801	Indicates when there is a change made to configuration data for an in-service Border Control Point
RTP802	Indicates that the Border Control Point is not correctly configured

Integrated Element Manager Server

The following table is a list of the possible device types that may be reflected in the Component ID field of some IEMS logs. The IEMS logs are listed in the table [IEMS logs](#).

Device types for IEMS logs

Device or platform name	NE Type
Network elements	
CICM	CICM-Node
ERS 8600	NE-ERS_8600
MAS	NE-MAS

Device types for IEMS logs

Device or platform name	NE Type
MG 3200	NE-MG_3200
MS 2000	NE-MS2000
Session Server	NE-SS, NE-SS-UNIT
STORM	NE-STORM
USP	NE-USP
Element Managers	
APS Mgr	EMS-APS-Mgr
CEM Mgr	EMS-CEM-Mgr
CICM Mgr	EMS-CICM-Mgr, CICM-Mgr-Node
CS2K Core Mgr	EMS-CS2K-Mgr, CS2000-CORE, CALL-AGENT-CORE
FPM	FPM-UNIT
GWC	GWC, CMT
IEMS Mgr	EMS-IEMS
MCS Mgr (Managing NE type - MCS/CSE MX)	EMS-CSE-Mgr, CSE-UNIT
MCS Mgr (Managing NE type - Media portal)	MP-UNIT
MDM	EMS-MDM-Mgr
MG9K Mgr	EMS-MG9K-Mgr
SAM21 Mgr	EMS-SAM21-Mgr
UAS Mgr	EMS-UAS-Mgr
UNEM Mgr	EMS-UNEM-Mgr, UMUX-1500, UMUX-1200, UMUX-900

Device types for IEMS logs

Device or platform name	NE Type
SSLines Mgr	EMS-SSLines-Mgr, SSLines-Unit
Platforms	
SPFS	PLAT-SSPFS
MDM	PLAT-MDM
Applications	
NPM	APPLN-NPM
QoS Collector	APPLN-QOS
SBRM	APPLN-SBRM
Certificate Manager	APPLN-PKMGR

The following table lists the individual logs that the Integrated Element Manager Server (IEMS) generates.

IEMS logs (Sheet 1 of 7)

Log ID	Description
BKM300	Indicates when a system backup fails
BKM600	Indicates when a system backup completes successfully
CSEM300	Indicates alarm sets and alarm clears for IEMS logs
CSEM600	Indicates INFO and unmapped logs for these logs
EMSS304	Indicates that the pam_mkhomedir module has timed out
EMSS315	Indicates the PAM login servlet health monitor detects the PAM login servlet is not functional
EMSS316	Indicates the pam_mkhomedir module cannot use the script that is owned by the user

IEMS logs (Sheet 2 of 7)

Log ID	Description
EMSS317	Indicates the pam_mkhomedir module cannot get the script
EMSS318	Indicates the pam_mkhomedir module cannot continue since the euid is not root
EMSS319	Indicates the pam_is_authentication module cannot get the configuration file
EMSS325	Indicates the pam_is_authentication module cannot get the auth url
EMSS326	Indicates the pam_is_authentication module is blocked and timed out
EMSS327	Indicates the script (default is mkhomedir) cannot access the directory or files
EMSS330	Indicates that the PAM proxy did not initialize the single signon facility and SSO tokens will not be generated
EMSS331	Indicates that the PAM proxy can not authenticate the user due to an unhandled internal error
EMSS351	Indicates an exception that is raised while making a request to the servlet
EMJS340	Indicates the state of communication between the Integrated EMS server and the device
EMJS341	Indicates that an SNMP data collection job fail
EMJS350	Indicates the state of the FTP connection with the device
EMJS351	Generated by IEMS to inform the OSS that the user configured in the indicated Job Instance does not have the privileges required to rename an OM file on the specified device
EMJS360	Indicates the state of a report file
EMJS371	Indicates that no file is available to transfer
EMJS540	Indicates the status of a job

IEMS logs (Sheet 3 of 7)

Log ID	Description
EMJS560	Indicates that the state of the Report Job
EMJS570	Indicates that the transfer job has resumed
EMJS640	Indicates that an SNMP OID mismatch has occurred
EMJS641	Indicates the successful completion of an SNMP data collection job
EMJS642	Indicates the partial completion of an SNMP data collection job
EMJS651	Indicates the successful completion of the CSV data collection job
EMJS652	Indicates the state of the CSV data collection job
EMJS661	Indicates the successful completion of a report job
EMJS662	Indicates the state of a report job
EMJS671	Indicates the completion of a transfer job
EMJS672	Indicates the failure of a transfer job
EMJS840	Indicates that an alarm threshold has reached the maximum value
EMJS841	Indicates that the alarm threshold has returned to normal
EMSS300	Indicates that the client-side Pam + Radius SPI is unable to communicate with the server-side Radius interface
EMSS301	Indicates that there are problems with the server-side Radius proxy
EMSS302	Indicates that the IS PAM+ Plug-in fails to communicate with the Integrated EMS SPI
EMSS305	Indicates that the Identity Server (IS_ PAM+ Plug-in fails to communicate with the Integrated EMS SPI

IEMS logs (Sheet 4 of 7)

Log ID	Description
EMSS306	Indicates that a packet from the Radius server is corrupted
EMSS307	Indicates that a packet from the Radius server has failed verification
EMSS308	Indicates that the client-side PAM+ Radius SPI is unable to communicate with the Radius Identity Server
EMSS309	Indicates that a packet from the Radius server does not contain all required fields
EMSS310	Indicates that the client configuration file cannot be opened
EMSS311	Indicates that the PAM+ Radius SPI is unable to communicate with the Radius Identity Server
EMSS312	Indicates that the client-side PAM+ Radius SPI is unable to update file systems
EMSS313	Indicates that the client-side PAM+ Radius SPI receives a <code>accountExpiredException</code> from the Radius server, regardless of the debug level set in the <code>/etc/pam.conf</code> file
EMSS314	Indicates the identity server health monitor detects the server process is not functional
EMSS320	Indicates there is a failure to initialize the single sign on (SSO) facility. SSO tokens will not be generated
EMSS321	Indicates there is a failure to authenticate the user due to an unhandled internal error
EMSS322	Indicates that no single-sign-on token is available after authentication
EMSS323	Indicates that no single-use tokens are generated due to an unhandled internal error
EMSS324	Indicates that the UNIX user's profile cannot be read due to an unhandled internal error

IEMS logs (Sheet 5 of 7)

Log ID	Description
EMSS330	Indicates that the PAM proxy did not initialize the single signon facility and SSO tokens will not be generated
EMSS331	Indicates that the PAM proxy can not authenticate the user due to an unhandled internal error
EMSS351	Indicates an exception that is raised while making a request to the servlet
EMSS 600	Indicates that the PAM Radius daemon modifies the /etc/passwd or /etc/group files
EMSS 601	Indicates that there are successful or failed authentication requests of the authentication module
EMSS 602	Indicates successful or failed PAM SPI events from PAM + Plug-Ins
EMSS 603	Indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token create event
EMSS 604	Indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token destroy event
EMSS 605	Indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token timeout event
IEMS398	Indicates Integrated EMS is unable to communicate with a managed device
IEMS399	Indicates that Integrated EMS regained communication with a managed device
IEMS601	Generated when the IEMS receives an event from a device that is not configured in the IEMS inventory
IEMS602	Generated when the IEMS receives an event from a device in the IEMS inventory but the event type is not recognized
IEMS603	Indicates missed notifications

IEMS logs (Sheet 6 of 7)

Log ID	Description
IEMS604	Generated when IEMS receives a clear event without a corresponding raise event
IEMS606	Indicates that the event count has exceeded the configured threshold limit or that the deletion of events is complete
IEMS607	Indicates there is a discrepancy in the active alarm list between Integrated EMS and the managed component
IEMS614	Generated when IEMS receives an OSI state change SNMP notification trap from an IEMS component
IEMS615	Generated when it receives an orphaned clear, which is a clear event from a device when there is no corresponding raise event
IEMS616	Generated when an SNMP protocol authentication failure occurs. It is an INFO event
PKM300	Generated when an attempt to create and validate an X509 certificate has failed or when X509 certificate creation and validation succeeds after previously having failed
PKM301	Generated when an attempt to deliver an X509 certificate to an application has failed or when delivery of an X509 certificate succeeds after previously having failed
PKM302	Generated when an X509 certificate used by a device to authenticate itself during call control operations has expired
PKM303	Generated when the expiration date of an X509 certificate has reached the forewarning date for the last alarm before expiration
PKM304	Generated when the expiration date of an X509 certificate has reached the date for the initial expiration warning

IEMS logs (Sheet 7 of 7)

Log ID	Description
PKM305	Generated when an X509 certificate used by a device to authenticate itself for OAM&P functions has expired
PKM306	Generated to provide advance warning that a WEBPKPROXY certificate has been delivered and needs to be installed
TMN301	Generated when an application error is detected
TMN302	Generated when a system error occurs.
TMN303	Generated when a communication error occurs
TMN304	Generated when a connection error occurs
TMN309	Generated when a data server error occurs
TMN311	Generated when a fatal error occurs
TMN600	Generated by Log Normalizer when the normalizer process is successfully started and when delrep messages are sent successfully to the SDM OSF server
TMN601	Generated if the version summary file is not found, meaning that the archive is empty.
TMN604	Generated to provide information about application status
TMN605	Generated to provide Core restart information

MCS 5200

The following table lists the individual logs that the MCS 5200 generates.

MCS 5200 logs (Sheet 1 of 9)

Log ID	Description
AC 102	Indicates that the Trunk Framing settings on the connected PSTN switch do not match those provisioned on the Audiocodes Mediant 2000
AC 105	Indicates that the port on the gateway is unable to tell the trunk is in-service
AC 107	Indicates there is a physical problem in the connectivity of the trunk to the gateway
AC 128	Indicates that the gateway is no longer responding to SNMP polling
DBCM 101	Indicates that a network element has lost communication with the database
DBMN 101	Indicates that the System Manager cannot communicate with the SNMP agent that provides the database monitoring raw data
DBMN 102	Indicates an inability of the database SNMP agent to process the requests sent by the System Manager
DBMN 103	Indicates that the operational state of the database server process is a value other than "UP"
DBMN 401	Indicates that the amount disk space used by the database is approaching its limit
DBMN 425	Indicates that the amount of disk space available for an Oracle table space is approaching its limit
DBMN 727	Indicates that the database replication system encountered an error that prevents it from keeping the primary and secondary databases in sync
DBMN 728	Indicates that the persistence job that keeps the primary and secondary databases in sync is no longer running

MCS 5200 logs (Sheet 2 of 9)

Log ID	Description
DBMN 826	Indicates that the replication queue between the primary and secondary database instances is not being serviced
EPMTC 401	Indicates the configured percentage of unreachable static clients has been reached
FTP 703	Indicates that the FTP operation of OAM records to the OSS destination failed due to the error encountered in creating directory on the base directory configured
FTP 704	Indicates that the FTP operation of OAM Record to the OSS destination failed with an error message
FTP 706	Indicates that the FTP operation of OAM records failed because of failure of login for the userid and password configured
IMDB 700	Indicates that an internal cache in the network element (NE) has failed to load its data from the database during system initialization
IMDB 701	Indicates that an internal cache in the network element (NE) has failed to synchronize its data with the database during regular system operation
IMDB 702	Indicates that an internal table of the network element (NE) that is kept in memory has reached or is nearing its capacity
KCRE 201	Indicates that a license key code resource owner is unable to update the resource management tables with its new key code limit from a newly applied license key
LKEY 470	Indicates the license key limit for a resource has reached or exceeded thresholds licensable limits
LKEY 750	Indicates the System Manager is not able to retrieve the license key from the database
LKEY 751	Indicates that the license key file could not be decrypted

MCS 5200 logs (Sheet 3 of 9)

Log ID	Description
LKEY 752	Indicates an error occurred during validation of the license key
LKEY 753	Indicates an error occurred during validation of the license key file
LKEY 754	Indicates an error occurred validating the license key file against the target system hardware
LKEY 755	Indicates that the license key upgrade failed because the supplied license key was intended for a system with a newer software release
LOADS 801	Indicates a new load becomes available in the loads directory (/var/mcp/loads)
MAS 102	Indicates the MAS Provisioning Manager is unable to communicate with the database
MAS 103	Indicates the MAS Provisioning Manager is unable to communicate with one of the Media Application Server(s) configured in the system
MAS 504	Indicates the number of pending transactions in the database exceeds 100,000
MAS 701	Indicates an error was encountered during the initialization of the MAS Provisioning Manager
MAS 705	Indicates more than two Media Application Servers have been found for a given pooled entity configured in the system
NCAS 101	Indicates the NCAS link to the CS2K Core has been disconnected
NECM 101	Indicates the System Manager is unable to communicate with an online network element (NE) instance
NECM 102	Indicates that the Fault/Performance Manager (FPM) that is configured to manage network element (NE) has no running instance

MCS 5200 logs (Sheet 4 of 9)

Log ID	Description
NED 101	Indicates the local communication between a managed network element instance (NEI) and the network element daemon (NED) on the NEI's server is lost
NIF 100	Indicates a network element instance configured with a floating IP address is unable to send a gratuitous ARP to associate the IP address with a logical interface
NIF 200	Indicates a network element instance in a fault tolerant configuration is, during activation, unable to "up" a logical interface associated with the configured floating IP Address
NIF 201	Indicates a failure in a network interface card, preventing any packets from being sent on it.
OLC 401	Indicates the calls will be failing as the component has gone in overload mode
OLC 402	Indicates the database has gone into overload mode
OLC 403	Indicates the memory is exhausted
R6AS0	Indicates the R6AS servertime configuration item of a Session Manager is modified
RESM 701	Indicates the resource management partition audit raised an alarm when the resource management partition table usage values differ from the actual usage values returned from the resource owner
RESM 702	Indicates the resource management partition audit raised an alarm when the resource management partition table usage percentage are above the alarm thresholds
RTA 101	Indicates that the status of the standard recording stream is down
RTA 201	Indicates that there is an exception occurred when recording a data record into the spool directory of the network element instance

MCS 5200 logs (Sheet 5 of 9)

Log ID	Description
RTP 101	Indicates difficulties (e.g. network communication problems, software issues) are being encountered when attempting initial communication to setup the Media Blade specified by Blade Name (\$1)
RTP 102	Indicates an OutOfServiceAlarm
RTP 103	Indicates a timer-driven event checks the percentage of the configured media ports that are in use and then determines that the current usage level exceeds a configured threshold
RTP 104	Indicates a timer-driven event detected a failed status on one of the available host network interfaces
RTP 106	Indicates a communications problem (e.g. network difficulties) was encountered when attempting to communicate with the Media Blade specified by Blade Name (\$1)
RTP 107	Indicates link issues (e.g. carrier sense fails) were encountered when attempting to communicate over a problem interface (specified by Interface Name \$2) on the identified Media Blade (specified by Blade Name \$1)
RTP 108	Indicates a Session Manager does not receive responses to requests made to the only available Border Control Point in its media resource pool
RTP 109	Indicates a Session Manager does not receive responses to requests made to an available Border Control Point in its media resource pool
RTP 801	Indicates there is a change made to configuration data for an in-service Border Control Point
RTP 802	Indicates this Border Control Point is not configured correctly
RTP 804	Indicates difficulties were encountered when attempting to initialize/configure an Border Control Point

MCS 5200 logs (Sheet 6 of 9)

Log ID	Description
RTP 805	Indicates that the corresponding service node is hosting the Standby Service Instance (ready to become active in the event of a failure)
RTP 806	Indicates that the Border Control Point Cluster is in an invalid cluster configuration
RTP 815	Indicates a change to “Border Control Point Cluster” data using a Live Update of Border Control Point Cluster Configuration Parameters Data is NOT supported
RTP 816	Indicates a change to “Border Control Point Cluster” data using a Live Update of Border Control Point Cluster Fault Tolerance Data is NOT supported
RTP 817	Indicates a change to “Border Control Point Cluster” data using a Live Update of Border Control Point Cluster Gateway Controllers Data is NOT supported
RTP 818	Indicates a change to “Border Control Point Cluster” data using a Live Update of Border Control Point Cluster Session Managers Data is NOT supported
RTP 819	Indicates a change to “Border Control Point Cluster” data using a Live Update of Border Control Point Cluster Static Routes Data is NOT supported
RTP 820	Indicates a change to “Border Control Point Cluster” data using a Live Update of Border Control Point Cluster Service Instances Data is NOT supported
SEC 820	Indicates a certificate in the internal keystore will expire in 89 days or less
SEC 821	Indicates a certificate in the internal truststore will expire in 89 days or less
SIP 401	Indicates a SIP protocol alarm for call failures

MCS 5200 logs (Sheet 7 of 9)

Log ID	Description
<u>SMCM 101</u>	Indicates an online network element (NE) instance cannot communicate with the System Manager
<u>SRVR 101</u>	Indicates the SNMP agent on the server cannot be contacted
<u>SRVR 102</u>	Indicates the Server Monitor encountered unexpected error responses to the SNMP queries
<u>SRVR 401</u>	Indicates the CPU Occupancy of the monitored Server equals or exceeds the configured threshold
<u>SRVR 401</u>	Indicates the CPU Occupancy of the monitored Server equals or exceeds the configured threshold
<u>SRVR 402</u>	Indicates the RAM Utilization of the monitored Server equals or exceeds the configured threshold
<u>SRVR 403</u>	Indicates the disk space utilization for a partition on the monitored Server equals or exceeds the configured threshold
<u>SRVR 404</u>	Indicates the interface utilization for a physical interface on the monitored Server equals or exceeds the configured threshold
<u>SVCA 801</u>	Indicates the service address of System Manager was changed from the Management Console
<u>SYNC 200</u>	Indicates that the configuration data for an NE Instance is out-of-sync
<u>SYS 101</u>	Raises an alarm in the MCP Management Console alarm browser
<u>SYS 102</u>	Indicates a fault tolerant Status message was received by a network element instance when no peer is provisioned for that instance
<u>SYS 103</u>	Indicates a fault tolerant Status message was received by a network element instance when from a peer whose IP address is different from that of the provisioned peer

MCS 5200 logs (Sheet 8 of 9)

Log ID	Description
SYS 104	Indicates a network element is in a fault tolerant configuration and a peer instance informs an instance that it believes it to be failed
SYS 105	Indicates a network element instance is isolated from the network
SYS 106	Indicates an unusual condition where a peer network element instance believes it is network isolated but is still able to communicate the isolation condition to the local instance
SYS 703	Indicates a network element instance in a fault tolerant configuration when a peer instance is in the ACTIVATING phase but fails to transition to ACTIVE within the time specified by the engineering parameter "FaultTolerance:PeerActivityTransitionTimeout"
SYS 704	Indicates a network element instance in a fault tolerant configuration when a peer instance is in the DEACTIVATING phase but fails to transition to SHUTDOWN within the time specified by the engineering parameter "FaultTolerance:PeerActivityTransitionTimeout"
SYS 707	Indicates a fault tolerant network element instance requested synchronization from it's peer but was rejected
TCF 902	Indicates a failure to create all requested TCP servers or UDP based sockets for a particular subsystem
TCF 903	Indicates a failure to create a TCP server or UDP based socket
THLD 401	Indicates a generic threshold alarm provided by the OM framework
THLD 402	Indicates a generic threshold alarm provided by the OM framework

MCS 5200 logs (Sheet 9 of 9)

Log ID	Description
TSVR 700	Indicates the failure by the session manager to connect to the terminal server provisioned in the voicemail server configuration page on the provisioning client
TSVR 701	Indicates that the session manager failed to connect to the terminal server on the specified address and port

Media Server 2000

The following table lists the individual logs that the Media Server 2000 generates.

Media Server 2000 logs (Sheet 1 of 2)

Log ID	Description
AMS300	Indicates a board reset on the Media Server 2000 node
AMS301	Indicates a fatal error the Media Server 2000 node
AMS302	Indicates a configuration error on the Media Server 2000 node
AMS303	Indicates a temperature alarm
AMS304	Indicates a feature key error on the Media Server 2000 node
AMS305	Indicates board call resource alarm on the Media Server 2000 node
AMS306	Indicates a board controller failure alarm on the Media Server 2000 node
AMS307	Indicates an ethernet link alarm on the Media Server 2000 node
AMS308	Indicates a board overload on the Media Server 2000 node
AMS309	Indicates an active alarm table overflow on the Media Server 2000 node

Media Server 2000 logs (Sheet 2 of 2)

Log ID	Description
AMS310	Indicates an ATM port alarm on the Media Server 2000 node
AMS311	Indicates an audio provisioning alarm on the Media Server 2000 node
AMS312	Indicates an operational state change on the Media Server 2000 node to “disabled”
AMS314	Indicates the NAT placed in front of a device has been identified as a symmetric NAT.
AMS500	Indicates a board started condition on the Media Server 2000 node
AMS501	Indicates an admin state change on the Media Server 2000 node
AMS600	Contains status of board hardware elements being tested.
AMS800	Indicates crossing of performance monitoring threshold.

Policy Controller

The following table lists the individual logs that the Policy Controller generates.

Policy Controller (Sheet 1 of 3)

Log ID	Description
SPCM300	Generated by the Policy Controller application maintenance process for a variety of informational purposes
SPCM301	Generated when the Policy Controller application, running on an enabled Policy Controller unit, is not in-service
SPCM302	Generated when the Policy Controller application state goes out of sync between two Policy Controller units

Policy Controller (Sheet 2 of 3)

Log ID	Description
SPCM500	Generated when the current state of the SIP application maintenance process changes from its last known state
SPCP301	Indicates that the Policy Controller application server signaling interface has a communication failure
SPCP302	Indicates that the Policy Controller has lost database connection
SPCP303	Indicates that the Application server request failure ratio exceeds the predefined threshold value
SPCP304	Indicates that the Policy Controller Endpoint Number exceeds the Endpoint Block Size
SPCP305	Indicates that the Policy Controller Endpoint Number exceeds the Endpoint Block Warning Size
SPCP501	Indicates that the Policy Controller application has started up
SPCP502	Indicates that the Policy Controller application has shut down
SPCP601	Indicates that a Flow Status Audit has completed
SPCP602	Indicates that a CAC request from the application server has been denied
SPCP603	Indicates that a the Policy Controller callp has accepted a topology change
SPCP604	Indicates that callP has detected that the Ingress Id of the Network Segment sent in a GateSet message from the GWC is not present in the Policy Controller database
TPM301	Indicates that the Topology Manager has lost database connection
TPM501	Indicates that the Topology Manager application has started up

Policy Controller (Sheet 3 of 3)

Log ID	Description
TPM502	Indicates that the Topology Manager application has shut down
TPM601	Indicates that the Topology Manager application has accepted a topology change

QoS Collector Application group

The following table lists the individual logs that the QoS Collector Application group generates.

QoS Collection Application logs

Log ID	Description
QCA201	Indicates Qca.properties not available at QCA start-up, or other problems related to properties/qca.properties
QCA202	Indicates old file retention directory (today-x) is being removed, OR file found in active directory when QCA started
QCA203	Indicates QCA cannot be stopped due to several possible reasons
QCA300	Indicates file handler or server socket could not be started
QCA301	Indicates QoS record received with unsupported length or unsupported version
QCA302	Indicates out of sequence QoS record received, OR problem processing binary QoS record
QCA305	Indicates connection to client is closed OR the binary QoS Record header could not be processed
QCA310	Indicates the log reports minor, major or critical disk space issues
QCA315	Generated for file writing or file access problems
QCA322	Indicates new GWC connection received

Session Server

The following table lists the individual logs that the Session Server generates.

Session Server logs (Sheet 1 of 9)

Log ID	Description
CPUM300	Generated when the CPU occupancy level of the Session Server unit reaches a minor, major, or critical level
CPUM399	Generated when a CPUM300 alarm is cleared
CRTM700	Generated when either option 1 (self-signed certificate) or option 2 (certificate signing request) is used during the execution of the Certificate Management Tool
CRTM701	Generated when option 1 (self-signed certificate) is used during the execution of the Certificate Management Tool
DBSE300	Generated any time a change in database connectivity is detected
NCAS325	Generated when alarm NCAS325 is raised because the non-call associated signaling (NCAS) link has gone down
NCAS501	Generated by the SIP Gateway application when an out-of-band REFER request is received but does not validate and the request can not be accepted
NCAS502	Generated by the Session Server Trunks application when it cannot communicate to the splite process
NCAS601	Generated by the SIP Gateway application when a non-call associated signaling (NCAS) link is configured at the CS 2000 Session Server Manager
NMSS115	Generated by the SIP Gateway application when an error occurs while sending NMS TCAP messages to SCTP

Session Server logs (Sheet 2 of 9)

Log ID	Description
NMSS116	Generated by the SIP Gateway application when an error occurs while receiving NMS TCAP messages from SCTP
NMSS117	Generated by the SIP Gateway application when an error occurs while sending REJ messages over SCTP
NMSS118	Generated by the SIP Gateway application when an error occurs while receiving REJ over messages from SCTP
SIPC301	Generated when the SIP Gateway Call Processing Application will not receive any incoming SIP messages
SIPC310	Indicates overload condition status among other things.
SIPC350	Generated by SIP gateway application when a serious software error such as segment violation occurs
SIPC361	Indicates that a duplicate IP address was detected
SIPC370	Indicates the statistics of the audit messaging
SIPC371	Indicates that the Call Processing audit has convicted because of a timeout of the SIP INFO message since the last audit cycle
SIPC372	Indicates that the Call Processing audit has convicted because of the GCP audit since the last audit cycle
SIPC550	Generated when a Critical alarm is generated to a loss of connectivity between the database and the CallP application
SIPC625	Generated when a remote IP address does not respond to heartbeat messages
SIPC650	Generated when the SIP Gateway Call Processing Application goes to get data from the database for a particular table and no data is found

Session Server logs (Sheet 3 of 9)

Log ID	Description
SIPC750	Generated when the SIP Gateway Call Processing Application drops incoming SIP messages due to Access Control List restrictions
SIPM300	Generated by the SIP Gateway application maintenance process for a variety of unexpected reasons or conditions
SIPM301	Generated when the SIPM301 critical alarm is raised
SIPM302	Generated when SIP Gateway application state goes out of sync between the two Session Server units
SIPM500	Generated with a SIP Maintenance State Change
SIPS300	Generated during the alarming of dropped connection requests.
SIPS301	Generated by authentication failure events
SIPS302	Generated as a result of regular alarm process checks to ensure the local server certificate continues to be valid
SIPS305	Generated during the initialization (unlock) of the SIP Gateway application
SIPS310	Generated during the initialization (unlock) of the SIP Gateway application
SIPS600	Generated during the connection setup of SIP Gateway application call processes
SIPS601	Generated from TLS authentication failure events
SIPS604	Generated during initialization (unlock) of the SIP Gateway application, indicating when the current local certificate will expire
SIPS605	Generated during initialization (unlock) of the SIP Gateway application, indicating that TLS Security is enabled

Session Server logs (Sheet 4 of 9)

Log ID	Description
<u>SIPS606</u>	Generated when there is a problem importing the trusted certificate provisioned into the database
<u>SIPS607</u>	Indicates which remote server is not able to connect with the local server (SIP Gateway application running on the Session Server)
<u>STGW700</u>	Generated when callp activity is interrupted or negatively impacted
<u>STGW700 (INFO AUDIT - 481 Received)</u>	Generated when the SST call audit receives a 481 Unknown Call response for a SIP INFO audit message
<u>STGW700 (INFO AUDIT - No Response)</u>	Generated when a response is not received for a SIP INFO audit message sent to a SIP endpoint
<u>STGW700 (SIP AUDIT - Double Pass Failure)</u>	Generated when the SST call audit fails to audit a SIP endpoint twice on successive audit cycle
<u>STGW700 (GCP AUDIT - Abnormal Condition--Missing Profile Data)</u>	Indicates that the SST call audit detected missing profile data for the call being audited
<u>STGW700 (GCP AUDIT - Abnormal Condition--Missing Server Data)</u>	Indicates that the SST call audit detected missing remote SIP server data for the call being audited
<u>STGW700 (GCP AUDIT - Double Pass Failure)</u>	Sends audit requests to the DPT GWC to ensure that active calls on the SST are still active on the associated DPT GWC
<u>STGW700 (GCP AUDIT - Force Release)</u>	Generated when a force release is performed to clear a SST call

Session Server logs (Sheet 5 of 9)

Log ID	Description
STGW700 (GCPListener Socket RecvFrom Failed)	Indicates that a UDP socket read error occurred in the GCPListener task
STGW700 (SLGTGN digits not stripped)	Generated when an incoming INVITE contains only prefix digits
STGW700 (WaitThread poll failed)	Indicates that the SST call processing subsystem experienced a failure when trying to poll a UDP socket
STGW800	Indicates that communications to a DPT GWC has been established (Inactive to Active) or that communications to a DPT GWC has been lost (Active to Inactive)
USM300	Generated when swchecker fails to process and add a parcel file to the SST patching system
USM301	Generated for some patch application failures
USM303	Generated for some patch removal failures
USM305	Generated when a miscellaneous error occurs in the SST patching system
USM600	Generated when a parcel file is successfully processed by swchecker and added to the NGSS patching system
USM601	Generated for successful patch application
USM602	Generated during a patch application if it is necessary to restart an SST application process
USM603	Generated for successful patch removal
USM604	Generated during a patch removal if it is necessary to restart an NGSS application process
USM605	Generated when the ngssdeletepatch command successfully removes a patch from the SST patching system

Session Server logs (Sheet 6 of 9)

Log ID	Description
XTS300	Indicates that memory resources are low or near exhaustion
XTS301	Indicates that the CPU load average for one or more time segments has exceeded a preset threshold
XTS302	Indicates that free space on the root file system is low
XTS303	Indicates that at least one software process has terminated abnormally and may retain system resources such as memory space or CPU usage
XTS304	Indicates one or more of the Network File System (NFS) mounted file systems is inaccessible
XTS305	Indicates that the platform software lost time synchronization to one or more Network Time Protocol (NTP) servers, or the drift, is excessive
XTS306	Indicates that CPU utilization has exceeded a preset threshold
XTS309	Indicates that a peripheral hardware component has a PCI bus fault, Error Checking and Correction (ECC) memory fault, or a parity error
XTS314	Generated when application memory resources are running low
XTS315	Indicates that the standby call processing application on the inactive Session Server is not ready for takeover
XTS316	Indicates that the standby call processing application is out of service and the Session Server node is not operational
XTS331	Indicates that the Session Server active unit cannot communicate to the mate unit through the ethernet connections
XTS335	Indicates that one of PTP ethernet interfaces is down

Session Server logs (Sheet 7 of 9)

Log ID	Description
XTS336	Indicates that one or more ethernet links are unable to communicate with the network
XTS351	Indicates a response to several CON and APL alarms
XTS355	Indicates the inactive unit is jammed to prevent a Switch of Activity (SwAct)
XTS382	Indicates that one or more sensors on the server chassis is reporting an alarm condition)
XTS383	Indicates that a power supply module is reporting an alarm condition
XTS391	Indicates that a disk drive has certain major or minor alarms
XTS392	Indicates a error result has been returned from regularly occurring NGCL audit testing for any of a number of conditions
XTS395	Indicates a error result has been returned from regularly occurring NCGL file system audit tests
XTS600	Generated by the NCGL operating system when all the conditions which raised alarm XTS300 have been cleared
XTS601	Generated by the NCGL operating system when all the conditions which raised alarm XTS301 have been cleared
XTS602	Generated by the NCGL operating system when all the conditions which raised alarm XTS302 have been cleared
XTS603	Generated by the NCGL operating system when all the conditions which raised alarm XTS303 have been cleared
XTS604	Generated by the NCGL operating system when all the conditions which raised alarm XTS304 have been cleared

Session Server logs (Sheet 8 of 9)

Log ID	Description
XTS605	Generated by the NCGL operating system when all the conditions which raised alarm XTS305 have been cleared
XTS606	Generated by the NCGL operating system when all the conditions which raised alarm XTS306 have been cleared
XTS609	Generated by the NCGL operating system when all the conditions which raised alarm XTS309 have been cleared
XTS614	generated when all the conditions which raised alarm XTX314 are cleared
XTS615	Generated by the NCGL operating system when all the conditions which raised alarm XTS315 have been cleared
XTS616	Generated by the NCGL operating system when all the conditions which raised alarm XTS316 have been cleared
XTS631	Generated by the NCGL operating system when all the conditions which raised alarm XTS331 have been cleared
XTS635	Generated by the NCGL operating system when all the conditions which raised alarm XTS335 have been cleared
XTS636	Generated by the NCGL operating system when all the conditions which raised alarm XTS336 have been cleared
XTS638	Generated when the switch link operation is executed on the LAN links of one unit in a mated pair Session Server Trunks platform
XTS651	Generated by the NCGL operating system when all the conditions which raised alarm XTS351 have been cleared
XTS655	Generated by the NCGL operating system when all the conditions which raised alarm XTS355 have been cleared

Session Server logs (Sheet 9 of 9)

Log ID	Description
XTS670	Generated by the NCGL operating system when a SwAct of the system has been initiated
XTS671	Generated by the NCGL operating system when a SwAct of the system has been completed
XTS676	Generated when a reboot is initiated on a simplex Session Server Trunks platform
XTS677	Generated when a mate reboot is initiated on the standby unit in a mated pair Session Server Trunks platform
XTS678	Generated when the Halt command is executed on a simplex Session Server Trunks platform
XTS679	Generated when the halt mate command is executed on the Session Server Trunks platform. The halt mate command stops operation of the standby unit
XTS682	Written by the NGCL operating system when a sensor alarm for the server chassis is cleared
XTS683	Written by the NGCL operating system when a sensor alarm for a power supply module is cleared
XTS691	Generated by the NCGL operating system when all the conditions which raised alarm XTS391 have been cleared
XTS692	Generated by the NCGL operating system when all the conditions which raised alarm XTS392 have been cleared
XTS695	Generated by the NCGL operating system when all the conditions which raised alarm XTS395 have been cleared

Universal Signaling Point

The following table lists the individual logs that the Universal Signaling Point (USP) generates.

Note: For more information about USP logs, refer to the *Log and Operational Measurement Descriptions for Universal Signaling Point*

(USP), version 3.0.3. These logs also appear on the Graphical User Interface (GUI).

USP logs

Log ID	Description
M3UA101	Indicates M3UA path status changes
M3UA102	Indicates M3UA pathset status changes.
M3UA103	Indicates M3UA protocol violation events
M3UA104	Indicates invalid sctp association establish request
M3UA105	Indicates error message received
M3UA106	Indicates a GWC node as an M3UA signaling link state change to USP
M3UA107	Indicates traffic is discarded because routeset is unavailable
M3UA108	Indicates unexpected message received
USP398	Indicates an SNMP timeout in a USP device
USP399	Clears all other USP logs

Supplementary logs

The following documents reference logs and/or alarms that do not appear in this volume:

Note: The terms Passport, PVG and MDM have been re-branded in conjunction with the new Nortel Networks' brand simplified naming format. Passport is now referred to as the Nortel Networks Multiservice Switch, PVG is now the Nortel Networks Media Gateway 7480/15000, and MDM is now the Nortel Networks Multiservice Data Manager.

- For XA-CORE logs, refer to the *XA-Core Reference Manual*, 297-8991-810.
- For information about Multiservice Switch alarms associated with your component, refer to *Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference*, NN10600-500 and *Nortel Networks Multiservice Switch 15000, Media Gateway 15000 and*

*Preside MDM in Succession Networks Fault Management Overview
PT-AAL1/UA-AAL1/UA-IP, NN10092-911.*

For information about Passport 8600 logs and traps, refer to the following documents:

- *Preside Passport 8600 Device Integration Cartridge User Guide, 241-6003-110.*
- *Configuring Network Management- Passport 8000 Series Software Release 3.5, 314723-B.*
- *System Messaging Platform Reference Guide- Passport 8000 Series Software Release 3.5, 315015-B.*

BKM300

The Synchronized Backup Manager (BKM) generates log report BKM300 when a system backup fails.

Format

The log report format for BKM300 is as follows:

```
Aug 23 21:00:01 BKM300 NONE INFO System Backup Failure
System backup failed. Reason: SESM not running.
```

Selected field descriptions

Descriptions for each field in the log report appear in the following table:

Field	Value	Description
Reason	Variable	Indicates the reason system backup failed

Action

Correct the problem in the system based on the failure reason. When the problem is corrected, re-attempt backup.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

BKM600

The Synchronized Backup Manager (BKM) generates log report BKM600 when a system backup completes successfully.

Format

The log report format for BKM600 is as follows:

```
Aug 23 21:00:01 BKM600 NONE INFO System Backup  
Complete  
System backup <yymmdd_hhmmss> completed successfully.
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS340

Log report EMJS340 indicates the state of communication between the IEMS server and the device.

The IEMS generates log report EMJS340.

Format

The format for log report EMJS340 is as follows:

```
MSH10 * EMJS340 FEB25 11:45:19 7033 TBL IEMS OM Collec-
tion Job Alarm
Location: 10.102.15.138
Job Instance: CollectionJob4
State: Raise
Category: processingError
Cause: underlyingResourceUnavailable
ComponentId:EMS-IEMS=10.102.15.138;Soft-
ware=CollectionJob4;
Time: Feb 25 11:45:19 2005
Description: Request Timed out to the device
0.0.0.0-PP8600
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
State	Raise, Clear	Indicates the state of the log.
ComponentId	character string	Indicates the details of the component.

Action

If the alarm condition persists, validate the state of the associated device. In addition, validate the associated configuration attributes in the IEMS and the associated device.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS341

Log report EMJS341 indicates that an SNMP data collection job fails.

The IEMS generates log report EMJS341.

Format

The format for log report EMJS341 is as follows:

```
MSH10 * EMJS341 FEB25 11:45:20 7034 TBL IEMS OM Collection Job Status
Location: 10.102.15.138
Job instance: CollectionJob4
State: Raise
Category: other
Cause: communicationsSubsystemFailure
ComponentID: EMS-IEMS=10.102.15.138,Software=CollectionJob4;
Time: Feb 25 11:45:20 2005
Description: Collection job CollectionJob4 unable to collect any
attributes. Refer to the perf_log.txt debug log on the IEMS
server
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	character string	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
Time	character string	Indicates the date and time of the log.
ComponentId	character string	Indicates the details of the component.

Action

If the alarm condition persists, analyze the perf_log.txt debug log on the IEMS server.

Associated OM registers

This log report is associated with the following OMs:

- numOf60MinFailedCollectionJobs
- numOf24HrFailedCollectionJobs
- numOf12HrFailedCollectionJobs
- numOf5MinFailedCollectionJobs
- numOf15MinFailedCollectionJobs
- numOf30MinFailedCollectionJobs

Additional information

This log report requires no additional information.

EMJS350

IEMS generates log report EMJS350 when the IEMS encounters problems with an sftp/ftp session to a managed device, which is used to collect its associated OM data files.

Format

The raise and clear formats for log report EMJS350 are as follows:

```
<OFFICE>    * EMJS350 MMMDD hh:mm:ss ##### TBL  IEMS OM Processing Job Alarm
Location: <IEMS DisplayName>;<IEMS IP address>
Job Instance: <Job Name>
State: <Raise|Clear>
Category: processingError
Cause: underlyingResourceUnavailable
ComponentID: IEMS=<IEMS DisplayName>;Software=<Job Name>;<device
type>=<device DisplayName>
Time: Mmm DD hh:mm:ss YYYY
Description: <string that will be wrapped to the next line if >80
chars>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IEMS Display Name IP address	Indicates the IEMS display name in the IEMS GUI, followed by the IP address of the IEMS server. If the IEMS virtual IP is present in the device, then the IEMS display name will be the IP address. Otherwise, the IEMS display name will be the DNS name or host name. Example: Location: 47.135.154.36;47.135.154.36
Job Instance	character string	Indicates the job name provisioned by the user. Example: msh10mdm collection
State	character string	Indicates if the alarm is raised or cleared.
Category	character string	Indicates the X.733-based category of the alarm. In this example, processingError.
Cause	character string	Indicates the cause of the alarm. In this example, underlyingResourceUnavailable.

Field	Value	Description
ComponentId	character string	Indicates the IEMS display name (see the Location field description for details); the job name (see the Job Instance description for details); the type of device the job is for and that device's provisioned display name.
Time	character string	Indicates the date/time of the alarm raise. Example: Jan 31 12:05:01 2006
Description	character string	Indicates that the file renaming privileges are not present or have been obtained. Raise example: Not able to rename file after collection, Insufficient user privileges <IP address> Clear example: File renaming privileges obtained <IP address>

Action

If the alarm condition persists, validate the state of the associated device. In addition, validate the associated configuration attributes in the IEMS and the associated device.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS351

EMJS351 is generated by IEMS to inform the OSS that the user configured in the indicated Job Instance does not have the privileges required to rename an OM file on the specified device.

Format

The raise and clear formats for log report EMJS351 are as follows:

```
<OFFICE>    * EMJS351 MMMDD hh:mm:ss ##### TBL IEMS OM Processing Job Alarm
Location: <IEMS DisplayName>;<IEMS IP address>
Job Instance: <Job Name>
State: <Raise|Clear>
Category: processingError
Cause: underlyingResourceUnavailable
ComponentID: IEMS=<IEMS DisplayName>;Software=<Job Name>;<device
type>=<device DisplayName>
Time: Mmm DD hh:mm:ss YYYY
Description: <string that will be wrapped to the next line if >80
chars>
```

Selected field descriptions

The following table explains selected fields in the log report.

Field	Value	Description
Location	IEMS Display Name IP address	Indicates the IEMS display name in the IEMS GUI, followed by the IP address of the IEMS server. If the IEMS virtual IP is present in the device, then the IEMS display name will be the IP address. Otherwise, the IEMS display name will be the DNS name or host name. Example: Location: 47.135.154.36;47.135.154.36
Job Instance	character string	Indicates the job name provisioned by the user. Example: msh10mdm collection
State	character string	Indicates if the alarm is raised or cleared.
Category	character string	Indicates the X.733-based category of the alarm. In this example, processingError.

Field	Value	Description
Cause	character string	Indicates the cause of the alarm. In this example, underlyingResourceUnavailable.
ComponentId	character string	Indicates the IEMS display name (see the Location field description for details); the job name (see the Job Instance description for details); the type of device the job is for and that device's provisioned display name.
Time	character string	Indicates the date/time of the alarm raise. Example: Jan 31 12:05:01 2006
Description	character string	Indicates that a performance data collection connection has been lost or cannot be established to a device. Raise examples: Not able to establish the <FTPISTFTP> connection with the device <IP address> 5-min connection lost with the IP: <IP address> Port:1646 Clear examples: Successfully established the <FTPISTFTP> connection with the device <IP address> Successfully established the FTP connection with the device USP-1336

Action

None.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS360

Log report EMJS360 indicates the IEMS has encountered a problem creating the CSV or XML output data file on the IEMS server.

The IEMS generates log report EMJS360.

Format

The formats for log report EMJS360 are as follows:

Example 1

The following example is for a raised alarm.

```
znc0s0jh      * EMJS360 MAY04 01:18:25 0060 TBL OM Report Job Alarm
Location: 47.142.94.66
Job instance: Test_sspfs_report
State: Raise
Category: processingError
Cause: fileError
ComponentId: EMS-IEMS=47.142.94.66;Software=Test_sspfs_report;
SSPFS=znc0s0jh-SSPFS-Unit-0
Time: May 04 01:18:25 2005
Description: Error occurred while generating file.
File Name: SSPFS.47.142.94.68-SSPFS.OMs.Test_sspfs_report.
2005.05.04_01.18.25_EST.xml
```

Example 2

The following example is for a cleared alarm.

```
znc0s0jh      EMJS360 MAY04 01:30:13 0080 TBL OM Report Job Alarm
Location: 47.142.94.66
Job instance: Test_sspfs_report
State: Clear
Category: processingError
Cause: fileError
ComponentId: EMS-IEMS=47.142.94.66;Software=Test_sspfs_report;
SSPFS=znc0s0jh-SSPFS-Unit-0
Time: May 04 01:30:13 2005
Description: Report file generation success.
File Name: SSPFS.47.142.94.68-SSPFS.OMs.Test_sspfs_report.
2005.05.04_01.30.13_EST.xml.gz
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
State	Raise, Clear	Indicates the state of the job report.
ComponentId	character string	Indicates the details of the component.
Time	character string	Indicates the date and time of the log.
FileName	character string	Indicates the file name that causes the error when the report file is generated.
Description	character string	Indicates the state of the report file generation.

Action

This log report implies that the IEMS OM collection subsystem is unable to successfully create the associated CSV or XML report file on the IEMS server. For detailed error information, monitor the perf_log.txt debug log on the IEMS server.

Associated OM registers

This log report has the associated OM: numOfFailedReportJobs.

Additional information

This log report requires no additional information.

EMJS371

Log report EMJS371 is generated when the IEMS attempts to transfer the associated IEMS CSV or XML output file to a remote system but is unable to login to the remote system.

The IEMS generates log report EMJS371.

Format

The format for log report EMJS371 is as follows:

```
MSH10 * EMJS371 FEB25 13:59:59 1430 TBL IEMS OM Processing Job Alarm
Location: 10.102.15.138
Job instance: TransferJob7
State: Raise
Category: communications
Cause: transmitFailure
ComponentID: EMS-IEMS=10.102.15.138,Software=TransferJob7;
Time: Feb 25 13:59:59 2005
Description: Login incorrect.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
ComponentId	character string	Indicates the details of the component.
Time	character string	Indicates the date and time of the log.
File name	character string	Indicates the filename.
Destination	IP address	Indicates the IP address of the destination.

Action

Verify the associated IEMS transfer job is configured with a valid userid and password.

Associated OM registers

This log report has the following associated OMs:

- numOf12HrFailedTransferJobs
- numOf24HrFailedTransferJobs
- numOf5MinFailedTransferJobs
- numOf60MinFailedTransferJobs
- numOf30MinFailedTransferJobs
- numOf15MinFailedTransferJobs

Additional information

This log report requires no additional information.

EMJS540

Log report EMJS540 is generated when the state of an IEMS collection job has been changed.

The IEMS generates log report EMJS540.

Format

The format for log report EMJS540 is as follows:

```
MSH10    EMJS540 FEB25 14:41:59 1681 <OFFL/RTS> OM Collection Job
Status
Location: 10.102.15.138
Job Instance: CollectionJob12
State: <Resumed/Enabled/Disabled/Suspended>
Category: other
ComponentID: EMS-IEMS=10.102.15.138, Software=CollectionJob12
Time: Feb 25 14:41:59 2005
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
State	Resumed, Enabled, Disabled, Suspended	Indicates the state of the job.
ComponentId	character string	Indicates the details of the component.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS560

Log report EMJS560 indicates the state of an IEMS report job has been changed.

The IEMS generates log report EMJS560.

Format

The format for log report EMJS560 is as follows:

```
MSH10  EMJS560 FEB25 14:43:15 1690 <OFFL/RTS> OM Report Job Status
Location: 10.102.15.138
Job Instance: ReportJob13
State: <Suspended/Resumed/Disabled/Enabled>
Category: other
ComponentID: EMS-IEMS=10.102.15.138,Software=ReportJob13
Time: Feb 25 14:43:15 2005
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Job Instance	character string	Indicates the job name.
State	Suspended, Resumed, Disabled, Enabled	Indicates the state of the job.
Component Id	character string	Indicates the IP address and job name of the device.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS570

Log report EMJS570 indicates the state of an IEMS transfer job has been changed.

The IEMS generates log report EMJS570.

Format

The format for log report EMJS570 is as follows:

```
MSH10  EMJS570 FEB25 14:43:15 1690 <OFFL/RTS> OM Transfer Job Status
Location: 10.102.15.138
Job Instance: ReportJob13
State: <Suspended/Resumed/Disabled/Enabled>
Category: other
ComponentID: EMS-IEMS=10.102.15.138,Software=ReportJob13
Time: Feb 25 14:43:15 2005
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
State	Suspended, Resumed, Disabled, Enabled	Indicates the state of the job.
Component Id	character string	Indicates the details of the component.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS640

Log report EMJS640 is generated by the IEMS OM collection sub-system when errors are detected when parsing the collected CSV input file or attempting to collect data from an SNMP device. When parsing a collected CSV file, the event description will indicate the associated line number in the file that cannot be parsed. When attempting to collect data from an SNMP-based device, the event description will list the OIDs that could not be collected.

Format

The format for log report EMJS640 is as follows:

```
MSH10    EMJS640 FEB25 14:00:18 1432 INFO IEMS OM Collection Job Status
Location: 10.102.15.138
Job instance: CollectionJob4
State: Info
Category: processingError
Cause: datasetProblem
ComponentID:EMS-IEMS=10.102.15.138;Software+CollectionJob4;
Invalid OID List: .1.3.6.1.4.2272.1.100.9.11.1.5, .1.3.6.1.4.1.
2272.1.100.9.11.1.4
Time: Feb 25 14:00:18 2005
Description: SNMP OID data collection failure for
192.168.2.57-PP8600
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
ComponentId	character string	Indicates the details of the component.
Time	character string	Indicates the date and time of the log.

Action

For detailed error information, monitor the perf_log.txt debug log on the IEMS server.

Associated OM registers

This log report has the following associated OMs:

- numOf15MinParitalSuccessfulJobs
- numOf12HrParitalSuccessfulJobs
- numOf24HrParitalSuccessfulJobs
- numOf30MinParitalSuccessfulJobs
- numOf5MinParitalSuccessfulJobs
- numOf60MinParitalSuccessfulJobs

Additional information

This log report requires no additional information.

EMJS641

Log report EMJS641 indicates the successful completion of an SNMP data collection job.

The IEMS generates log report EMJS641.

Format

The format for log report EMJS641 is as follows:

```
MSH10      EMJS641 FEB25 14:10:36 1482 INFO IEMS OM Collection Job
Status
Location: 10.102.15.138
Job Instance: CollectionJob4
State: Successful
Category: other
ComponentID: EMS-IEMS=10.102.15.138,Software=CollectionJob4;
Time: Feb 25 14:10:36 2005
Description: Processing successfully done for the MOs:
[10.102.15.130-PP8600, 10.102.15.131-PP8600,
192.168.2.54-PP8600, 192.168.2.57-PP8600]
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
ComponentId	character string	Indicates the details of the component.

Action

This log report requires no action.

Associated OM registers

This log report has the following associated OMs:

- numOf24HrSuccessfulJobs
- numOf60MinSuccessfulJobs
- numOf12HrSuccessfulJobs
- numOf30MinSuccessfulJobs
- numOf5MinSuccessfulJobs
- numOf15MinSuccessfulJobs

Additional information

This log report requires no additional information.

EMJS642

Log report EMJS642 is generated when the IEMS is unable to collect the OM data for all the devices configured in an IEMS collection job.

The IEMS generates log report EMJS642.

Format

The format for log report EMJS642 is as follows:

```
MSH10    EMJS642 FEB25 18:55:27 3711 INFO IEMS OM Collection Job Status
Location: 10.102.15.138
Job instance: CollectionJob11
State: Incomplete
Category: other
ComponentID: EMS-IEMS=10.102.15.138,Software=CollectionJob11;
Time: Feb 25 18:55:27 2005
Description: Collection job CollectionJob11 unable to collect
all attributes. Refer to the perf_log.txt debug log file on the
IEMS server
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
ComponentId	character string	Indicates the details of the component.

Action

For detailed error information, monitor the perf_log.txt debug log file on the IEMS server.

Associated OM registers

This log report has the following associated OMs:

- numOf15MinPartialSuccessfulJobs
- numOf12HrPartialSuccessfulJobs
- numOf24HrPartialSuccessfulJobs

- numOf30MinPartialSuccessfulJobs
- numOf5MinPartialSuccessfulJobs
- numOf60MinPartialSuccessfulJobs

Additional information

This log report requires no additional information.

EMJS651

Log report EMJS651 indicates the successful completion of the CSV data collection job.

The IEMS generates log report EMJS651.

Format

The format for log report EMJS651 is as follows:

```
MSH10    EMJS651 FEB25 14:26:13 1587 INFO IEMS OM Processing Job Status
Location: 10.102.15.138
Job Instance: CollectionJob12
State: Successful
Category: other
ComponentID: EMS-IEMS=10.102.15.138,Software=CollectionJob12;
Time: Feb 25 14:26:13 2005
Description: Processing successfully done for the MOs:
[IEMS-Mgr]
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
ComponentID	character string	Indicates the details of the component.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS652

Log report EMJS652 is generated to report the failure of a CSV or MDM collection job.

The IEMS generates log report EMJS652.

Format

The format for log report EMJS652 is as follows:

```
MSH10    EMJS652 MAR04 17:30:15 0495 INFO IEMS OM Processing Job Status
Location: 47.142.94.68
Job Instance: mscColl_AM
State: Failure
Category: other
ComponentID: EMS-IEMS=47.142.94.68,Software=mscColl_AM;
Time: Mar 04 17:30:15 2005
Description: Invalid file format
File Name: {wnc0y0ns.us.nortel.com-CSE-Mgr=No files available in
the Directory (/export/home/maint/omDir/mcsOMfiles/SM_0/AM1_0/csv)
to process. Check done for the MO :
wnc0y0ns.us.nortel.com-CSE-Mgr}
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
State	Incomplete, Failure	Indicates the state of the job.
ComponentId	character string	Indicates the details of the component.

Action

For detailed error information, monitor the perf_log.txt debug log on the IEMS server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS661

Log report EMJS661 indicates the successful completion of a report job.

The IEMS generates log report EMJS661.

Format

The format for log report EMJS661 is as follows:

```
MSH10      EMJS661 FEB25 14:26:23 1589 INFO IEMS OM Report Job Status
Location: 10.102.15.138
Job instance: ReportJob6
State: Successful
Category: other
ComponentID: EMS-IEMS=10.102.15.138,Software=ReportJob6;
Time: Feb 25 14:26:23 2005
Description: /data/oms/1
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
Component Id	character string	Indicates the details of the component.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS662

Log report EMJS662 is generated to report the failure of an IEMS report job.

The IEMS generates log report EMJS662.

Format

The format for log report EMJS662 is as follows:

```
znc0s0jh  EMJS662 MAY02 04:25:00 0142 TBL IEMS OM Report Job Status
Location: 47.142.94.66
Job Instance: iems_report
State: Failure
Category: processingError
Cause: fileError
ComponentID: EMS-IEMS=47.142.94.66,Software=iems_report;
Time: May 02 04:25:00 2005
Description: /data/oms/1
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
State	Incomplete, Failure	Indicates the state of the job - Incomplete or Failure.
Time	character string	Indicates the date and time of the log.
ComponentId	character string	Indicates the details of the component.
Equipment identifier	IP address	Indicates the hostname on which the IEMS server is running

Action

For detailed error information, monitor the perf_log.txt debug log on the IEMS server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS671

Log report EMJS671 indicates the status of a transfer job.

The IEMS generates log report EMJS671.

Format

The format for log report EMJS671 is as follows:

```
MSH10 EMJS671 MAR31 00:40:06 3811 INFO IEMS OM Transfer Job Status
Location: 10.102.15.138
Job instance: TransferJob14
State: Successful
Category: other
ComponentID: EMS-IEMS=10.102.15.138,Software=TransferJob14;
Time: Mar 31:00:40:06 2005
Description: TransferJob14 job has been executed successfully
FileName : GWC.10.102.15.48-GWC.OMs.GWCREPORT2005.03.31_00.40.02_
EST.xml.gz
Destination: 10.102.15.18
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
ComponentID	character string	Indicates the details of the component.
Destination	IP address	Indicates the name of the device to which the file is transferred.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS672

Log report EMJS672 indicates the failure of a transfer job.

The IEMS generates log report EMJS672.

Format

The format for log report EMJS672 is as follows:

```
znc0s0jh    EMJS672 MAY02 09:11:32 0502 TBL IEMS OM Transfer Job Status
Location: 47.142.94.66
Job instance: sspfs_tran
State: Incomplete
Category: other
ComponentID: EMS-IEMS=47.142.94.66,Software=sspfs_tran;
Time: May 02 09:11:32 2005
File Name:
SSPFS.47.142.94.68-SSPFS.OMs.bob.2005.05.02_07.38.14_EST.csv.
gz,
Destination: 47.142.94.68
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Job Instance	character string	Indicates the job name.
State	Incomplete	Indicates the state of the job.
Time	character string	Indicates the date and time of the log.
ComponentId	character string	Indicates the details of the component.
FileName	character string	Indicates the file name.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS840

Log report EMJS840 is generated when the IEMS OM collection subsystem detects that a collected attribute has exceeded a configured threshold.

The IEMS generates log report EMJS840.

Format

The format for log report EMJS840 is as follows:

```
znc0s0jh *** EMJS840 MAY04 00:48:35 0008 TBL Threshold Alarm
  Location: 47.142.94.66
  Job Instance: sspfs
  Time: May 04 00:48:35 2005
  State: Critical
  Category: Threshold
  Cause: Threshold Alarm
  ComponentID: EMS-IEMS=47.142.94.66;Software=sspfs;Node=47.142.94.68
  Monitored Value: iplnReceives
  Collected Value: 13271720
  Threshold Type: max
  Threshold: 100
  Rearm Value: 80
  Description: Threshold Exceeded
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Job Instance	character string	Indicates the job name.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the IP address, job name and node ID of the device.
Monitored Value	character string	Indicates the OID for which the data is collected.

Field	Value	Description
Collected Value	integer	Indicates the actual value collected from the device for this OID.
Threshold type	character string	Indicates the threshold type based on the configured threshold (Max/Min/Equal).
Threshold	integer	Indicates the actual threshold value configured for a threshold.
Rearm Value	integer	Indicates the actual rearm value configured for a threshold.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMJS841

Log report EMJS841 is generated when the IEMS OM collection subsystem detects that a collected attribute dropped below a configured threshold value. This log is used to clear the alarm event raised in the log report EMJS840 event.

The IEMS generates log report EMJS841.

Format

The format for log report EMJS841 is as follows:

```
znc0s0jh  EMJS841 MAY04 00:52:15 0020 TBL Threshold Alarm
Location: 47.142.94.66
Job Instance: sspfs
Time: May 04 00:52:15 2005
State: Clear
Category: Threshold
Cause: Threshold Alarm
ComponentID: EMS-IEMS=47.142.94.66;Software=sspfs;Node=
47.142.94.68
Monitored Value: iplnReceives
Collected Value: 13273301
Threshold type: max
Description: Collected Value is below the Threshold limit.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Job Instance	character string	Indicates the job name.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the IP address, job name and node ID of the device.
Monitored Value	character string	Indicates the OID for which the data is collected.

Field	Value	Description
Collected Value	integer	Indicates the actual value collected from the device for this OID.
Threshold type	character string	Indicates the threshold type based on the configured threshold (Max/Min/Equal).

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS300

Log report EMSS300 indicates that the client-side PAM + Radius SPI is unable to communicate with the server-side Radius interface.

Note: This log is sent directly to syslog through the standard UNIX syslog C API.

The generates log report EMSS300.

Format

The format for log report EMSS300 is as follows:

```
znc0s0jh      EMSS300 JUN30 11:09:16 0721 INFO EMSS^M
Location: <CLIENT - hostname>
Time: Jun 30 11:09:16
Category: communicationsAlarm
Probable Cause: connectionEstablishmentError
Component Id: PAM+ Radius SPI
Description: RADIUS server <SERVER-hostname> failed to
respond.
Recovery Action: Please verify network connectivity for both
client and server machines; verify the RADIUS server is
running.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	communications Alarm	Indicates the category of the alarm.
Probable cause	connection Establishment Error	Indicates the probable cause of the alarm.
Client-hostname	character string	Indicates the hostname of the client.
Time	character string	Indicates the date and time of the log.
Server-hostname	character string	Indicates the hostname of the server.

Action

Verify network connectivity for both client and server machines. Verify that the Radius server is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS301

Log report EMSS301 indicates that a problem is detected by the Radius server in the process of handling a given authentication request. These problems are unexpected exceptions detected by Radius server plugins. These problems can be due to incorrect Radius server setup or the unavailability of a critical Radius server dependency.

The IEMS generates log report EMSS301.

Format

The format for log report EMS301 is as follows:

```
znc0s0jh    EMSS301 JUN30 11:09:16 0721 INFO EMSS^M
<Device name:device port> EMSS
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: outOfService
Component Id: Radius Proxy
Description: <LoginException message from Radius>
Recovery Action: Check the status of the Sun IS and restart if
necessary.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingErrorAlarm	Indicates the category of the alarm.
Probable cause	outOfService	Indicates the probable cause of the alarm.
Device name:device port	character string	Indicates the device name and device port.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Check the status of the SunOne Identity Server (S1 IS) and restart if necessary.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS302

Log report EMSS302 indicates that the Radius policy plugin detects no single-sign-on token. This indicates that there is a problem with the Sun Identity Server or that the Sun Identity Server is not running.

The IEMS generates log report EMSS302.

Format

The format for log report EMSS302 is as follows:

```
znc0s0jh      EMSS302 JUN30 11:09:16 0721 INFO EMSS^M
<Device name:device port> EMSS
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: outOfService
Component Id: Radius Proxy
Description: No single-sign-on token available
after authentication.
Recovery Action: Check the status of Sun IS and restart if
necessary.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingErrorAlarm	Indicates the category of the alarm
Probable Cause	outOfService	Indicates the probable cause of the alarm
Device name:device port	character string	Indicates the device name and device port.
application name	character string	Indicates the application name.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Check the status of the Sun Identity Server and restart if necessary.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS304

Log report EMSS304 indicates that the pam_mkhomedir module has timed out. This log is produced when the pam_mkhomedir module invokes the script mkhomedir, but the script does not return within the timeout period (default 30 seconds).

The IEMS generates log report EMSS304.

Format

The format for log report EMSS304 is as follows:

```
znc0s0jh      EMSS304 JUN30 11:09:16 0721 INFO EMSS^M
Location: <CLIENT - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: timeoutExpired
Component Id: PAM MAKE HOME DIRECTORY SPI
Description: Authentication with a pthread was timed out
(30 seconds)
Recovery Action: The process running the script file (script_
name) might not work properly and blocked the main process
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingErrorAlarm	Indicates the category of the alarm.
Probable cause	timeoutExpired	Indicates the probable cause of the alarm.
Client-hostname	character string	Indicates the hostname of the client.
Time	character string	Indicates the date and time of the log.
Server-hostname	character string	Indicates the hostname of the server.

Action

Check the process running the script and kill it if necessary.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS305

Log report EMSS305 indicates that the client side PAM+ Radius SPI is unable to communicate with the server-side Radius interface.

The IEMS generates log report EMSS305.

Format

The format for log report EMSS305 is as follows:

```
znc0s0jh    EMSS305 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: communicationsAlarm
Probable Cause: communicationsProtocolError
Component Id: PAM+ Radius SPI
Description: Error reading packet from RADIUS server <SERVER -
hostname>
Recovery Action: Please verify network connectivity for both
client and server machines; verify server is running.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	communications Alarm	Indicates the category of the alarm.
Probable cause	communications ProtocolError	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Verify network connectivity for both client and server machines. Verify that the Radius server is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS306

Log report EMSS306 indicates that a packet from the Radius server is corrupted. The PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS306 is sent directly to syslog through the standard Unix syslog C API.

The IEMS generates log report EMSS306.

Format

The format for log report EMSS306 is as follows:

```
znc0s0jh      EMSS306 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: communicationsAlarm
Probable Cause: communicationsProtocolError
Component Id: PAM+ Radius SPI
Description: RADIUS packet from server <SERVER - hostname>
is corrupted.
Recovery Action: Please verify network connectivity for both client
and server machines; verify RADIUS server is running.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	communications Alarm	Indicates the category of the alarm.
Probable cause	communications ProtocolError	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Verify network connectivity for both client and server machines. Verify that the server is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS307

Log report EMSS307 indicates that a packet from the Radius server has failed verification. The PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS307 is sent directly to syslog through the standard Unix syslog C API.

The IEMS generates log report EMSS307.

Format

The format for log report EMSS307 is as follows:

```
znc0s0jh      EMSS307 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: communicationsAlarm
Probable Cause: communicationsProtocolError
Component Id: PAM+ Radius SPI
Description: Packet from RADIUS server <SERVER - hostname>
fails verification.
Recovery Action: Please verify network connectivity for both client
and server machines; verify RADIUS server is running and that the
shared secret is correct.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	communications Alarm	Indicates the category of the alarm.
Probable cause	communications ProtocolError	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Verify network connectivity for both client and server machines. Verify that the server is running and that the shared secret is correct.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS308

Log report EMSS308 indicates that the client-side PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS308 is sent directly to syslog through the standard Unix syslog C API.

The IEMS generates log report EMSS308.

Format

The format for log report EMSS308 is as follows:

```
znc0s0jh      EMSS308 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: communicationsAlarm
Probable Cause: invalidMessageReceived
Component Id: PAM+ Radius SPI
Description: Response packet from RADIUS server <SERVER - hostname>
does not match the request packet id.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	communications Alarm	Indicates the category of the alarm.
Probable cause	invalidMessage Received	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS309

Log report EMSS309 indicates that a packet from the Radius server does not contain all required fields. The client-side PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS309 is sent directly to syslog through the standard Unix syslog C API.

The IEMS generates log report EMSS309.

Format

The format for log report EMSS309 is as follows:

```
znc0s0jh      EMSS309 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: communicationsAlarm
Probable Cause: invalidMessageReceived
Component Id: PAM+ Radius SPI
Description: Packet from RADIUS server <SERVER - hostname>
does not contain all required fields.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	communications Alarm	Indicates the category of the alarm.
Probable cause	invalidMessage Received	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS310

Log report EMSS310 indicates that the client configuration file cannot be opened. The PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS310 is sent directly to syslog through the standard Unix syslog C API.

The IEMS generates log report EMSS310.

Format

The format for log report EMSS310 is as follows:

```
znc0s0jh      EMSS310 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM+ Radius SPI
Description: Could not open client configuration file.
Recovery Action: Please verify access to /etc/raddb/server on the
client machine.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Verify network connectivity for both client and server machines. Verify that the server is running and that the configuration file is accessible.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS311

Log report EMSS311 indicates that the PAM+ Radius SPI is unable to communicate with the Radius Identity Server.

Note: Log report EMSS311 is sent directly to syslog through the standard Unix syslog C API.

The IEMS generates log report EMSS311.

Format

The format for log report EMSS311 is as follows:

```
znc0s0jh      EMSS311 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM+ Radius SPI
Description: Failed to read hostname or secret.
Recovery Action: Please verify access to /etc/raddb/server on the
client machine.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Verify network connectivity for both client and server machines. Verify that the server is running and that /etc/raddb/server is available on the client machine.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS312

Log report EMSS312 indicates that the pam_mkhomedir module is not able to retrieve user information from the NSSwitch. This log is produced when the pam_mkhomedir module attempts to retrieve user information from the NSSwitch by using getpwnam and fails.

Note: Log report EMSS312 is sent directly to syslog through the standard Unix syslog C API.

The IEMS generates log report EMSS312.

Format

The format for log report EMSS312 is as follows:

```
znc0s0jh      EMSS312 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM MAKE HOME DIRECTORY SPI
Description: Not able to do getpwnam with the user: (user_name) due
the error: (error message).
Recovery Action: Check NSSwitch configuration and ensure it works
with the user
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Time	character string	Indicates the date and time of the log.
SERVER - hostname	character string	Indicates the server and hostname.

Action

Check the NSSwitch configuration and ensure it works with the user.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS313

Log report EMSS313 indicates the radius server monitor detects the radius process is not functional.

Note: This log report is sent directly to syslog through the "logger" Unix utility.

Format

The format for log report EMSS313 is as follows:

```
znc0s0jh      EMSS313 JUN30 11:09:16 0721 INFO EMSS^M
Location: 47.142.94.68
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: outOfService
Component Id: CLASS=SYS;SYSTYPE=SECMon;SECMonComp=RADSVR
Description: RADSVR is unhealthy, will restart if currently
running.^M
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	outOfService	Indicates the probable cause of the alarm.

Action

The health monitor automatically attempts to restart the radius server if the radius server is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS314

Log report EMSS314 indicates the identity server health monitor detects the server process is not functional.

Note: This log report is sent directly to syslog through the "logger" Unix utility.

Format

The format for this log report is as follows:

```
znc0s0jh      EMSS314 JUN30 11:09:16 0721 INFO EMSS^M
Location: 47.142.94.68
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: outOfService
Component Id: CLASS=SYS;SYSTYPE=SECMon;SECMonComp=IS
Description: Identity Server (IS) is unhealthy, will restart
if currently running.^M
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	outOfService	Indicates the probable cause of the alarm.

Action

The health monitor automatically attempts to restart the identity server if the identity server is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS315

Log report EMSS315 indicates the PAM login servlet health monitor detects the PAM login servlet is not functional.

The IEMS generates log report EMSS315.

Format

The format for log report EMSS315 is as follows:

```
znc0s0jh      EMSS315 JUN30 11:09:16 0721 INFO EMSS^M
Location: <CLIENT - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: outOfService
Component Id: CLASS=SYS;SYSTYPE=SECMon;SECMonComp=WEBSERVICES
Description: PAM login servlet is unhealthy, restarting
WEBSERVICES.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	outOfService	Indicates the probable cause of the alarm.

Action

The health monitor automatically attempts to restart WEBSERVICES through servman if it is running already.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS316

Log report EMSS316 indicates the pam_mkhomedir module cannot use the script that is owned by the user.

The IEMS generates log report EMSS316.

Format

The format for log report EMSS316 is as follows:

```
znc0s0jh      EMSS316 JUN30 11:09:16 0721 INFO EMSS^M
Location: <CLIENT - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM MAKE HOME DIRECTORY SPI
Description: Not able to use the script (script_name) since
the ownership of the script is not root
Recovery Action: Change the ownership of the script file to
root
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Check the ownership of the script and change the owner to root.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS317

Log report EMSS317 indicates the pam_mkhomedir module cannot get the script.

The IEMS generates log report EMSS317.

Format

The format for log report EMSS317 is as follows:

```
znc0s0jh      EMSS317 JUN30 11:09:16 0721 INFO EMSS^M
Location: <CLIENT - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM MAKE HOME DIRECTORY SPI
Description: Not able to use the script (script_name) due to
(file errors)
Recovery Action: Please verify if the script file (script_
name) exists
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Verify the script is available and the name of the script is correct.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS318

Log report EMSS318 indicates the pam_mkhomedir module cannot continue since the euid is not root.

The IEMS generates log report EMSS318.

Format

The format for log report EMSS318 is as follows:

```
znc0s0jh      EMSS318 JUN30 11:09:16 0721 INFO EMSS^M
Location: <CLIENT - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM MAKE HOME DIRECTORY SPI
Description: No permissions to continue since the euid of the
current process is not root: (uid)
Recovery Action: The effective user id of the process has to
be root
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Make sure the effective user id of the process running the module is root.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS319

Log report EMSS319 indicates the pam_is_authentication module cannot get the configuration file.

The IEMS generates log report EMSS319.

Format

The format for log report EMSS319 is as follows:

```
znc0s0jh      EMSS319 JUN30 11:09:16 0721 INFO EMSS^M
Location: <CLIENT - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM IS AUTHENTICATION SPI
Description: Could not get IS auth configuration file: (file_
name)
Recovery Action: Please provide an IS auth config file with
pam opetion conf=/dir/file, or put you is auth config file
in the default location
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Verify if the configuration file is on the location configured by the pam option of if it is on the default location.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS320

Log report EMSS320 indicates the pam_is_authentication module cannot read the configuration file. This log is produced when the module attempts to read the contents of the configuration file but fails.

The IEMS generates log report EMSS320.

Format

The format for log report EMSS320 is as follows:

```
znc0s0jh      EMSS320 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM IS AUTHENTICATION SPI
Description: Could not open the IS auth configuration file
(file_name)
Recovery Action: Please verify the permissions of file
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Server-hostname	character string	Indicates the hostname of the server.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.

Action

Configure and start the SunOne Identity Server (S1 IS). Then restart the Tomcat servlet engine.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS321

Log report EMSS321 indicates the pam_is_authentication module cannot get the auth url.

The IEMS generates log report EMSS321.

Format

The format for log report EMSS321 is as follows:

```
znc0s0jh      EMSS321 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM IS AUTHENTICATION SPI
Description: Missing IS auth url from the config file (file_
name)
Recovery Action: Please verify the auth url is set correctly
in the config file: (file_name)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.

Action

Verify the auth url option is set correctly from the configuration file.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS322

Log report EMSS322 indicates the pam_is_authentication module is blocked and timed out.

The IEMS generates log report EMSS322.

Format

The format for log report EMSS322 is as follows:

```
znc0s0jh      EMSS322 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: timeoutExpired
Component Id: PAM IS AUTHENTICATION SPI
Description: Authentication was blocked and timed out
(seconds of timeout)
Recovery Action: Please check if IS processes work properly
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	timeoutExpired	Indicates the probable cause of the alarm.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.

Action

Verify the IS processes work properly. Restart IS processes if necessary.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS323

Log report EMSS323 indicates the pam_is_authentication module cannot get the configuration file.

The IEMS generates log report EMSS323.

Format

The format for log report EMSS323 is as follows:

```
znc0s0jh      EMSS323 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM IS VALIDATION SPI
Description: Could not get IS auth configuration file:
(file_name)
Recovery Action: Please provide an IS auth config file with
pam option conf=/dir/file, or put you is auth config file in
the default location
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm
Probable cause	fileError	Indicates the probable cause of the alarm.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.

Action

Verify if the configuration file is on the location configured by the pam option or if it is on the default location.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS324

Log report EMSS324 indicates the pam_is_module cannot read the configuration file.

The IEMS generates log report EMSS324.

Format

The format for log report EMSS324 is as follows:

```
znc0s0jh      EMSS324 JUN30 11:09:16 0721 INFO EMSS^M
Location: <SERVER - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM IS VALIDATION SPI
Description: Could not open the IS auth configuration file
(file_name)
Recovery Action: Please verify the permissions of file
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Location	character string	Indicates the server and hostname.
Time	character string	Indicates the date and time of the log.

Action

Verify the configuration file is readable.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS325

Log report EMSS325 indicates the pam_is_authentication module cannot get the auth url.

The IEMS generates log report EMSS325.

Format

The format for log report EMSS325 is as follows:

```
znc0s0jh      EMSS325 JUN30 11:09:16 0721 INFO EMSS^M
Location: <CLIENT - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM IS VALIDATION SPI
Description: Missing IS auth url from the config file (file_
name)
Recovery Action: Please verify the auth url is set correctly
in the config file: (file_name)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Verify the auth url option is set correctly from the configuration file.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS326

Log report EMSS326 indicates the pam_is_authentication module is blocked and timed out.

The IEMS generates log report EMSS326.

Format

The format for log report EMSS326 is as follows:

```
znc0s0jh      EMSS326 JUN30 11:09:16 0721 INFO EMSS^M
Location: <CLIENT - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: timeoutExpired
Component Id: PAM IS VALIDATION SPI
Description: Validation was blocked and timed out (seconds of
timeout)
Recovery Action: Please check if IS processes work properly
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	timeoutExpired	Indicates the probable cause of the alarm.

Action

Verify the IS processes work properly. Restart the IS processes if necessary.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS327

Log report EMSS327 indicates the script (default is mkhomedir) cannot access the directory or files.

The IEMS generates log report EMSS327.

Format

The format for log report EMSS327 is as follows:

```
znc0s0jh      EMSS327 JUN30 11:09:16 0721 INFO EMSS^M
Location: <CLIENT - hostname>
Time: Jun 30 11:09:16
Category: processingErrorAlarm
Probable Cause: fileError
Component Id: PAM Make Home Directory SPI
Description: File/Directory access error when executing the
script (script_name)
Recovery Action: Please perform actions according to the
error message: (error message)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Verify the directory files are available and accessible. The error messages show which files or directories to check.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS330

Log report EMSS330 indicates that the PAM proxy did not initialize the single signon facility and SSO tokens will not be generated.

The IEMS generates log report EMSS30.

Format

The format for log report EMSS330 is as follows:

```
MSH10      EMSS330 JUN30 11:09:16 0721 INFO <hostname> EMSS
Location: <hostname>
Time: Jun 30 11:09:16 2005
Category: processingErrorAlarm
Probable Cause: configurationOrCustomizationError
Component Id: PAM Proxy
Description: Failed to initialize single sign on facility. SSO
tokens will not be generated.
Recovery Action: Configure and start the Sun One Identity Server,
then restart the Tomcat servlet engine.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Hostname	character string	Indicates the hostname.
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.

Action

Configure and start the Sun One Identity Server. Then restart the Tomcat servlet engine.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS331

Log report EMSS331 indicates that the PAM proxy can not authenticate the user due to an unhandled internal error.

The IEMS generates log report EMSS331.

Format

The format for log report EMSS331 is as follows:

```
MSH10      EMSS331 JUN30 11:09:16 0721 INFO <hostname> EMSS
Location: <hostname>
Time: Jun 30 11:09:16 2005
Category: processingErrorAlarm
Probable Cause: softwareProgramError
Component Id: PAM Proxy
Description: Could not authenticate user due to unhandled internal error.
Recovery Action: Inspect the state of the centralized security server components. See debug logs in <filepath>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Hostname	character string	Indicates the hostname.
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Filepath	character string	Indicates the location of the debug logs.

Action

Inspect the state of the centralized security server components. View the debug logs.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS351

Log report EMSS351 indicates an exception that is raised while making a request to the servlet.

The IEMS generates log report EMSS351.

Format

The format for log report EMSS351 is as follows:

```
MSH10      EMSS351 JUN30 11:09:16 0721 INFO <hostname> EMSS
Location: <hostname>
Time: Tue Jun 30 11:09:16 2005
Category: communicationsAlarm
Probable Cause: communicationsProtocolError
Component Id: SSPFS=<hostname>;NODE=<host-
name>;CLASS=APPL;APPLTYPE=<application type>
Description: Exception caught while making request to the serv-
let. SAML
OAPBinding::send() failed while contacting SAML responder:
Failed to connect to <IP address>: Connection refused
Recovery Action: Please verify network connectivity for both cli-
ent and server machines; verify the SAML server is running.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Hostname	character string	Indicates the hostname.
Category	processingError Alarm	Indicates the category of the alarm.
Probable cause	fileError	Indicates the probable cause of the alarm.
Filepath	character string	Indicates the location of the debug logs.

Action

Verify network connectivity for both client and server machines. Verify that the SAML server is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS 600

Log report EMSS 600 indicates that the PAM Radius daemon modifies the /etc/passwd or /etc/group files.

The IEMS generates log report EMSS 600.

Format

The format for log report EMS 600 is as follows:

```
EMSS600 mmmdd hh:mm:ss NONE INFO <Device name:device port>  
<application name>  
Message: System files have been updated
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Device name:device port	character string	Indicates the device name and device port.
application name	character string	Indicates the application name.

Action

This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS 601

Log report EMSS 601 indicates that there are successful or failed authentication requests of the authentication module.

The IEMS generates log report EMSS 601.

Format

The format for log report EMS 601 is as follows:

```
EMSS601 mmmdd hh:mm:ss NONE INFO <Device name:device port>  
<application name>  
Message: <Successful (Failed) authentication attempt>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Device name:device port	character string	Indicates the device name and device port.
application name	character string	Indicates the application name.
Successful (Failed authentication attempt	character string	Indicates whether the authentication request is successful or has failed.

Action

This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS 602

Log report EMSS 602 indicates successful or failed PAM SPI events from PAM + Plug-Ins.

The IEMS generates log report EMSS 602.

Format

The format for log report EMS 602 is as follows:

```
EMSS602 mmmdd hh:mm:ss NONE INFO <Device name:device port>  
<application name>  
Message: Authentication successful/failed
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Device name:device port	character string	Indicates the device name and device port.
application name	character string	Indicates the application name.

Action

This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS 604

Log report EMSS 604 indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token destroy event. Sensitive token information is not included in these logs.

The IEMS generates log report EMSS 604.

Format

The format for log report EMS 604 is as follows:

```
mmm dd hh:mm:ss <device name:device port>Thread-28  
DESTROY: uid=administrator, ou=People, o=ca.nortel.com"
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
device name:device port	character string	Indicates the device name and device port.

Action

This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

EMSS 605

Log report EMSS 605 indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token timeout event. Sensitive token information is not included in these logs.

The IEMS generates log report EMSS 605.

Format

The format for log report EMS 605 is as follows:

```
mmm dd hh:mm:ss <device name:device port> Thread-28:  
IDLE TIMEOUT:uid=amAdmin, ou=People, o=ca.nortel.com"
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
device name:device port	character string	Indicates the device name and device port.

Action

This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS398

Log report IEMS398 indicates IEMS is unable to communicate with a managed device.

The IEMS generates log report IEMS398.

Format

The format for log report IEMS398 is as follows:

```
CABLAB *** IEMS398 DEC03 17:46:59 5150 FLT Communication Lost
Location: 47.135.43.7
Motification ID: 0
State: Raised
Category: Communications
Cause: Communications subsystem failure
Time: Dec 03 17:46:59 2004
ComponentId: ucary118c.ca.nortel.com
Specific Problem: Connection Lost
Description: IEMS Unable to communicate with managed device
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the name of the device.

Action

This log report requires the user to check network connectivity and device status to identify the cause of the communication failure.

Associated OM registers

This log report has the following associated OMs:

- numOfUnKnownDeviceStateTransitions
- numOfDevicesInUnKnownState

Additional information

This log report requires no additional information.

EMSS 603

Log report EMSS 603 indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token create event. Sensitive token information is not included in these logs.

The IEMS generates log report EMSS 603.

Format

The format for log report EMS 603 is as follows:

```
mmm dd hh:mm:ss <Device name:device port> Thread-28:
SESSION CREATE: uid=administrator, ou=People,
o=ca.nortel.com
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Device name:device port	character string	Indicates the device name and device port.

Action

This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS399

Log report IEMS399 indicates that IEMS regained communication with a managed device.

The IEMS generates log report IEMS399.

Format

The format for log report IEMS399 is as follows:

```
CABLAB      IEMS399 DEC03 17:47:49 5164 FLT Communication Regained
Location: 47.135.43.7
Notification ID: 0
State: Cleared
Category: Communications
Time: Dec 03 17:47:49 2004
Component Id: ucary118c.ca.nortel.com
Description: IEMS regained communication with the managed device
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the IEMS server.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the name of the device.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS601

Log report IEMS601 is generated when the IEMS receives an event from a device that is not configured in the IEMS inventory.

Format

The format for log report IEMS601 is as follows:

```
MSH10      IEMS601 0113 INFO IEMS SNMP Trap
Location: 47.142.106.203;47.142.106.203
Component Id: IEMS=47.142.106.203;Unknown=172.31.1.2
Description: SNMP Trap from unknown device
Event: .1.3.6.1.4.1.8072.4.0.2
Varbind0: .1.3.6.1.2.1.1.3.0: 3 hours, 51 minutes, 32 seconds.
Varbind1: .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.8072.4.0.2
```

Selected field descriptions

This log report has no selected field descriptions.

Action

Refer to *IEMS Configuration Management*, NN10330-511 and the configuration documentation for the unknown device and correct as required.

Associated OM registers

This log report has the following associated OMs:

- numOfEventsFromUnknownDevices
- numOfEventsFromUnknownSNMPDevices
- numOfEventsFromUnknownCustlogDevices

Additional information

This log report requires no additional information.

IEMS602

Log report IEMS602 is generated when the IEMS receives an event from a device in the IEMS inventory but the event type is not recognized.

Format

The format for log report IEMS602 is as follows:

```
MSH10      IEMS602 0031 INFO IEMS SNMP Trap
Location: 47.142.106.203;47.142.106.203
Component Id: IEMS=47.142.106.203;NE-STORM=Arthur
Description: Unknown SNMP Trap from managed device
Event: .1.3.6.1.4.1.8072.4.0.2
Varbind0: .1.3.6.1.2.1.1.3.0: 3 hours, 51 minutes, 32 seconds.
Varbind1: .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.8072.4.0.2
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the device that sent the associated event.

Action

Refer to the maintenance procedures for the device sending the SNMP trap.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS603

Log report IEMS603 is generated when the IEMS detects a gap in the sequence numbers for the events it is receiving from one of its managed devices.

The IEMS generates log report IEMS603.

Format

The format for log report IEMS603 is as follows:

```
MSH10      IEMS603 MAR31 12:01:29 9939 INFO Missed Notifications
Location:  10.102.15.138
Component Id: IEMS=msh10ptm-SAM21-Mgr
Time: Mar 31 12:01:29 2005
Description: Notification(s) missed in ML 112 - 237
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IEMS IP address.
Component name	character string	Indicates the component name of the device.
Time	character string	Indicates the date and time of the log.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEWS604

When IEMS receives a clear event without a corresponding raise event, this is referred to as an “orphaned clear” and will result in the generation of an extra IEMS615 INFO log. If that orphaned clear received by IEMS has no log name/number, it will give it one (IEWS604) before forwarding that event northbound to the OSS.

Note: MDM devices generate two types of clears and therefore IEMS does not generate this report for orphaned clears from MDM.

Format

The format for log report IEMS604 (STORM example) is as follows:

```
wnc0y0ns IEMS604 AUG22 11:57:54 4553 INFO Cleared
Location: a storm;47.131.125.5
Notification Id: 2151
State: Cleared
Time: Aug 22 11:57:54 2005
Component Id: STORMIA=bottom
Description: Status: Alarm cleared. Used memory percentage is
19.15.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	character string;IP address	Indicates the display name and IP address of the managed device.
Notification ID	Integer	Number used to set corresponding set and clear pairs.
State	character string	Whether an event was raised or cleared.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the component name.
Description	character string	Explanation of the event.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS606

Log report IEMS606 indicates that the event count has exceeded the configured threshold limit or that the deletion of events is complete.

The IEMS generates log report IEMS606.

Format

The format for log report IEMS606 is as follows:

```
RTPO      IEMS606 MAR01 11:12:36 5928 INFO Database Fault
Location: IEMS-Mgr (47.142.110.40)
State: INFO
Time: Mar 01 11:13:59 2005
Maximum No.of Event 1000000
Event count: 2116289
Description: Deletion of Events completed. The total number of
events deleted:1216289
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	IP address	Indicates the IP address of the event source.
Time	character string	Indicates the date and time of the log.
Maximum No. of Event	character string	Indicates the maximum number of events allowed before an event is generated.
Event count	character string	Indicates the total number of events in the database prior to the cleanup policy running.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS607

Log report IEMS607 indicates there is a discrepancy in the active alarm list between IEMS and the managed component. The discrepancy is found through alarm resynchronization. Differing alarm lists can occur when alarms have cleared in the managed component, but the clear log has not reached IEMS. In order to keep the downstream OSSs up to date, IEMS creates log report IEMS607.

The IEMS generates log report IEMS607.

Format

The format for log report IEMS607 is as follows:

```
MSH10  IEMS607 MAR31 00:40:13 3826 INFO IEMS Autogenerated Clear
Location: C1CM-000-B;10.102.15.153
NotificationID: 14
State: Clear
Time: Mar 31 00:40:13 2005
Specific Problem: Mate node failed - Broadcast failure and ask
components to promote to Master.
Category: equipment
Component Id: C1CM=C1CM-000-B;NodeType=C1cm
Description: Raised log: C1CM334; Audit: Mate Node Failed
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	character string;IP address	Indicates the display name and IP address of the managed device.
NotificationID	Integer	Indicates the notification Id field value from the database.
Time	character string	Indicates the date and time of the log.
Category	character string	Indicates the alarm category of the log.
Component Id	character string	Indicates the component Id field.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS614

Log report IEMS614 is generated when IEMS receives an OSI state change SNMP notification trap from an IEMS component.

IEMS generates log report IEMS614.

Format

The format for log report IEMS614 is as follows:

```
43 IEMS614 0004 INFO OSI State Change
    Location: MSCSimu_69;47.142.128.86
    Time: Apr 16 09:18:39 2005
    ComponentId:
    IEMS=47.153.164.133;CSE-UNIT=MSCSimu_69;47.142.128.86
    AdminState: unlocked
    OperationalState: enabled
    UnknownStatus: false
    Description: Received an OSI State Change SNMP Notification.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	character string; IP address	Indicates the display name and IP address of the managed device.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the component Id field.
AdminState	character string	Indicates the administrative states (locked, shutting down, or unlocked).
UnknownStatus	character string	Indicates the unknown status (ITU-T X.731). The value is true or false.
Description	character string	Indicates the trap meaning.

Action

No action required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS615

IEMS generates log report IEMS615 when it receives an orphaned clear, which is a clear event from a device when there is no corresponding raise event.

Note 1: When an orphaned clear is received without a log name or number, IEMS gives the clear a log name and number of IEMS604.

Note 2: MDM devices perform two types of clears and therefore IEMS does not generate this report for orphaned clears from MDM.

Format

The format for log report IEMS615 is as follows:

```
<OFFICE>      IEMS615 MMMDD hh:mm:ss <sequence number> INFO <Event Label>
Location: IEMS-Mgr;<hostname>
ComponentId: IEMS=IEMS-Mgr;<NE type>=<Equip Identifier>;<Component Id>
Time: Mmm DD hh:mm:ss YYYY
Description: Alarm clear event (<log name/number>) received
without a raise.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Sequence number	character string	Indicates a four-digit sequence number that can be used to detect lost logs. Value: 0000-9999
Event label	character string	Descriptive text about the log. Example: IEMS Received Stateless Clear
Component Id	character string	Displays the original component id field value that is extracted from the orphaned clear that IEMS received.
Hostname	character string; IP address	Indicates the IP address or hostname of the IEMS server. Example: 10.12.13.14

Field	Value	Description
NE type	character string	Indicates the device type where the orphaned clear originated. The value is a device type listed in the Device types for IEMS logs table. Example: NE-ERS_8600
Equip Identifier	character string	Indicates the value of the display name for a managed object. The display name is provisioned when the device is added into IEMS. If the device is auto-discovered, this name can come from the device itself or be a variation of the provisioned display name. Example for a duplex unit: SST NE: MYSST-Unit-0 and MYSST-Unit-1
Log name/number	character string	Displays a string of 5-7 characters indicating the log name and number. Example: IEMS604

Action

Please contact Nortel technical support

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IEMS616

Log report IEMS616 is generated when an SNMP protocol authentication failure occurs. It is an INFO event.

IEMS generates log report IEMS616.

Format

The format for log report IEMS616 is as follows:

```
<CLLI> IEMS616 MMMDD hh:mm:ss 0001 INFO <Type>=<IP Address> Info
Location: <display name>;<IP Address>
Cause: authenticationFailure
Time: <Mmm dd hh:mm:ss yyyy>
Component Id: <Type>=<IP Address>
Description: SNMP protocol authentication failure occurred
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	character string	Indicates the display name and IP address of the event source.
Cause	character string	Indicates the probable cause of the log.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the type and IP address of the device.

Action

No action required. This log report is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

PKM300

Log report PKM300 is generated when an attempt to create and validate an X509 certificate has failed or when X509 certificate creation and validation succeeds after previously having failed.

The Certificate Manager generates log report PKM300.

Format

The format for log report PKM300 in the raise state is as follows:

```
<OFFICE> ** PKM300 MMMDD hh:mm:ss 0721 TBL PKM Certificate generation failure
Location: PKManager=<hostname>
NotificationID: <NotificationID>
State: Raise
Category: ProcessingErrorAlarm
Cause: unspecifiedReason
Time: Mmm DD hh:mm:ss YYYY
Component Id: PKManager=<hostname>
Specific Problem: Failed to create valid certificate for CN: <device type> <IP address>
Description: Attempt to create and validate an X509 certificate failed
```

The format for log report PKM300 in the clear state is as follows:

```
<OFFICE> PKM300 MMMDD hh:mm:ss 0721 INFO PKM Certificate generation failure
Location: PKManager=<hostname>
NotificationID: <NotificationID>
State: Clear
Time: Mmm DD hh:mm:ss YYYY
Component Id: PKManager=<hostname>
Description: Attempt to create and validate an X509 certificate failed
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
NotificationID	integer	An integer which can be used in combination with the log name or number and component ID to uniquely identify the corresponding raise and clear logs for the alarm.
Category	character string	Indicates the X.733/X.736-based category of the alarm.
Cause	character string	Indicates the X.733/M.3100-based cause of the alarm.
Time	character string	Indicates the date/time of the alarm raise/clear.

Field	Value	Description
Hostname	character string	Indicates the hostname of the Certificate Manager.
Device type	character string	Indicates the device type which can be one of the following: GWC - Gateway Controller uses certificates for call processing control IPsec IKE communication with gateways. For example, GWC-1. MG9KVMG - MG 9000 virtual media gateway uses certificates for call processing control IPsec IKE communication with the gateway controller. For example, NE:1_9K01002-0-2 MG9KNE - MG 9000 network element uses certificates for OAM&P IPsec IKE communication with the MG 9000 Manager. For example, NE:1 (where 1 is the NE number). WEBPKPROXY - the Apache or Tomcat Certificate Manager proxy uses certificates for HTTPS connections to web browsers and servlets. For example, wnc0w0qy.us.nortel.com SSM - SSM uses certificates for OAM&P IPsec IKE communication used by the MG 9000 Manager to communicate with the MG 9000 network element. For example, SSM-1.

Action

If the state of the log is raise, verify that

- the Certificate Manager has been installed and initially configured correctly
- the Entity Default configured in Certificate Manager (Configure Broker-->Entity Settings) matches the issuer names of the

certificates generated by the Certificate Manager (Browse-->View Certificates). To view certificates, see "Viewing certificates using Certificate Manager" in *Nortel Carrier VoIP IPSec Security Service Implementation Overview*, NN10453-100.

If the state of the log is clear, no action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

PKM301

Log report PKM301 is generated when an attempt to deliver an X509 certificate to an application has failed or when delivery of an X509 certificate succeeds after previously having failed. Certificate Manager continues to attempt to deliver certificates to the affected device. The severity is major.

The Certificate Manager generates log report PKM301.

Format

The format for log report PKM301 in the raise state is as follows:

```
<OFFICE> ** PKM301 MMMDD hh:mm:ss 0721 TBL PKM Certificate delivery failure
Location: PKManager=<hostname>
NotificationID: <NotificationID>
State: Raise
Category: communicationsAlarm
Cause: transmitFailure
Time: Mmm DD hh:mm:ss YYYY
Component Id: PKManager=<hostname>
Specific Problem: Failed to deliver a certificate for CN: <device type>
<IP address>
Description: Attempt to deliver a certificate to an application for a
device failed
```

The format for log report PKM301 in the clear state is as follows:

```
<OFFICE> PKM301 MMMDD hh:mm:ss 0721 INFO PKM Certificate delivery failure
Location: PKManager=<hostname>
NotificationID: <NotificationID>
State: Clear
Time: Mmm DD hh:mm:ss YYYY
Component Id: PKManager=<hostname>
Description: Attempt to deliver a certificate to an application for a
device failed
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
NotificationID	integer	An integer which can be used in combination with the log name or number and component ID to uniquely identify the corresponding raise and clear logs for the alarm.
Category	character string	Indicates the X.733/X.736-based category of the alarm.
Cause	character string	Indicates the X.733/M.3100-based cause of the alarm.
Time	character string	Indicates the date/time of the alarm raise/clear.

Field	Value	Description
Hostname	character string	Indicates the hostname of the Certificate Manager.
Device type	character string	Indicates the device type which can be one of the following: GWC - Gateway Controller uses certificates for call processing control IPsec IKE communication with gateways. For example, GWC-1. MG9KVMG - MG 9000 virtual media gateway uses certificates for call processing control IPsec IKE communication with the gateway controller. For example, NE:1_9K01002-0-2 MG9KNE - MG 9000 network element uses certificates for OAM&P IPsec IKE communication with the MG 9000 Manager. For example, NE:1 (where 1 is the NE number). WEBPKPROXY - the Apache or Tomcat Certificate Manager proxy uses certificates for HTTPS connections to web browsers and servlets. For example, wnc0w0qy.us.nortel.com SSM - SSM uses certificates for OAM&P IPsec IKE communication used by the MG 9000 Manager to communicate with the MG 9000 network element. For example, SSM-1.

Action

If the state of the log is raise

- verify that network communication between device hosting the Certificate Manager application and the device hosting the element

managers is operational and that all management systems are available.

- verify whether a PKM306 log has been raised. If a PKM306 log is raised, follow the recovery procedure for the PKM306 log.
- verify that WEBSERVICES are running on all devices hosting the Certificate Manager and the element managers.
- verify that the WEBPKPROXY certificates listed in the Certificate Manager (Browse-->View Certificates) are the same certificates that are present in the /data/pkclient/certificates directory on the device, and that the certificates have been installed. To do this, establish a secure web session (https://) to the device and ensure that the certificate presented is the same as the certificate displayed in the Certificate Manager Browse-->View Certificates list. To view the certificates, see "Viewing Certificates using Certificate Manager" in *Nortel Carrier VoIP IPSec Security Service Implementation Overview*, NN10453-100.

If the WEBPKPROXY certificates are still REPLACE or CREATED, there is a communication problem with the target device. In this case, contact your next level of support.

If the state of the log is clear, no action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

PKM302

Log report PKM302 is generated when an X509 certificate used by a device to authenticate itself during call control operations has expired. The device cannot send or receive call control messages. Log report PKM302 is also generated when an X509 certificate for a call control device that was expired has been replaced with a new valid certificate. The severity is critical.

The Certificate Manager generates log report PKM302.

Format

The format for log report PKM302 in the raise state is as follows:

```
<OFFICE> *** PKM302 MMMDD hh:mm:ss 0721 TBL PKM Certificate expired
Location: PKManager=<hostname>
NotificationID: <NotificationID>
State: Raise
Category: timeDomainViolation
Cause: keyExpired
Time: Mmm DD hh:mm:ss YYYY
Component Id: PKManager=<hostname>
Specific Problem: Expired certificate for CN: <device type> <IP
address>
Description: A certificate used during call control operations has
expired
```

The format for log report PKM302 in the clear state is as follows:

```
<OFFICE> PKM302 MMMDD hh:mm:ss 0721 INFO PKM Certificate expired
Location: PKManager=<hostname>
NotificationID: <NotificationID>
State: Clear
Time: Mmm DD hh:mm:ss YYYY
Component Id: PKManager=<hostname>
Description: A certificate used during call control operations has
expired
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
NotificationID	integer	An integer which can be used in combination with the log name or number and component ID to uniquely identify the corresponding raise and clear logs for the alarm.
Category	character string	Indicates the X.733/X.736-based category of the alarm.
Cause	character string	Indicates the X.733/M.3100-based cause of the alarm.
Time	character string	Indicates the date/time of the alarm raise/clear.

Field	Value	Description
Hostname	character string	Indicates the hostname of the Certificate Manager.
Device type	character string	Indicates the device type which can be one of the following: GWC - Gateway Controller uses certificates for call processing control IPsec IKE communication with gateways. For example, GWC-1. MG9KVMG - MG 9000 virtual media gateway uses certificates for call processing control IPsec IKE communication with the gateway controller. For example, NE:1_9K01002-0-2 MG9KNE - MG 9000 network element uses certificates for OAM&P IPsec IKE communication with the MG 9000 Manager. For example, NE:1 (where 1 is the NE number). WEBPKPROXY - the Apache or Tomcat Certificate Manager proxy uses certificates for HTTPS connections to web browsers and servlets. For example, wnc0w0qy.us.nortel.com SSM - SSM uses certificates for OAM&P IPsec IKE communication used by the MG 9000 Manager to communicate with the MG 9000 network element. For example, SSM-1.

Action

If the state of the log is raise, this indicates that an existing condition has been escalated. It can also indicate a failure to deliver certificates in a timely manner to the device. If the state of the log is raise:

- if a PKM301 log is also raised, follow the recovery procedure for the PKM301 log.
- verify the state of the device certificate in Certificate Manager (Browse-->View Certificates). To view certificates, see "Viewing certificates using Certificate Manager" in *Nortel Carrier VoIP IPSec Security Service Implementation Overview*, NN10453-100. If the state is REPLACE, follow the recovery process for the PKM301 alarm. If this fails to advance the certificate to the DELIVERED state, contact your next level of support.
- If the certificate is an imported certificate or a GENERICINTERNAL certificate, delete the certificate and generate a new certificate.

If the state of the log is clear, no action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

PKM303

Log report PKM303 is generated when the expiration date of an X509 certificate has reached the forewarning date for the last alarm before expiration. A previous forewarning date has already passed. The alarm raised at that time has been escalated. Log report PKM303 is also generated when an X509 certificate has been replaced and delivered successfully to the device after the replaced certificate reached the last alarm before expiration date. The severity is major.

The Certificate Manager generates log report PKM303.

Format

The format for log report PKM303 in the raise state is as follows:

```
<OFFICE> ** PKM303 MMMDD hh:mm:ss 0721 TBL PKM Certificate Manager Trouble
  Location: PKManager=<hostname>
  NotificationID: <NotificationID>
  State: Raise
  Category: timeDomainViolation
  Cause: thresholdCrossed
  Time: Mmm DD hh:mm:ss YYYY
  Component Id: PKManager=<hostname>
  Specific Problem: A certificate will expire soon CN: <device type> <IP
  address>
  Description: Last forewarning of an impending certificate expiration
```

The format for log report PKM303 in the clear state is as follows:

```
<OFFICE> PKM303 MMMDD hh:mm:ss 0721 INFO PKM Certificate Manager Trouble
  Location: PKManager=<hostname>
  NotificationID: <NotificationID>
  State: Clear
  Time: Mmm DD hh:mm:ss YYYY
  Component Id: PKManager=<hostname>
  Description: Last forewarning of an impending certificate expiration
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
NotificationID	integer	An integer which can be used in combination with the log name or number and component ID to uniquely identify the corresponding raise and clear logs for the alarm.
Category	character string	Indicates the X.733/X.736-based category of the alarm.
Cause	character string	Indicates the X.733/M.3100-based cause of the alarm.
Time	character string	Indicates the date/time of the alarm raise/clear.

Field	Value	Description
Hostname	character string	Indicates the hostname of the Certificate Manager.
Device type	character string	Indicates the device type which can be one of the following: GWC - Gateway Controller uses certificates for call processing control IPsec IKE communication with gateways. For example, GWC-1. MG9KVMG - MG 9000 virtual media gateway uses certificates for call processing control IPsec IKE communication with the gateway controller. For example, NE:1_9K01002-0-2 MG9KNE - MG 9000 network element uses certificates for OAM&P IPsec IKE communication with the MG 9000 Manager. For example, NE:1 (where 1 is the NE number). WEBPKPROXY - the Apache or Tomcat Certificate Manager proxy uses certificates for HTTPS connections to web browsers and servlets. For example, wnc0w0qy.us.nortel.com SSM - SSM uses certificates for OAM&P IPsec IKE communication used by the MG 9000 Manager to communicate with the MG 9000 network element. For example, SSM-1.

Action

If the state of the log is raised for more than two hours, verify the expiration thresholds in Certificate Manager (Configure Broker-->Broker Settings). To log into the Certificate Manager, see "Launching the Certificate Manager" in *Nortel Carrier VoIP IPsec Security Service Implementation Overview*, NN10453-100. The values for all devices should be set to 168 hours for minor and 72 hours for

major. The values for the GWC should be set to 840 hours for minor and 420 hours for major. The certificate expiry days should be set to at least 90 days.

If the certificate is an imported certificate or a GENERICINTERNAL certificate, delete the certificate and generate a new certificate.

Verify whether a PKM301 or PKM306 log is raised and follow the recovery procedures for those logs. For details, see PKM301 and PKM306.

If the state of the log is clear, no action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

PKM304

Log report PKM304 is generated when the expiration date of an X509 certificate has reached the date for the initial expiration warning. Log report PKM304 is also generated when an X509 certificate has been replaced and delivered successfully to the device after the replaced certificate has raised the initial log. The severity is minor.

The Certificate Manager generates log report PKM304.

Format

The format for log report PKM304 in the raise state is as follows:

```
<OFFICE> * PKM304 MMMDD hh:mm:ss 0721 TBL PKM Certificate Manager Trouble
  Location: PKManager=<hostname>
  NotificationID: <NotificationID>
  State: Raise
  Category: timeDomainViolation
  Cause: thresholdCrossed
  Time: Mmm DD hh:mm:ss YYYY
  Component Id: PKManager=<hostname>
  Specific Problem: A certificate will expire soon CN: <device type> <IP
  address>
  Description: Initial forewarning of an impending certificate expira-
  tion
```

The format for log report PKM304 in the clear state is as follows:

```
<OFFICE> PKM304 MMMDD hh:mm:ss 0721 INFO PKM Certificate Manager Trouble
  Location: PKManager=<hostname>
  NotificationID: <NotificationID>
  State: Clear
  Time: Mmm DD hh:mm:ss YYYY
  Component Id: PKManager=<hostname>
  Description: Initial forewarning of an impending certificate expira-
  tion
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
NotificationID	integer	An integer which can be used in combination with the log name or number and component ID to uniquely identify the corresponding raise and clear logs for the alarm.
Category	character string	Indicates the X.733/X.736-based category of the alarm.
Cause	character string	Indicates the X.733/M.3100-based cause of the alarm.
Time	character string	Indicates the date/time of the alarm raise/clear.

Field	Value	Description
Hostname	character string	Indicates the hostname of the Certificate Manager.
Device type	character string	Indicates the device type which can be one of the following: GWC - Gateway Controller uses certificates for call processing control IPsec IKE communication with gateways. For example, GWC-1. MG9KVMG - MG 9000 virtual media gateway uses certificates for call processing control IPsec IKE communication with the gateway controller. For example, NE:1_9K01002-0-2 MG9KNE - MG 9000 network element uses certificates for OAM&P IPsec IKE communication with the MG 9000 Manager. For example, NE:1 (where 1 is the NE number). WEBPKPROXY - the Apache or Tomcat Certificate Manager proxy uses certificates for HTTPS connections to web browsers and servlets. For example, wnc0w0qy.us.nortel.com SSM - SSM uses certificates for OAM&P IPsec IKE communication used by the MG 9000 Manager to communicate with the MG 9000 network element. For example, SSM-1.

Action

If the state of the log is raise for more than two hours,

- verify that the Certificate Manager has been installed and initial configuration has been successfully completed.
- verify the expiration thresholds in Certificate Manager (Configure Broker-->Broker Settings). To log into the Certificate Manager, see

"Launching the Certificate Manager" in *Nortel Carrier VoIP IPSec Security Service Implementation Overview*, NN10453-100. The values for all devices should be set to 168 hours for minor and 72 hours for major. The values for the GWC should be set to 840 hours for minor and 420 hours for major. The certificate expiry days should be set to at least 90 days. If any changes are made to these values, wait for 30 minutes before taking any further action at the Certificate Manager.

- If the certificate is an imported certificate or a GENERICINTERNAL certificate, delete the certificate and generate a new certificate.
- Verify whether a PKM301 or PKM306 log is raised and follow the recovery procedures for those logs. For details see PKM301 and PKM306.

If the state of the log is clear, no action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

PKM305

Log report PKM305 is generated when an X509 certificate used by a device to authenticate itself for OAM&P functions has expired. The device cannot send or receive OAM&P commands. Log report PKM305 is also generated when an X509 certificate for an OAM&P device that was expired has been replaced with a new valid certificate. The severity is major.

The Certificate Manager generates log report PKM305.

Format

The format for log report PKM305 in the raise state is as follows:

```
<OFFICE> ** PKM305 MMMDD hh:mm:ss 0721 TBL PKM Certificate expired
  Location: PKManager=<hostname>
  NotificationID: <NotificationID>
  State: Raise
  Category: timeDomainViolation
  Cause: keyExpired
  Time: Mmm DD hh:mm:ss YYYY
  Component Id: PKManager=<hostname>
  Specific Problem: Expired certificate for CN: <device type> <IP
  address>
  Description: A certificate used for OAM&P functions has expired
```

The format for log report PKM305 in the clear state is as follows:

```
<OFFICE> PKM305 MMMDD hh:mm:ss 0721 INFO PKM Certificate expired
  Location: PKManager=<hostname>
  NotificationID: <NotificationID>
  State: Clear
  Time: Mmm DD hh:mm:ss YYYY
  Component Id: PKManager=<hostname>
  Description: A certificate used for OAM&P functions has expired
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
NotificationID	integer	An integer which can be used in combination with the log name or number and component ID to uniquely identify the corresponding raise and clear logs for the alarm.
Category	character string	Indicates the X.733/X.736-based category of the alarm.
Cause	character string	Indicates the X.733/M.3100-based cause of the alarm.
Time	character string	Indicates the date/time of the alarm raise/clear.

Field	Value	Description
Hostname	character string	Indicates the hostname of the Certificate Manager.
Device type	character string	Indicates the device type which can be one of the following: GWC - Gateway Controller uses certificates for call processing control IPsec IKE communication with gateways. For example, GWC-1. MG9KVMG - MG 9000 virtual media gateway uses certificates for call processing control IPsec IKE communication with the gateway controller. For example, NE:1_9K01002-0-2 MG9KNE - MG 9000 network element uses certificates for OAM&P IPsec IKE communication with the MG 9000 Manager. For example, NE:1 (where 1 is the NE number). WEBPKPROXY - the Apache or Tomcat Certificate Manager proxy uses certificates for HTTPS connections to web browsers and servlets. For example, wnc0w0qy.us.nortel.com SSM - SSM uses certificates for OAM&P IPsec IKE communication used by the MG 9000 Manager to communicate with the MG 9000 network element. For example, SSM-1.

Action

If the log is raised on a WEBPKPROXY certificate type, do the following:

- unmanage the WEBPKPROXY certificate. For details see "Deleting a WEBPKPROXY certificate using Certificate Manager" in Nortel

Carrier VoIP IPsec Security Service Implementation Overview, NN10453-100.

- recreate and reinstall the WEBPKPROXY certificate. For details see "Create and install WEBPKPROXY certificates for all management systems" in Nortel Carrier VoIP IPsec Security Service Implementation Overview, NN10453-100.

If the log is raised on an SSM certificate type, do the following:

- unmanage the WEBPKPROXY certificate. For details see "Deleting a WEBPKPROXY certificate using Certificate Manager" in Nortel Carrier VoIP IPsec Security Service Implementation Overview, NN10453-100.
- recreate and reinstall the WEBPKPROXY certificate. For details see "Create and install WEBPKPROXY certificates for all management systems" in Nortel Carrier VoIP IPsec Security Service Implementation Overview, NN10453-100.
- revoke the SSM certificate and wait for the certificate to move to the DELIVERED state. If it does not move to the DELIVERED state within 15 minutes, contact your next level of support.

If the state of the log is clear, no action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

PKM306

The Certificate Manager generates log report PKM306. Log report PKM306 is generated to provide advance warning that a WEBPKPROXY certificate has been delivered and needs to be installed. This alarm is raised when a WEBPKPROXY certificate state changes from REPLACE to DELIVERED. The severity is major.

The log report is clear when the WEBPKPROXY certificate is installed.

Format

The format for log report PKM306 in the raise state is as follows:

```
<OFFICE> ** PKM306 MMMDD hh:mm:ss 8969 PKM Certificate installation
required
  Location: PKManager=<hostname>
  NotificationID: <NotificationID>
  State: Raise
  Category: communicationsAlarm
  Cause: unspecifiedReason
  Time: Mmm DD hh:mm:ss YYYY
  Component Id: PKManager=<hostname>
  Specific Problem: Certificate installation required soon: <device
type> <IP address>
  Description: Certificates for the identified CertMgr Proxy need to be
installed.
```

The format for log report PKM306 in the clear state is as follows:

```
<OFFICE> PKM306 MMMDD hh:mm:ss 0013 INFO PKM Certificate installation
required
  Location: PKManager=<hostname>
  NotificationID: <NotificationID>
  State: Clear
  Time: Mmm DD hh:mm:ss YYYY
  Component Id: PKManager=<hostname>
  Description: Certificates for the identified CertMgr Proxy need to be
installed.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Category	character string	Indicates the X.733/X.736-based category of the alarm.
NotificationID	integer	An integer which can be used in combination with the log name or number and component ID to uniquely identify the corresponding raise and clear logs for the alarm.
Cause	character string	Indicates the X.733/M.3100-based cause of the alarm.
Time	character string	Indicates the date/time of the alarm raise/clear.
Hostname	character string	Indicates the hostname of the Certificate Manager.
Device type	character string	Indicates the device type: WEBPKPROXY - the Apache or Tomcat Certificate Manager proxy uses certificates for HTTPS connections to web browsers and servlets. For example, wnc0w0qy.us.nortel.com

Action

At the Certificate Manager, view all WEBPKPROXY certificates and note the active date and time for the certificate which is alarmed and verify that the certificate is in a DELIVERED state. If the certificate is in a DELIVERED state, perform procedure "Installing a WEBPKPROXY certificate" to clear the PKM306 alarm in *Nortel Carrier VoIP IPSec Security Service Implementation Overview*, NN10453-100. To launch the Certificate Manager, see "Launching the Certificate Manager" in *Nortel Carrier VoIP IPSec Security Service Implementation Overview*, NN10453-100.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

QCA201

Qca.properties not available at QCA start-up, or other problems related to properties/qca.properties.

Format

The format for log report QCA201 is as follows:

```
MSH10      QCA201 MAY30 15:23:09 4853 INIT msh10ptm
Location: msh10ptm
Category: processingError
Cause: configurationOrCustomizationError
Time: May 30 15:23:09 2005
ComponentID: /opt/nortel/qca/properties/qca.properties
SpecificProblem: Missing qca.properties file.
Description: Could not read properties. QCA is starting with default
settings.
```

Selected field descriptions

The following table explains selected fields in the log report.

Event / Error	Priority/ Event Type	Description
Qca.properties not available at QCA start-up.	Warning INIT	Properties file (properties/qca.properties) not available. QCA is starting with default settings.
portNumber property not in properties/qca.properties at QCA start-up.	Warning INIT	portNumber property not in properties/qca.properties. QCA is starting with default port number of 20000
portNumber property in properties/qca.properties not in range at QCA start-up.	Warning INIT	portNumber property in properties/qca.properties not in range. QCA is starting with default port number of 20000
portNumber property in properties/qca.properties not a number at QCA start-up.	Warning INIT	portNumber property in properties/qca.properties could not be used. QCA is starting with default port number of 20000
MaxFileSize property not in properties/qca.properties.	Warning INIT	QCA is starting with default maximum file size of 1 MByte

Event / Error	Priority/ Event Type	Description
MaxFileSize property in properties/qca.properties not in range.	Warning INIT	QCA is starting with default maximum file size of 1 MByte
MaxFileSize property in properties/qca.properties not a number.	Warning INIT	MaxFileSize property in properties/qca.properties could not be used. QCA is starting with default maximum file size of 1 MByte
MaxFileTime property not in properties/qca.properties.	Warning INIT	QCA is starting with default maximum file time of 15 minutes
MaxFileTime property in properties/qca.properties not in range.	Warning INIT	QCA is starting with default maximum file time of 15 minutes
MaxFileTime property in properties/qca.properties not a number.	Warning INIT	MaxFileTime property in properties/qca.properties could not be used. QCA is starting with default maximum file time of 15 minutes
RetainFileTime property not in properties/qca.properties.	Warning INIT	QCA is starting with default retain file time of 5 days
RetainFileTime property in properties/qca.properties not in range.	Warning INIT	QCA is starting with default retain file time of 5 days
RetainFileTime property in properties/qca.properties not a number.	Warning INIT	RetainFileTime property in properties/qca.properties could not be used. QCA is starting with default retain file time of 5 days
recycleToD property not in properties/qca.properties.	Warning INIT	QCA is starting with default recycle hour of day of 0
recycleToD property in properties/qca.properties not in range.	Warning INIT	QCA is starting with default recycle hour of day of 0
recycleToD property in properties/qca.properties not a number.	Warning INIT	recycleToD property in properties/qca.properties could not be used. QCA is starting with default recycle hour of day of 0
fileExt property not in properties/qca.properties.	Warning INIT	QCA is starting with default file extension of xml

Event / Error	Priority/ Event Type	Description
oldFileCompression property not in properties/qca.properties.	Warning INIT	QCA is starting with default value of true
oldFileCompression property in properties/qca.properties not true or false.	Warning INIT	oldFileCompression property in properties/qca.properties could not be used. QCA is starting with default value of true
closedFileCompression property not in properties/qca.properties.	Warning INIT	QCA is starting with default value of true
closedFileCompression property in properties/qca.properties not true or false.	Warning INIT	closedFileCompression property in properties/qca.properties could not be used. QCA is starting with default value of true
nodeName property not in properties/qca.properties.	Warning INIT	QCA is starting with default value of QCA

Action

None. The QCA uses the default value.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

QCA202

Old file retention directory (today-x) is being removed, OR file found in active directory when QCA started.

Format

The format for log report QCA202 is as follows:

```
MSH10      QCA202 JUN10 14:42:55 8808 INIT msh10ptm
            Location: msh10ptm
            Category: processingError
            Cause: thresholdCrossed
            Time: Jun 10 14:42:55 2005
            ComponentID: /data/qca/20000/output/today-1
            SpecificProblem: retainFileTime limit (1 days) crossed.
            Description: Removing closed file retention directory:today-1 as it
                        is older than 1 days.
```

Selected field descriptions

The following table explains selected fields in the log report.

Event / Error	Priority/ Event type	Description
old file retention directory (today-x) is being removed.	None/INIT	File Recovery: removing closed file retention directory: <i>directory</i> as it is older than x days.
File found in active directory when QCA started.	None/INIT	File Recovery: file <i>file name</i> found in active directory. This could indicate that the QCA failed. Please check debug logs.

Action

None. The QCA uses the default value.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

QCA203

QCA cannot be stopped due to several possible reasons. Examples: the qca.properties file may be missing, the system cannot determine the QCA port number, QCA is not running on specified port, an out-of-range port number is specified, or similar issues.

Format

The format for log report QCA203 is as follows:

```
MSH10      QCA203 JUN10 12:22:43 8628 INIT msh10ptm
Location: msh10ptm
Category: processingError
Cause: configurationOrCustomizationError
Time: Jun 10 12:22:43 2005
ComponentID: /opt/nortel/qca/properties/qca.properties
SpecificProblem: Missing qca.properties file.
Description: Could not read properties.  QCA cannot be stopped.
Action: Restore qca.properties file.
```

Selected field descriptions

The following table explains selected fields in the log report:

Event/Error	Priority/ Event Type	Descriptions
QCA cannot be stopped	None INIT	QCA not running on specified port. Cannot stop QCA. Use query_qca command to determine the port QCA is running on and make sure it matches with portNumber in qca.properties file. Missing qca.properties file. Could not read properties. QCA cannot be stopped. Attribute portNumber missing from qca.properties while trying to stop QCA. Cannot determine QCA port number to stop QCA.

Event/Error	Priority/ Event Type	Descriptions
QCA cannot be stopped	None INIT	Incorrect portNumber specified in qca.properties. Cannot determine QCA port number to stop QCA. Use query_qca command to determine the port QCA is running on. Make sure it matches with portNumber in qca.properties file. Out of Range QCA Port number specified. Cannot determine QCA port number to stop QCA. Use query_qca command to determine the port QCA is running on. Make sure it matches with portNumber in qca.properties file

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

QCA300

File handler or server socket could not be started.

Format

The format for log report QCA300 is as follows:

```
MSH10      QCA300 JUN10 12:44:39 8730 FAIL msh10ptm
Location: msh10ptm
Category: processingError
Cause: communicationsSubsystemFailure
Time: Jun 10 12:44:39 2005
SpecificProblem: Socket creation error.
Description: QCA not started: <exception error message>
```

Selected field descriptions

The following table explains selected fields in the log report:

Event/Error	Priority/ Event Type	Descriptions
File handler or server socket could not be started.	None FAIL	QCA not started: Could not open server socket QCA not started: Could not create File Handler.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

QCA301

QoS record received with unsupported length or unsupported version.

Format

The format for log report QCA301 is as follows:

```
MSH10      *   QCA301 JUN10 18:14:47 9275 FLT   msh10ptm
Location: msh10ptm
NotificationID: 9
State: Raise
Category: Processing Error
Cause: corruptData
Time: Jun 10 18:14:47 2005
ComponentID: GWC99
SpecificProblem: The QCA has received records with
1 length errors from the source.
Description: If 10 (or more) records with unsupported
length are received consecutively, Major fault log is
generated and the connection is closed.
```

Selected field descriptions

The following table explains selected fields in the log report:

Events/Error	Priority/ Event Type	Description
QoS Record received with Unsupported Length. (Notification Id: 9)	Minor FLT	The QCA has received records with < numberOfLengthErrors> length errors from the source. If 10 (or more) records with unsupported length are received consecutively, Major fault log is generated and the connection is closed.
10 sequential QoS Records received with Unsupported Length.	Major FLT	10 unsupported length records received. The connection to the client will be closed.

Events/Error	Priority/ Event Type	Description
QoS Record received with Unsupported Version. (Notification Id: 57)	Minor FLT	The QCA has received records with <NumberOfVersionErrors> version errors from the source. If 10 (or more) records with unsupported version are received consecutively, Major fault log is generated and the connection is closed.
10 sequential QoS Records received with Unsupported Version	Major FLT	10 unsupported version records received.The connection to the client will be closed.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

QCA302

Out of sequence QoS record received, OR problem processing binary QoS record.

Format

The format for log report QCA302 is as follows:

```
MSH10      QCA302 JUN10 18:13:53 9259 FLT  msh10ptm
Location: msh10ptm
Category: processingError
Cause: informationOutOfSequence
Time: Jun 10 18:13:53 2005
ComponentID: GWC-99
SpecificProblem: Unexpected Record Sequence Number
Description: Out of sequence QoS record received.
Sequence Number = 4 Previous sequence number = 2
```

Selected field descriptions

The following table explains selected fields in the log report:

Event/Error	Priority/ Event Type	Description
Out of sequence QoS record received	None FLT	Out of Sequence QoS Record received.
Problem processing binary QoS record.	None FLT	Problem processing binary QoS record.:Relevant MGC is mentioned in Component ID attribute of the log.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

QCA305

Connection to client is closed OR the binary QoS Record header could not be processed.

Format

The format for log report QCA305 is as follows:

```
MSH10      QCA305 JUN10 18:08:57 9165 INFO msh10ptm
            Location: msh10ptm
            Category: communications
            Cause: communicationsSubsystemFailure
            Time: Jun 10 18:08:57 2005
            SpecificProblem: Connection closed
            Description: Client at, IP Address:
            msh10client.succession.bl. Port: 2922 closed
            connection.
```

Selected field descriptions

The following table explains selected fields in the log report:

Event/Error	Priority/ Event Type	Description
Connection closed	None ERROR	MSGTYPEERROR, Client at <IP Address> : closed connection
Connection closed	None INFO	CONNECTIONCLOSED, Client at <IP Address> : closed connection
Connection closed	None ERROR	HEADERERROR, Client at <IP Address> closed connection
Connection closed	None FLT	CONNECTION CLOSED: Error while processing QoS Record Header. Client at < IP address > local port closed connection.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

QCA310

The log reports minor, major or critical disk space issues.

Format

The format for log report QCA310 is as follows:

```
MSH10    ***  QCA310 JUN10 18:13:27 9244 TBL  msh10ptm
Location: msh10ptm
NotificationID: 49
State: Raise
Category: Processing Error
Cause: storageCapacityProblem
Time: Jun 10 18:13:27 2005ComponentID: /data/qca/
SpecificProblem: checkDiskSpace() has shown that there is less than
104857600 bytes available on the local disk.
Description: More Disk space is required immediately.
```

Selected field descriptions

The following table explains selected fields in the log report:

Event/Error	Priority/ Event Type	Description
Disk space shortage, local disk requires more free space. Disk Space is below 100Mb.	Critical TBL	Component /data/qca, checkDiskSpace() has shown that there is less than 104857600 bytes available on the local disk. More Space is required immediately

Event/Error	Priority/ Event Type	Description
Disk Space is starting to run seriously low. This means that the available space is below 500Mb.	Major TBL	Component /data/qca, checkDiskSpace() has shown that there is less than 104857600 bytes available on the local disk. More Space is required immediately.
Disk space is below the minimum threshold. Initially set at 1Gb.	Minor TBL	/data/qca. Less than 1073741824 bytes available on the local disk. Major alarm will be raised if the disk space continues to drop.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

QCA315

Generated for file writing or file access problems. For the Warning level, it means that a request to get a new file name has failed, or the QCA has failed to write the footer information to the active file while attempting to close. Other reasons, for example, might be: could not get new file to write records; file <file name> is corrupted or removed; could not write to the active file; active file exists but cannot write records to it. In some cases, QCA will shut down.

Format

The format for log report QCA315 is as follows:

```
MSH10      QCA315 JUN13 10:54:29 9552 FLT  msh10ptm
Location: msh10ptm
Category: processingError
Cause: fileError
Time: Jun 13 10:54:29 2005
ComponentID: /data/qca/20000/output/active//data/
qca/20000/output/active/QCA.QCA.QoS.2005.06.13_10.53_EDT.xml
SpecificProblem: Active file: /data/qca/20000/output/
active/QCA.QCA.QoS.2005.06.13_10.53_EDT.xmlhas been removed/deleted.
Description: Data may have been lost.  Creating new file,
and attempting to write records again.  Failure to do so will
result in QCA shutdown.
```

Selected field descriptions

The following table explains selected fields in the log report:

Event/Error	Priority/ Event Type	Description
A request to get a new file name has failed, there are either 10000 files with the same name or the new file can not be created.	Warning FLT	Unable to get an unused file name for <fileName> Please check the output directory ACTION: Output directories need to be checked.
The QCA has failed to write the footer information to the active file whilst attempting to close. The active file might have been compressed without the footer information.	Warning FLT	Cannot write the FOOTER to the active file. This file is corrupted FileName = <fileName> ACTION: Check the file and confirm that all XML tags have been closed
The active file did not exist when trying to write to it. Attempt to get new file then failed. Further failures will result in the QCA being shutdown.	None FLT	Active file <fileName> has been removed. Data may have been lost. Creating new file, and attempting to write record again. Failure to do so will result in shutdown of the QCA. ACTION: File IO problems, if problem is resolved the Major alarm will be withdrawn.
Attempting to write data to file, the active file does not exist. Try to get new file. This has failed. Sleep The thread and try and get new file again. This also failed. No file to write to, QCA will shutdown.	None FAIL	Could not get new file to write records. File <fileName> is corrupted or removed. QCA shutting down. ACTION: Check: disk space and write permissions. If all is well try starting QCA again.
The XML writer and the file all seem well, unfortunately the file cannot be accessed at in either the first or second attempt, serious problem with file IO. QCA will shutdown.	None FAIL	Could not write to the active file. Active file exists but cannot write records to it. Reason unknown. QCA shutting down ACTION: Check: disk space and write permissions. If all is well try starting QCA again.

Event/Error	Priority/ Event Type	Description
The QCA has encountered inconsistent errors when building the directory structure for old files, old files may have been deleted and directory locked. The error should never appear, as it is the last resort.	None FAIL	Cannot create directories under output directory. Cannot write records. QCA shutting down ACTION: Check: directory structure, active and old file
Attempt to rename the active file from the active directory to the today directory has failed. Serious error, but no loss of data immediately. Files can be moved by hand if required	None FLT	Could not rename active file <fileName> to file <new File Name>. Please check write permissions for the output directory ACTION: Check the directories exist and all the write permission
Could not create new active file. Data is being lost.QCA must shut down.	None FAIL	Could not get new file for writing. Critical Error: <reason>. QCA shutting down. ACTION: Check the active directory for old files and permissions.
Attempt to compress an old active file has failed.	None FLT	Could not compress file: <fileName>. File compression failed. ACTION: Check the active directory for old files and permissions.
Failed to rename directories on the Recycle_day proc. This is where all files are moved along a level and the last gets deleted.	None FLT	Could not rename director from <dirName> to <newDirName>. Check disk space and permissions. ACTION: Check disk space and permissions.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

QCA322

New GWC connection received.

Format

The format for log report QCA322 is as follows:

```
MSH10      QCA322   JUN10 18:13:53 9258 INFO msh10ptm
Location: msh10ptm
Category: communications
Time: Jun 10 18:13:53 2005
ComponentID: GWC-99
SpecificProblem: New GWC connection
Description: New connection from GWC-99. Sequence Number = 1
```

Selected field descriptions

The following table explains selected fields in the log report:

Event/Error	Priority/ Event Type	Description
New GWC connection received.	None INFO	New GWC Connection.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CSEM300

Log report CSEM300 addresses a change of format for northbound events on the log feeds of Integrated EMS (IEMS) when used in conjunction with Core Element Manager (CEM).

Log report CSEM300 acts as an envelope to contain Communication Server 2000 (CS 2000) and SuperNode Data Manager (SDM) logs. The logs in the IEMS will be encapsulated inside log report CSEM300 in the northbound NT STD and SCC2 feeds. Log report CSEM300 indicates alarm sets and alarm clears for these logs. The northbound feeds from IEMS have new fields placed in them as indicated in the example in the Format section that follows.

The CEM is an optional component that allows the user to have an active alarm list in IEMS and SDM for CS 2000. The user can suppress logs (cause them to be removed) and un-suppress logs (cause them to be included) in the incoming log stream that the CEM receives from the Core. For information about suppressing and un-suppressing logs, refer to procedure "Specifying the logs delivered from the CM to the CS 2000 Core Manager" in *CS 2000 Core Manager Configuration Management*, NN10104-511.

Format

The log report format for CSEM300 is as follows:

Note: In the following format example, log SDM308 is encapsulated inside log CSEM300.

```
comp5iems * CSEM300 FEB08 10:47:46 0515 TBL Alarm set
      Equip Id: 250Q SDM-0
      Notification Id: 0000007058
      Category: processingError
      Cause: backupFailure
      ComponentID: SDM-0
      LogKey: SDM308
      Description:
      "RTPU08AZ| |* | |SDM308|FEB08|10:47:45|8441|
      TBL| SDM Base Maintenance
      System image backup (S-Tape) must be created
      Application Configuration Change.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
LogKey	variable	Indicates the original log name of the log encapsulated inside log CSEM300.

Action

This log report requires the action associated with the log identified in the LogKey field.

Associated OM registers

This log report has OM registers associated with the log identified in the LogKey field.

Additional information

This log report has the additional information associated with the log identified in the LogKey field.

CSEM600

Log report CSEM600 addresses a change of format for northbound events on the log feeds of Integrated EMS (IEMS) when used in conjunction with Core Element Manager (CEM).

Log report CSEM600 acts as an envelope to contain Communication Server 2000 (CS 2000) and SuperNode Data Manager (SDM) logs. The logs in the IEMS will be encapsulated inside log report CSEM600 in the northbound NT STD and SCC2 feeds. Log report CSEM600 indicates INFO and unmapped logs for these logs. The northbound feeds from IEMS have new fields placed in them as indicated in the example in the Format section that follows.

The CEM is an optional component that allows the user to have an active alarm list in IEMS and SDM for CS 2000. The user can suppress logs (cause them to be removed) and un-suppress logs (cause them to be included) in the incoming log stream that the CEM receives from the Core. For information about suppressing and un-suppressing logs, refer to procedure "Specifying the logs delivered from the CM to the CS 2000 Core Manager" in *CS 2000 Core Manager Configuration Management*, NN10104-511.

Format

The log report format for CSEM600 is as follows:

Note: In the following format example, log DDMS350 is encapsulated inside log CSEM600.

```
comp5iems      CSEM600 FEB08 10:48:32 0516 INFO Log
                Equip Id: 250Q SDM-0
                Notification Id: 0000007064
                Category: processingError
                Cause: ddmsINFO
                ComponentID: SDM-0
                LogKey: DDMS350
                Description:
                "RTPU08AZ| |***| |DDMS350|FEB08|10:48:30|8449|
                FAIL| Process Status
                Process Exception
                Subsystem: ddmsdcnh
                Terminated. Process shutdown.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
LogKey	variable	Indicates the original log name of the log encapsulated inside log CSEM600.

Action

This log report requires the action associated with the log identified in the LogKey field.

Associated OM registers

This log report has OM registers associated with the log identified in the LogKey field.

Additional information

This log report has the additional information associated with the log identified in the LogKey field.

TMN301

Log Report TMN301 is generated when an application error is detected.

Format

The log report format for TMN301 is as follows:

```
May 19 15:48:17 <Machine> syslog: TMN301 <Severity>
TBL Application error
Status: Trouble raised
Location: <software_entity> <user (process id)>
Description: <description>
Action: <action>
```

Note: This example is in syslog format. Your format may differ.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Machine	Variable	Indicates the name of the machine with the problem.
Severity	Critical, Major, or Minor	Indicates the severity of the alarm.
software_entity	Variable	Indicates the location of the problem software entity.
user (process id)	Variable	Indicates the process ID number.
description	Variable	Describes the error.
action	Variable	Indicates the action to take.

Action

The action will vary, depending on the error. Refer to the log report for the specific action to take.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN302

Log Report TMN302 is generated when a system error occurs.

Format

The log report format for TMN302 is as follows:

```
May 19 15:48:17 <Machine> syslog: TMN302 <Severity>  
TBL System error  
Status: Trouble raised  
Location: <software_entity> <user (process id)>  
Description: <description>  
Action: <action>
```

Note: This example is in syslog format. Your format may differ.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Machine	Variable	Indicates the name of the machine with the problem.
Severity	Critical, Major, or Minor	Indicates the severity of the alarm.
software_entity	Variable	Indicates the location of the problem software entity.
user (process id)	Variable	Indicates the process ID number.
description	Variable	Describes the error.
action	Variable	Indicates the action to take.

Action

The action will vary, depending on the error. Refer to the log report for the specific action to take.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN303

Log Report TMN303 is generated when a communication error occurs.

Format

The log report format for TMN303 is as follows:

```
comp5iems *** TMN303 FEB14 15:48:17 4635 CBSY
Communication error
Location: Normalization Layer maint (33344)
Description: store is disconnected
Action: Check Archive Process
```

Selected field descriptions

This log report has no selected field descriptions.

Action

The action will vary, depending on the error. Refer to the log report for the specific action to take.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN304

Log Report TMN304 is generated when a connection error occurs.

Format

The log report format for TMN304 is as follows:

```
May 19 15:48:17 <Machine> syslog: TMN304 <Severity>  
TBL Connection error  
Status: Trouble raised  
Location: <software_entity> <user (process id)>  
Description: <description>  
Action: <action>
```

Note: This example is in syslog format. Your format may differ.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Machine	Variable	Indicates the name of the machine with the problem.
Severity	Critical, Major, or Minor	Indicates the severity of the alarm.
software_entity	Variable	Indicates the location of the problem software entity.
user (process id)	Variable	Indicates the process ID number.
description	Variable	Describes the error.
action	Variable	Indicates the action to take.

Action

The action will vary, depending on the error. Refer to the log report for the specific action to take.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN309

Log Report TMN309 is generated when a data server error occurs.

Format

The log report format for TMN309 is as follows:

```
May 19 15:48:17 <Machine> syslog: TMN309 <Severity>  
TBL Data Server error  
Status: Trouble raised  
Location: <software_entity> <user (process id)>  
Description: <description>  
Action: <action>
```

Note: This example is in syslog format. Your format may differ.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Machine	Variable	Indicates the name of the machine with the problem.
Severity	Critical, Major, or Minor	Indicates the severity of the alarm.
software_entity	Variable	Indicates the location of the problem software entity.
user (process id)	Variable	Indicates the process ID number.
description	Variable	Describes the error.
action	Variable	Indicates the action to take.

Action

If the problem persists, contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN311

Log Report TMN311 is generated when a fatal error occurs.

Format

The log report format for TMN311 is as follows:

```
comp5iems *** TMN311 May19 15:48:17 3090 CBSY Fatal
error
Location: Log List Server maint (28374)
Description: Connection with llClient lost
Action: check llClient
```

Selected field descriptions

This log report has no selected fields.

Action

The action will vary, depending on the error. Refer to the log report for the specific action to take.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN600

Log Report TMN600 is generated by Log Normalizer when the normalizer process is successfully started and when delrep messages are sent successfully to the SDM OSF server.

Format

The log report format for TMN600 is as follows:

```
comp5iems    TMN600 FEB14 10:58:01 0159 INFO
              Information only
              Location: DAL maint(24540)
              Description: Failure to decode OM
              tuple: group = TOPQOCPS, tuple number = 0
```

Selected field descriptions

This log report has no selected field descriptions.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN601

Log Report TMN601 is generated if the version summary file is not found, meaning that the archive is empty. It is normal for the version summary file to not be found when the archive process is started for the first time.

Format

The log report format for TMN601 is as follows:

```
May 19 15:48:17 <Machine> syslog: TMN601 NONE INFO
File IO info
Location: <software_entity> <user (process id)>
Description: <description>
```

Note: This example is in syslog format. Your format may differ.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Machine	Variable	Indicates the name of the machine.
software_entity	Variable	Indicates the location of the software entity.
user (process id)	Variable	Indicates the process ID number.
description	Variable	Describes the process or the error.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN604

Log Report TMN604 is generated to provide information about application status.

Format

The log report format for TMN604 is as follows:

```
comp5iems    TMN604 FEB14 11:30:01 2979 INFO
              Application status
              Location: rscReporter root (nodes:15368)
              Description: Connection to Process Control is
                          re-established.
```

Selected field descriptions

This log report has no selected field descriptions.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

TMN605

Log Report TMN605 is generated to provide Core restart information.

Format

The log report format for TMN605 is as follows:

```
comp5iems FEB10 16:12:47 3708 INFO Core Restart Info
Location: <software_entity> <user (process ID)>
Description: Last restart type: <type>, last restart
time :
<yyyy/mm/dd HH:MM:SS.000 A>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
type	• warm restart • cold restart • reload restart • warm swact • cold swact • norestart swact • abort swact • unknown	Indicates the type of Core restart.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AC 102

Log report AC 102 indicates the Trunk Framing settings on the connected PSTN switch do not match those provisioned on the Audiocodes Mediant 2000.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	AC/ACODE
Alarm name:	Far end LOF
Event type:	COMMUNICATION
Severity:	
Clear condition:	Far end is correctly configured for proper framing.

Format

The format for log report AC 102 is as follows:

```
Far end LOF (a.k.a., Yellow Alarm). Trunk (DS1  
Number): $1.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	String	Trunk Number of Trunk with configuration problem

Action

Ensure the configuration of the trunk frame settings on the gateway are set to match those on the PSTN switch.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

AC 105

Log report AC 105 indicates that the port on the gateway is unable to tell the trunk is in-service. At this point, the trunk will attempt to send an Alarm Indication Signal (AIS).

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	AC/ACODE
Alarm name:	Near end sending AIS
Event type:	COMMUNICATION
Severity:	
Clear condition:	Misconfiguration in the gateway is corrected.

Format

The format for log report AC 105 is as follows:

Near end sending AIS. Trunk (DS1 Number) : \$1.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	String	Trunk Number of Trunk with configuration problem.

Action

Ensure the configuration of the trunk on the PSTN switch and the configuration of the gateway trunk complement each other.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

AC 107

Log report AC 107 indicates there is a physical problem in the connectivity of the trunk to the gateway. In order to receive this alarm, the far end could be offline or disconnected.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	AC/ACODE
Alarm name:	Near end Loss Of Signal
Event type:	COMMUNICATION
Severity:	
Clear condition:	Gateway is active and PSTN connectivity is correct.

Format

The format for log report AC 107 is as follows:

Near end Loss Of Signal. Trunk (DS1 Number): \$1.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	String	Trunk Number

Action

Determine why the signal has been lost from the far end. This alarm will clear once the trunk recovers.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

AC 128

Log report AC 128 indicates the gateway is no longer responding to SNMP polling. Either SNMP is misconfigured, the gateway is network isolated, or the gateway is not operational.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	AC/ACODE
Alarm name:	Audiocodes Gateway Communications link down
Event type:	COMMUNICATION
Severity:	
Clear condition:	Gateway sends communication link up trap or the management server detects that the gateway is reachable through polling.

Format

The format for log report AC 128 is as follows:

```
IFMIB - Communications link down.
```

Selected field descriptions

This log report has no selected fields.

Action

Determine why the gateway is not responding. Log into the Web Interface to the gateway to verify communication and configuration.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

DBCM 101

Log report DBCM 101 indicates a network element has lost communication with the database. A periodic audit task on each network element instance periodically tests the communication path between itself and each online database instance. This alarm is posted when the test fails and is cleared when the test succeeds.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	DBCM/DBCOMM
Alarm name:	DBComm
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	Connection to DB established

Format

The format for log report DBCM 101 is as follows:

No connection to <db-instance>.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
db-instance	DB Instance 0 or DB Instance 1	The database instance that cannot be reached.

Action

The most probable cause for this alarm is a network connectivity problem between the server on which the network element instance resides and the server on which the database instance resides. This can result from disconnected cabling or incorrectly configured routers, firewalls, or other network equipment.

Another possible (less likely) cause is that the database instance itself has stopped running or is experiencing some serious difficulty.

Once the underlying fault in the network or database instance has been corrected the alarm will clear automatically.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

DBMN 101

Log report DBMN 101 indicates that the System Manager cannot communicate with the SNMP agent that provides the database monitoring raw data.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	DBMN/DBMON
Alarm name:	SNMP Agent Communication Failure
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	Communications with the SNMP Agent on the DB Server is established.

Format

The format for log report DBMN 101 is as follows:

SNMP Request Timeout

Selected field descriptions

This log report has no selected fields.

Action

This alarm is usually the result of a network failure that prevents communication between the System Manager and the SNMP agent running on the database server. But it can also be caused by a fault in the SNMP agent itself, e.g. the agent may have exited abnormally or may be configured to listen on the wrong address or UDP port.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

DBMN 102

Log report DBMN 102 indicates an inability of the database SNMP agent to process the requests sent by the System Manager.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	DBMN/DBMON
Alarm name:	SNMP Agent Communication Error
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	The communications issue is resolved and the Database Monitor restarted.

Format

The format for log report DBMN 102 is as follows:

```
SNMP Request Error
```

Selected field descriptions

This log report has no selected fields.

Action

Contact next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

DBMN 103

Log report DBMN 103 indicates that the operational state of the database server process is a value other than “UP”.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	DBMN/DBMON
Alarm name:	Database Server Process not operational
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	The communications issue is resolved and the Database Monitor restarted.

Format

The format for log report DBMN 103 is as follows:

The Database Server Process operational state is \$1.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	UNKNOWN, DOWN, HALTED, CONGESTED, RESTARTING	The operational state of the database server process.

Action

Contact next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

DBMN 401

Log report DBMN 401 indicates that the amount disk space used by the database is approaching its limit.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	DBMN/DBMON
Alarm name:	Disk Space Utilization Threshold
Event type:	THRESHOLD
Severity:	Minor, Major, or Critical
Clear condition:	Sustained Disk Space Utilization below the defined threshold level.

Format

The format for log report DBMN 401 is as follows:

```
Disk Space Utilization has reached or exceeded the
defined threshold level of $1%.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	1 <= n <= 100	The threshold value that was met or exceeded. There are thresholds for minor, major, and critical alarms.

Action

Contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

DBMN 425

Log report DBMN 425 indicates that the amount of disk space available for an Oracle table space is approaching its limit.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	DBMN/DBMON
Alarm name:	Oracle Tablespace Utilization Threshold
Event type:	THRESHOLD
Severity:	Minor, Major, or Critical
Clear condition:	Sustained Tablespace Utilization below the defined threshold level.

Format

The format for log report DBMN 425 is as follows:

```
The defined threshold level of $1% is exceeded for
Tablespace [ $2 ].
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	1 <= n <= 100	Threshold value for the alarm.
\$2	varies	Tablespace name

Action

Contact next level of support.

Associated OM registers

OM Group OracleTableSpaceStats records table space utilization.

Additional information

None

DBMN 727

Log report DBMN 727 indicates that the database replication system encountered an error that prevents it from keeping the primary and secondary databases in sync.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	DBMN/DBMON
Alarm name:	Oracle Replication Link Errors
Event type:	ABNORMAL
Severity:	Major
Clear condition:	The link errors are resolved.

Format

The format for log report DBMN 727 is as follows:

```
Conflicts or incorrectly formed transactions have  
caused $1 errors on link [ $2 ]
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	number	number of errors
\$2	varies	replication link name

Action

Contact next level of support if the problem persists.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

DBMN 728

Log report DBMN 728 indicates that the persistence job that keeps the primary and secondary databases in sync is no longer running.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	DBMN/DBMON
Alarm name:	Oracle Broken Job
Event type:	ABNORMAL
Severity:	Minor
Clear condition:	Resolve the issue and reschedule the job.

Format

The format for log report DBMN 728 is as follows:

The job [\$1] is broken.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	varies	The persistence job name.

Action

Contact next level of support if the problem persists.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

DBMN 826

Log report DBMN 826 indicates that the replication queue between the primary and secondary database instances is not being serviced.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	DBMN/DBMON
Alarm name:	Oracle Replication Link Deferred Transactions
Event type:	ADMINISTRATIVE
Severity:	Major
Clear condition:	Reduction in the size of the replication queue for this link as transactions are processed.

Format

The format for log report DBMN 826 is as follows:

```
The replication queue for link [ $1 ] is not being serviced. The queue size is [ $2 ].
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	varies	Replication link name
\$2	number	The size of the replication queue

Action

Contact next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

EPMTC 401

Log report EPMTC 401 indicates the configured percentage of unreachable static clients has been reached. This alarm is raised on the Session Manager.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	EMTC/EPMTC
Alarm name:	Unreachable Static Clients
Event type:	THRESHOLD
Severity:	Warning
Clear condition:	Manual acknowledgement of the alarm by the craftsperson. If no manual acknowledgement has occurred, the start of the next audit will clear the raised alarm.

Format

The format for log report EPMTC 401 is as follows:

```
The number of unreachable static clients has exceeded
the configured percentage of [X] % ... currently
there are [Y] unreachable clients.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
[X]	Integer	The configured percentage of unreachable static clients when the alarm will be raised.
[Y]	Integer	The number of unreachable static clients.

Action

Service the affected subscribers. Make sure the subscribers' clients are connected and registered.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

FTP 703

Log report FTP 703 indicates the FTP operation of OAM records to the OSS destination failed due to the error encountered in creating directory on the base directory configured.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	FTP/FTP
Alarm name:	Invalid FTP Directory
Event type:	ABNORMAL
Severity:	Major
Clear condition:	When the next FTP operation is successful.

Format

The format for log report FTP 703 is as follows:

```
The FTP directory is invalid. <directory>. Stream:
<stream-name>, System: <system-name>.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
directory	String	The destination directory in which the FTP operation failed.
stream-name	For recording stream of a network element instance: <network-element-short-name>_<network element instance_number>. Example: AM1_0. For monitor element: the short name of the monitor element. Example: MAS1	The identity of the recording stream.
system-name	one of "log", "acct", or "om"	The system name of the recording stream.

Action

Check the permission of making new directory under the base directory and userid configured.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

FTP 704

Log report FTP 704 indicates the FTP operation of OAM Record to the OSS destination failed with an error message.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	FTP/FTP
Alarm name:	FTP Error
Event type:	ABNORMAL
Severity:	Major
Clear condition:	When the next FTP operation is successful.

Format

The format for log report FTP 704 is as follows:

The File Transport operation receive the following message: <msg> for host: <host-name> and file: <file-name>. Stream: <stream-name>, System: <system-name>.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
msg	String	Message received from the FTP destination
Host-name	String	Host name of the FTP Destination
File-name	String	Name of file that is transferring.

Field	Value	Description
Stream-name	For recording stream of a network element instance: <network-element-short-name>_<network element instance_number>. Example: AM1_0. For monitor element: the short name of the monitor element. Example: MAS1	The identity of the recording stream
System-name	one of “log”, “acct”, or “om”	The system name of the recording stream.

Action

Check the condition of the FTP server. If no error found, contact the next level of support if problem persists.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

FTP 706

Log report FTP 706 indicates the FTP operation of OAM records failed because of failure of login for the userid and password configured.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	FTP/FTP
Alarm name:	FTP Login Error
Event type:	ABNORMAL
Severity:	Major
Clear condition:	When the next FTP operation is successful.

Format

The format for log report FTP 706 is as follows:

```
Failed to establish or login to FTP session for host :  
<Host-name> and user: <User-id>. Stream:  
<Stream-name>, System: <System-name>.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Host-name	String	The host name of the FTP destination
User-id	String	User id used for logging on to the FTP destination

Field	Value	Description
Stream-name	For recording stream of a network element instance: <network-element-short-name>_<network element instance_number>. Example: AM1_0. For monitor element: the short name of the monitor element. Example: MAS1	The identity of the recording stream
System-name	one of “log”, “acct”, or “om”	The system name of the recording stream.

Action

Check the validity of userid and password configured. Contact next level of support if userid and password are valid and problem persists.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

IMDB 700

Log report IMDB 700 indicates an internal cache in the network element (NE) has failed to load its data from the database during system initialization.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	IMDB/IMDB
Alarm name:	IMDB_Init
Event type:	ABNORMAL
Severity:	Critical
Clear condition:	Table information loaded.

Format

The format for log report IMDB 700 is as follows:

Initial load failed: \$1

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	IMDB Table Name	An internal table to the NE that is kept in memory storing cached information from the database.

Action

This alarm occurs when data fails to be loaded from the database during NE initialization. Typically this is due to failure to communicate with the database. In such instances, the system tries to recover on the next audit cycle (approximately ten seconds). If persistent, the NE may need to be rebooted to clear the condition, and/or the connection to the database may require maintenance.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

IMDB 701

Log report IMDB 701 indicates an internal cache in the network element (NE) has failed to synchronize its data with the database during regular system operation.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	IMDB/IMDB
Alarm name:	IMDB_Resync
Event type:	ABNORMAL
Severity:	Major
Clear condition:	Table information synced.

Format

The format for log report IMDB 701 is as follows:

```
Resync with DB failed: $1
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	IMDB Table Name	An internal table to the NE that is kept in memory storing cached information from the database.

Action

This alarm occurs when data fails to be resynchronized with the database during NE initialization. Typically this is due to failure to communicate with the database. In such instances, the system tries to recover on the next audit cycle (approximately ten seconds). If persistent, the NE may need to be rebooted to clear the condition, and/or the connection to the database may require maintenance.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

IMDB 702

Log report IMDB 702 indicates an internal table of the network element (NE) that is kept in memory has reached or is nearing its capacity.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	IMDB/IMDB
Alarm name:	IMDB_Capacity
Event type:	ABNORMAL
Severity:	Minor (70-80%), Major (80-90%), Critical (90%+). All alarms have 2% hysteresis.
Clear condition:	Table utilization reduced.

Format

The format for log report IMDB 702 is as follows:

Table \$1 at or nearing capacity.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	IMDB Table Name	An internal table to the NE that is kept in memory storing cached information from the database or dynamically generated information.

Action

Check configuration parameters to verify that system resources are being utilized at expected levels.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

KCRE 201

Log report KCRE 201 indicates a license key code resource owner is unable to update the resource management tables with its new key code limit from a newly applied license key.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	KCRE/KCRES
Alarm name:	Resource Management License Key Update Failure
Event type:	RESOURCE_AVAILABILITY
Severity:	Major
Clear condition:	Resource management updated with new license key limit.

Format

The format for log report KCRE 201 is as follows:

```
unable to update resource management with new license
key limit. Resource: "<res>". License Key Limit:
<lk_lim>.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
res	String 1 – 64 characters long	Name of the resource
lk_lim	Number from 1 - 9223372036854775807	Resource limit from new license key for the keycode associated with the resource <res>.

Action

Fix underlying problem and update license key again.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

LKEY 470

Log report LKEY 470 indicates the license key limit for a resource has reached or exceeded thresholds licensable limits.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	LKEY/LKEYSYS
Alarm name:	LKEY_RESOURCE
Event type:	THRESHOLD
Severity:	Critical, Major depending on the threshold crossed
Clear condition:	When resource usage is reduced.

Format

The format for log report LKEY 470 is as follows:

```
<Keycode Name> Limit: <Keycode Limit>, Usage:  
<Keycode Usage>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Keycode Name	String	A licensable resource
Keycode Limit	Integer	Units licensed
Keycode Usage	Integer	Licensable resource usage

Action

Update license key to support more resources or reduce resource usage.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

LKEY 750

Log report LKEY 750 indicates the System Manager is not able to retrieve the license key from the database.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	LKEY/LKEYSYS
Alarm name:	700_LKEY_ERROR_CRITICAL
Event type:	ABNORMAL
Severity:	Critical
Clear condition:	When database is available.

Format

The format for log report LKEY 750 is as follows:

```
License key problem detected: Could not retrieve  
license key.
```

Selected field descriptions

This log report has no selected fields.

Action

Ensure that the System Manager can establish connectivity to the primary database. Ensure that the System Manager is configured to communicate with the correct database.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

LKEY 751

Log report LKEY 751 indicates that the license key file could not be decrypted. This can be caused by: an invalid license key file, incompatible version of the license key file, or a corrupt license key file.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	LKEY/LKEYSYS
Alarm name:	LKEY_DECRYPTPTION_FAILED_CRITICAL
Event type:	ABNORMAL
Severity:	Critical
Clear condition:	When valid license key is installed.

Format

The format for log report LKEY 751 is as follows:

```
License key problem detected: License key decryption
failed.
```

Selected field descriptions

This log report has no selected fields.

Action

Ensure that the license key is intended for the target system. Ensure that the license key file is not corrupted. Otherwise contact support team and provide them with the header information located in the license key file.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

LKEY 752

Log report LKEY 752 indicates an error occurred during validation of the license key.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	LKEY/LKEYSYS
Alarm name:	LKEY_KEYCODE_752_CRITICAL_752
Event type:	ABNORMAL
Severity:	Critical
Clear condition:	When valid license key is installed.

Format

The format for log report LKEY 752 is as follows:

```
License key problem detected: License key keycode  
creation failed.
```

Selected field descriptions

This log report has no selected fields.

Action

Ensure that the license key is intended for the target system software version. Otherwise contact support team and provide them with the header information located in the license key file.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

LKEY 753

Log report LKEY 753 indicates an error occurred during validation of the license key file. This alarm is generated when a license key has keycodes that are not compatible with the installed software.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	LKEY/LKEYSYS
Alarm name:	LKEY_PARSER_ERROR_CRITICAL_753
Event type:	ABNORMAL
Severity:	Critical
Clear condition:	When valid license key is installed.

Format

The format for log report LKEY 753 is as follows:

```
License key problem detected: License key parser
failed.
```

Selected field descriptions

This log report has no selected fields.

Action

Ensure that the license key file being entering via the System Manager is a valid license key. Otherwise contact support team and provide them with the header information located in the first lines of the license key file.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

LKEY 754

Log report LKEY 754 indicates an error occurred validating the license key file against the target system hardware.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	LKEY/LKEYSYS
Alarm name:	LKEY_HARDWARE_MISMATCH_ERROR_CRITICAL_754
Event type:	ABNORMAL
Severity:	Critical
Clear condition:	When valid license key is installed.

Format

The format for log report LKEY 754 is as follows:

```
License key problem detected: License key does not  
match hardware.
```

Selected field descriptions

This log report has no selected fields.

Action

Ensure that the license key is intended for the target system. Ensure that the license key file is not corrupted. Otherwise contact support team and provide them with the header information located in the license key file.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

LKEY 755

Log report LKEY 755 indicates that the license key upgrade failed because the supplied license key was intended for a system with a newer software release. The supplied license key is not compatible with the target system installed software.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	LKEY/LKEYSYS
Alarm name:	LKEY_SOFTWARE_MISMATCH_ERROR_CRITICAL_755
Event type:	ABNORMAL
Severity:	Critical
Clear condition:	When valid license key is installed.

Format

The format for log report LKEY 755 is as follows:

```
License key problem detected: License key not  
compatiable with installed software version.
```

Selected field descriptions

This log report has no selected fields.

Action

Upgrade target system software release or contact support team to obtain a valid license key file.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

LOADS 801

Log report LOADS 801 indicates a new load becomes available in the loads directory (`/var/mcp/loads`). This alarm is manually clearable.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	LOAD/LOADS
Alarm name:	Load(s) Available
Event type:	ADMINISTRATIVE
Severity:	Minor
Clear condition:	None. Acknowledge/Clear alarm and deploy new load if appropriate.

Format

The format for log report LOADS 801 is as follows:

New Load(s) Available: <new load names>
Other Load(s) Available: <existing load names>

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
new load names	variable-length string	Names all new loads added to the loads directory.
<existing load names>	variable-length string	Names all existing loads in the loads directory (not including the new loads).

Action

Acknowledge/Clear the alarm and deploy a new load if appropriate.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

MAS 102

Log report MAS 102 indicates the MAS Provisioning Manager is unable to communicate with the database. The MAS Prov Manager keeps on trying to connect to the database at regular intervals and clears the alarm when it is able to communicate with the database.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	MAS/MEDAPSVR
Alarm name:	Database Communication Error
Event type:	COMMUNICATION
Severity:	CRITICAL
Clear condition:	Alarm is cleared when the database connection is re-established.

Format

The format for log report MAS 102 is as follows:

Media Application Server (MAS) Provisioning Manager cannot communicate with database. If there are any pending transactions in the database, those may not be processed correctly. As a result, subscriber data on MAS may not be current.

Selected field descriptions

This log report has no selected fields.

Action

Ensure that there is network connectivity between the web server and the database. Ensure that the database is up and running. If no problem is found then contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

MAS 103

Log report MAS 103 indicates the MAS Provisioning Manager is unable to communicate with one of the Media Application Server(s) configured in the system. The MAS Prov Manager keeps on trying to connect to the MAS with which it lost the connection and clears the alarm when the connection is restored.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	MAS/MEDAPSVR
Alarm name:	Media Application Server Unreachable
Event type:	COMMUNICATION
Severity:	CRITICAL
Clear condition:	Alarm is cleared when the connection with Media Application Server is re-established.

Format

The format for log report MAS 103 is as follows:

```
The connection with Media Application Server has been
lost. As a result, subscriber data on the MAS may not
be current. Details of the MAS and the affected
domains are as follows: $1.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	IP Address, list of domains and the pooled entities having that MAS as one of the routes.	IP address of the MAS, domain and the pooled entity for which that MAS has been configured.

Action

Ensure that there is network connectivity between the web server and the MAS with which the connection was lost. Ensure that the MAS is up and running. If no problem is found then contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

MAS 504

Log report MAS 504 indicates the number of pending transactions in the database exceeds 100,000. These transactions correspond to the subscriber information that needs to be updated on the corresponding Media Application Server (MAS). This alarm indicates that the subscriber information on the MAS is no up to date. The transactions are processed periodically by the MAS Provisioning Manager and the alarm is cleared when the number of pending transactions falls below the upper threshold.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	MAS/MEDAPSVR
Alarm name:	Pending Transactions Table Size Exceeded Error
Event type:	THRESHOLD
Severity:	Warning
Clear condition:	Alarm is cleared when the pending transactions are processed successfully and deleted from the pending transactions table.

Format

The format for log report MAS 504 is as follows:

The number of pending transactions corresponding to the subscriber data stored on the Media Application Server (MAS) has exceeded the upper threshold. The subscriber data on MAS may not be current. The number of pending transactions are {\$1}.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	A numeric value greater than 100,000 indicating the number of pending transactions in the database when the alarm is raised.	Number of pending transactions in the database.

Action

Ensure that network connectivity between all the Media Application Server(s) and the web server is there. Ensure that all the MAS configured in the system are up and running. Ensure that there are no other MAS provisioning alarms in the system. If no problem is found, then contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

MAS 701

Log report MAS 701 indicates an error was encountered during the initialization of the MAS Provisioning Manager. Web server restart is required to clear this alarm.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	MAS/MEDAPSVR
Alarm name:	MAS Prov Manager Initialization Error
Event type:	ABNORMAL
Severity:	CRITICAL
Clear condition:	If the problem is fixed, alarm will be cleared upon the next restart of the web server.

Format

The format for log report MAS 701 is as follows:

```
A Media Application Server (MAS) Provisioning Manager
initialization error has occurred. Provisioning
changes affecting subscribers with MAS services will
not be reflected on the associated MAS.
```

Selected field descriptions

This log report has no selected fields.

Action

Contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

MAS 705

Log report MAS 705 indicates more than two Media Application Servers have been found for a given pooled entity configured in the system. This alarm is automatically cleared when an active MAS is changed to Inactive state or the pooled entity configuration is changed to have only 2 active MAS.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	MAS/MEDAPSVR
Alarm name:	Pooled Entity Configuration Error
Event type:	ABNORMAL
Severity:	Minor
Clear condition:	Alarm is cleared when pooled entity configuration is updated to valid values.

Format

The format for log report MAS 705 is as follows:

```
A configuration error has been detected for the
following pooled entity.
Details are as follows: $1
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Text describing the domain and the pooled entity for which more than 2 active MAS have been configured.	Name of the Pooled Entity and the Domain it belongs to.

Action

Verify that only 2 Active Media Application Servers have been provisioned for a pooled entity. Failing that, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

NCAS 101

Log report NCAS 101 indicates the NCAS link to the CS2K Core has been disconnected.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	NCAS/NCAS
Alarm name:	NCAS
Event type:	COMM
Severity:	Minor
Clear condition:	Connection to 2K Core established.

Format

The format for log report NCAS 101 is as follows:

NCAS Link to [X] disconnected.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
[X]	IP Address	IP address of the CS2K Core

Action

Verify network connectivity between the System Manager and the CS2K Core. Ensure Scplite is able to bring up an SCTP connection to the CS2K Core. Ensure the CS2K Core is available and accepting SCTP client connections.

Associated OM registers

NCAS OM group.

Additional information

None

NECM 101

Log report NECM 101 indicates the System Manager is unable to communicate with an online network element (NE) instance.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	NECM/NECOMM
Alarm name:	NEComm
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	Connection to NE instance established.

Format

The format for log report NECM 101 is as follows:

Connection to <NE_Instance> down.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
NE_Instance	<NE short name>_<inst.ID>	The identity of the NE instance with which the System Manager cannot communicate.

Action

Check network connectivity between the servers running the System Manager and the indicated NE instance.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

NECM 102

Log report NECM 102 indicates that the Fault/Performance Manager (FPM) that is configured to manage network element (NE) has no running instance.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	NECM/NECOMM
Alarm name:	NEComm
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	The FPM instance becomes active.

Format

The format for log report NECM 102 is as follows:

The FPM, <fpm_name>, has no active instance. All elements that are managed by this FPM would not be able to report logs, alarms and OMs.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Fpm_name	String	The identity of the Fault/Performance Manager

Action

Check the operational status of the NE instance of the Fault/Performance Manager. Check network connectivity between the servers running the System Manager and the indicated NE instance.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

NED 101

Log report NED 101 indicates the local communication between a managed network element instance (NEI) and the network element daemon (NED) on the NEI's server is lost. Normally, this happens because the NED process has exited.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	NED/NEDMN
Alarm name:	NED Communication Down
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	NED communication reestablished.

Format

The format for log report NED 101 is as follows:

```
Local communication with NED (Network Element Daemon)
lost. This normally indicates NED has died, in which
case it should automatically be restarted.
```

Selected field descriptions

This log report has no selected fields.

Action

This alarm normally indicates NED has died, in which case it should shortly be restarted by the "init" process. This will re-establish communication and the alarm will clear. If the problem persists, contact next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

NIF 100

Log report NIF 100 indicates a network element instance configured with a floating IP address is unable to send a gratuitous ARP to associate the IP address with a logical interface.

The <subsystem> generates log report <log report>...

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	NIF/NETIFACE
Alarm name:	Gratuitous ARP failed
Event type:	RESOURCE_AVAILABILITY
Severity:	Major
Clear condition:	Gratuitous ARP sent.

Format

The format for log report NIF 100 is as follows:

```
Failed to send gratuitous ARP for floating logical
interface.
```

```
Interface <ifaceName>
IP Address: <ipAddress>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
ifaceName	String	Name of the floating interface
ipAddress	Dotted IP Address	IP address of floating interface

Action

Ensure the ethernet cards are connected to the network. If not, reconnect them. If so and if problem persists over restarts, contact next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

NIF 200

Log report NIF 200 indicates a network element instance in a fault tolerant configuration is, during activation, unable to "up" a logical interface associated with the configured floating IP Address.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	NIF/NETIFACE
Alarm name:	Floating IP Address not up.
Event type:	RESOURCE_AVAILABILITY
Severity:	Major
Clear condition:	Network interface functional.

Format

The format for log report NIF 200 is as follows:

```
Logical interface for floating IP Address is not up.  
Floating logical IP Address: <ipAddress>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
ipAddress	Dotted IP Address	IP address of floating interface owned by active instance

Action

If problem persists over restarts, contact next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

NIF 201

Log report NIF 201 indicates a failure in a network interface card, preventing any packets from being sent on it.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	NIF/NETIFACE
Alarm name:	Network interface failed.
Event type:	RESOURCE_AVAILABILITY
Severity:	Critical
Clear condition:	Network interface running.

Format

The format for log report NIF 201 is as follows:

```
Network interface failed.  
Name: <ifaceName>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
ifaceName	String	Name of the failed network interface

Action

Ensure the card is connected to the network. If not, reconnect it. If so, contact next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

OLC 401

Log report OLC 401 indicates the calls will be failing as the component has gone in overload mode.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	OVLD/OVLDCTRL
Alarm name:	Call Queue Overload Control
Event type:	THRESHOLD
Severity:	Severity depends on the level of traffic and if it exceeds the provisioned threshold values. Minor - presence notifications except to self won't be generated Major - Same as in Minor, additionally, IM will be blocked. Critical - Everything except in-session messages and new 911 originations/terminations will be blocked.
Clear condition:	Alarm will clear automatically when call load drops below configured thresholds.

Format

The format for log report OLC 401 is as follows:

```
Call Overload Control - Full Session Blocking
```

Selected field descriptions

This log report has no selected fields.

Action

The call load has gone above the threshold limits. Wait till the call load drops..

Associated OM registers

This log report has no associated OM registers.

Additional information

None

OLC 402

Log report OLC 402 indicates the database has gone into overload mode.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	OVLD/OVLDCTRL
Alarm name:	Database Overload Control
Event type:	THRESHOLD
Severity:	Minor
Clear condition:	Alarm will clear automatically when database load drops below configured thresholds.

Format

The format for log report OLC 402 is as follows:

```
DB Overload Control - Full Session Blocking
```

Selected field descriptions

This log report has no selected fields.

Action

The database has gone in overload mode. Wait till the load drops.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

OLC 403

Log report OLC 403 indicates the memory is exhausted.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	OVLD/OVLDCTRL
Alarm name:	Memory Overload Control
Event type:	THRESHOLD
Severity:	Major
Clear condition:	Alarm will clear automatically when memory usage drops below configured thresholds.

Format

The format for log report OLC 403 is as follows:

```
Memory Overload Control - Full Session Blocking
```

Selected field descriptions

This log report has no selected fields.

Action

The memory is exhausted on the component. Wait till the memory usage drops.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

R6AS0

Log report R6AS0 indicates the R6AS servertype configuration item of a Session Manager is modified.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	R6AS/R6AS
Alarm name:	R6AS Configuration Modification
Event type:	ABNORMAL
Severity:	Major
Clear condition:	Session Manager restarted.

Format

The format for log report R6AS0 is as follows:

```
R6AS configuration modified while instance is not  
offline
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm can only be cleared by restarting the Session Manager which raised it.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RESM 701

Log report RESM 701 indicates the resource management partition audit raised an alarm when the resource management partition table usage values differ from the actual usage values returned from the resource owner. The alarm text will contain the resource and resource partition for the partition that has the discrepancy. Also, the value from the resource management table (Tracked Usage) and the value returned from the resource owner (Actual Usage) will be displayed. The partition audit runs upon boot up of the System Manager. If an audit raises an alarm upon any partition, it will reschedule itself to run in one hour. If no alarm is raised in during an audit, the audit will reschedule itself for the upcoming midnight hour.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RESM/RESMGMT
Alarm name:	Resource Management Partition Usage Discrepancy
Event type:	ABNORMAL
Severity:	Major
Clear condition:	Resource partition usage is back in sync with resource management.

Format

The format for log report RESM 701 is as follows:

```
Resource partition usage out of sync with resource  
management. Resource: "<res>" Partition: "<part>".  
Tracked Usage: <trk_usg>. Actual usage: <act_usg>.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
res	String 1 – 64 characters long	Name of the resource
part	String 1 – 64 characters long	Name of the partition

Field	Value	Description
trk_usg	Number from 1 - 9223372036854775807	Value that resource management had for the partition usage at the time the audit ran.
act_usg	Number from 1 - 9223372036854775807	Value that resource owner returned for the partition usage at the time the audit ran.

Action

Contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RESM 702

Log report RESM 702 indicates the resource management partition audit raised an alarm when the resource management partition table usage percentage are above the alarm thresholds. The partition audit will alarm partitions based on the following criteria:

- Partition Size = 0
No alarms
- Partition Size = 1-10
Critical Alarm at 100%
- Partition Size 11- 9223372036854775807
Minor Alarm from 80%-89%
Major Alarm from 90%-99%
Critical Alarm at 100%

The alarm text will contain the usage percentage at the time the audit was run as well as the resource name and resource partition name for the partition in question. Also, the usage value from the resource management table and the partition size will be displayed. The partition audit runs upon boot up of the System Manager. If an audit raises an alarm upon any partition, it will reschedule itself to run in one hour. If no alarm is raised in during an audit, the audit will reschedule itself for the upcoming midnight hour.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RESM/RESMGMT
Alarm name:	Resource Management Partition Threshold
Event type:	ABNORMAL
Severity:	MINOR, MAJOR, OR CRITICAL (See Explanation)
Clear condition:	Resource partition usage is below 5% of the partition size <size>.

Format

The format for log report RESM 702 is as follows:

Resource partition usage is at \$5% of the partition size. Resource: "<res>" Partition: "<part>". Usage: <usg>. Size: <size>.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
res	String 1 – 64 characters long	Name of the resource
part	String 1 – 64 characters long	Name of the partition
usg	Number from 1 - 9223372036854775807	Value that resource management had for the partition usage at the time the audit ran.
size	Number from 1 - 9223372036854775807	Value that resource management had for the partition size at the time the audit ran.

Action

Lower resource usage or increase partition size.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTA 101

Log report RTA 101 indicates that the status of the standard recording stream is down.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTA/RECTRAGT
Alarm name:	Standard Recording Stream Unavailable
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	When the connection for Standard Recording Stream is up.

Format

The format for log report RTA 101 is as follows:

```
Number of Standard Recording Stream for <system-name>  
system is Down: <number-down>/1. Stream:  
<stream-name>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
system-name	one of "log", "acct", or "om"	The system name of the recording stream.

Field	Value	Description
number-down	Either 0 or 1	Number of recording stream that is down.
stream-name	For recording stream of a network element instance: <network-element-short-name>_<network element instance_number>. Example: AM1_0. For monitor element: the short name of the monitor element. Example: MAS1	The identity of the recording stream

Action

Ensure that there is no network problem. Ensure that the element manager (FPM, SM or AM) is running.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 101

Log report RTP 101 indicates difficulties (e.g. network communication problems, software issues) are being encountered when attempting initial communication to setup the Media Blade specified by Blade Name (\$1).

Once set, this alarm condition is checked whenever the RTP Media Portal receives a request for a new connection, and when a timer activated event audits the communication channel with the Media Blades.

If communication to a Media Blade fails, or network interface carrier sense fails, then this alarm is generated.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	Blade Out Of Service On Initialization
Event type:	COMMUNICATION
Severity:	Critical
Clear condition:	The host will periodically attempt to re-establish network connectivity. When problem is resolved and network connectivity is established, or the software issue is resolved, this condition will be cleared.

Format

The format for log report RTP 101 is as follows:

```
$1 experienced the following problem: Problem  
allocating $2 ports for this blade
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	blade1-blade16	Name of the Media Blade experiencing the problem
\$2	Integer	This is the number of media ports configured for the specified Media Blade

Action

Ensure network connectivity between the host and blade, or network connectivity on its other interfaces (link LED(s) lit on blade card). Verify that the Media Blade software is running (Telnet to the suspect Media Blade).

Contact your next level of support.

Associated OM registers

RTPMPAvailableBladesMeter (Integer): Meter showing number of blades available to provide service.

Additional information

None

RTA 201

Log report RTA 201 indicates that there is an exception occurred when recording a data record into the spool directory of the network element instance.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTA/RECTRAGT
Alarm name:	RecordBlock Not Record
Event type:	RESOURCE_AVAILABILITY
Severity:	Major
Clear condition:	When the RecordBlock can be recorded.

Format

The format for log report RTA 201 is as follows:

```
Unable to record RecordBlock in $1 system, stream:
$2.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	One of "log", "om" or "acct"	The name of the recording system experiencing the problem.
\$2	For recording stream of a network element instance: <network-element-short-name>_<network element instance_number>. Example: AM1_0. For monitor element: the short name of the monitor element. Example: MAS1	The identity of the recording stream

Action

Ensure that the disk of the system is not full.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 102

Log report RTP 102 indicates an OutOfServiceAlarm. This can occur when a timer-driven event checks availability of currently configured Media Blades. If the full set of configured Media Blades are not available to provide service then this alarm is raised.

This alarm is raised with multiple severities as follows:

- Critical - the RTP Media Portal has no available Media Blades in its resource pool.
- Major - the RTP Media Portal has removed one or more, but not all, Media Blades from its available resource pool.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	Portal Out Of Service
Event type:	COMMUNICATION
Severity:	Critical (if all configured Media Blades are unavailable), Major (if some of the configured Media Blades are unavailable)
Clear condition:	The host will periodically attempt to bring Media Blade(s) into service. When all configured Media Blades are providing service, this condition will be cleared.

Format

The format for log report RTP 102 is as follows:

```
Portal has $1 out of $2 blades are out of service
```


Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Integer	The number of configured Media Blades that are not available to provide service.
\$2	Integer	The total number of configured Media Blades.

Action

Ensure network connectivity between the host and blade, or network connectivity on its other interfaces (link LED(s) lit on blade card).

Contact your next level of support..

Associated OM registers

RTPMPAvailableBladesMeter (Integer): Meter showing number of blades available to provide service.

Additional information

None

RTP 103

Log report RTP 103 indicates a timer-driven event checks the percentage of the configured media ports that are in use and then determines that the current usage level exceeds a configured threshold.

Alarm severity is based on the thresholds configured for the following parameters:

- Critical – the "Critical Port Usage Alarm Level" (Type: Percent) configuration parameter defines the onset level of the Critical alarm. The percent of port usage at which the number of ports in use (over all media blades) causes a critical alarm.
- Major – the "Major Port Usage Alarm Level" (Type: Percent) configuration parameter defines the onset level of the Major alarm. The percent of pool usage at which the number of ports in use (over all media blades) causes a major alarm.
- Minor – the "Minor Port Usage Alarm Level" (Type: Percent) configuration parameter defines the onset level of the Minor alarm. The percent of pool usage at which the number of ports in use (over all media blades) causes a minor alarm.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	Portal Port Usage
Event type:	COMMUNICATION
Severity:	Critical, Major, Minor
Clear condition:	The host will periodically query available media port resources. This condition will be cleared when the percentage of available port resources falls below the onset threshold (configurable parameters).

Format

The format for log report RTP 103 is as follows:

1% ports in use. There are \$2 available ports out of the \$3 originally allocated.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Percent	The percentage of configured media ports that are in use on this RTP Media Portal.
\$2	Integer	The number of media ports available to service new session requests.
\$3	Integer	The total number of media ports configured on the RTP Media Portal.

Action

Ensure that the configured capacity limits (the "ports" configuration parameter) provide adequate capacity to handle session load. This alarm is cleared once occupancy falls below the configured onset threshold.

Contact your next level of support.

Associated OM registers

RTPMPPortUsageMeter (Integer): Meter showing number of ports in use.

Additional information

None

RTP 104

Log report RTP 104 indicates a timer-driven event detected a failed status on one of the available host network interfaces. (Note: If both host network interfaces are failed, this alarm will not be displayed because communications with the host card will be lost).

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	Host Interface Failure
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	The host will periodically query the status of its interfaces. This condition will be cleared when both interfaces indicate an in-service status.

Format

The format for log report RTP 104 is as follows:

```
Portal host shows $1 Interface(s) is(are) down: $2
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Integer	The number of interfaces experiencing problems.
\$2	Interface Name	Listing of interfaces experiencing problems (e.g. eth0, eth1)

Action

Ensure network connectivity. Verify interfaces have a good connection to the network (link LED is lit on the host card).

Ensure that IP Failover functionality is enabled on the RTP Media Portal. Verify the host IP failover settings were properly configured during Installation and Commissioning. Verification and configuration of

these settings is performed using the "PortalConfig.pl" script on the Host.

This alarm is cleared once both host Network Interfaces exhibit no communications problems.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 106

Log report RTP 106 indicates a communications problem (e.g. network difficulties) was encountered when attempting to communicate with the Media Blade specified by Blade Name (\$1).

Once set, this alarm condition is checked whenever the RTP Media Portal receives a request for a new connection, and when a timer-driven event audits the communication channel with the Media Blades.

If communication to a Media Blade fails then this alarm is generated

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	Blade Out Of Service For Network Difficulty
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	The host will periodically attempt to re-establish communications. When communications are re-established, this condition will be cleared.

Format

The format for log report RTP 106 is as follows:

```
$1 experienced the following problem:  Communication
problem between the host and blade
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Blade1-Blade16	Blade Name

Action

Ensure network connectivity between the host and blade, or network connectivity on its other interfaces (link LED(s) lit blade card).

Contact next level of support.

Associated OM registers

RTPMPAvailableBladesMeter (Integer) - Meter showing number of blades available to provide service.

RTPMPActiveBladesMeter (Integer) - Meter showing number of blades with active connections.

Additional information

None

RTP 107

Log report RTP 107 indicates link issues (e.g. carrier sense fails) were encountered when attempting to communicate over a problem interface (specified by Interface Name \$2) on the identified Media Blade (specified by Blade Name \$1).

Once set, this alarm condition is checked periodically to determine if the issue is resolved.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	Blade Out Of Service For Public Network Difficulty
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	The host will periodically attempt to re-establish network connectivity. When network connectivity is established, this condition will be cleared.

Format

The format for log report RTP 107 is as follows:

```
$1 experienced the following problem:  $2 is showing  
a missing link carrier status
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Blade1-Blade16	Blade Name.
\$2	eth0-eth1	Interface Name

Action

Ensure network connectivity between the host and blade, or network connectivity on its other interfaces (link LED(s) lit on the blade card).

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 108

Log report RTP 108 indicates a Session Manager does not receive responses to requests made to the only available RTP Media Portal in its media resource pool.

When this condition arises, the Session Manager removes this RTP Media Portal from its resource pool. This impacts the Session Manager's ability to process calls that require a RTP Media Portal.

The condition clears when the Session Manager detects a resumption in communications with the affected RTP Media Portal – causing the Session Manager to add the RTP Media Portal back into its media resource pool.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	Lost connection with Media Portal
Event type:	COMMUNICATION
Severity:	Critical
Clear condition:	The RTP Media Portal may issue an MPCP message (e.g. MPCP response to an outstanding request), and will periodically attempt to advertise its availability (by sending MPCP RSIP messages), to the Session Manager. Either of these events will re-establish the control channel connection between the Session Manager and the RTP Media Portal and clear this alarm.

Format

The format for log report RTP 108 is as follows:

```
Communication Error : Lost connection with LAST Media  
Portal at IPAddress: $1
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Dotted IP Address	IP address for control channel messaging (MPCP) that identifies this specific RTP Media Portal.

Action

Ensure the referenced RTP Media Portal is accessible over the network and functional.

If not functional, may need to restart the Media Portal. Contact next level of support..

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 109

Log report RTP 109 indicates a Session Manager does not receive responses to requests made to an available RTP Media Portal in its media resource pool.

When this condition arises, the Session Manager removes the suspect RTP Media Portal from its resource pool. This decreases the available media resource capacity available to the Session Manager's to process calls that require a RTP Media Portal.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	Lost connection with Media Portal
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	The RTP Media Portal may issue a session message (e.g. MPCP response message), and will periodically attempt to advertise its availability to the Session Manager (by sending MPCP RSIP messages) to the Session Manager. Either of these events will re-establish the control channel connection between the Session Manager and the RTP Media Portal and clear the alarm.

Format

The format for log report RTP 109 is as follows:

```
Communication Error : Lost connection with Media  
Portal at IPAddress: $1
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Dotted IP Address	IP address for control channel messaging (MPCP) that identifies this specific RTP Media Portal.

Action

Ensure the referenced RTP Media Portal is accessible over the network and functional.

If not functional, may need to restart the RTP Media Portal. Contact next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 801

Log report RTP 801 indicates there is a change made to configuration data for an in-service RTP Media Portal.

The alarm is intended to highlight this data change has not been picked up by the in-service RTP Media Portal because the RTP Media Portal does not support live configuration updates. However; the configuration change is stored persistently so that it can be picked up by the RTP Media Portal on its next initialization. Until that time the run-time data and the persistently stored data are not synchronized.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	RTP Media Portal does NOT support Live Configuration Update
Event type:	ADMINISTRATIVE
Severity:	Minor
Clear condition:	Configuration Data change will take effect when the RTP Media Portal is reinitialized.

Format

The format for log report RTP 801 is as follows:

```
Live Update of RTP Media Portal Configuration Data is
NOT supported.
```

Selected field descriptions

This log report has no selected fields.

Action

Configuration Data change will take effect and the alarm will clear when the RTP Media Portal is reinitialized. Reinitialization can be performed in the next maintenance window through use of the following maintenance commands: Stop/Start, Restart, or Kill/Start.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 802

Log report RTP 802 indicates this RTP Media Portal is not configured correctly.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	System Property Portal.Config.BRHOME is NOT defined
Event type:	ADMINISTRATIVE
Severity:	Critical
Clear condition:	System Property Portal.Config.BRHOME is NOT defined. This property must be defined for the RTP Media Portal to operate correctly to clear this alarm.

Format

The format for log report RTP 802 is as follows:

```
System Property Portal.Config.BRHOME is NOT defined.
```

Selected field descriptions

This log report has no selected fields.

Action

The System Property Portal.Config.BRHOME must be defined for the RTP Media Portal to operate correctly.

Please contact your next level of technical support..

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 804

Log report RTP 804 indicates difficulties were encountered when attempting to initialize/configure an RTP Media Portal (e.g. RTP Media Packet Engine is not loaded, cluster configuration is incorrect, error encountered configuring Fault Tolerance HA Layer, attempting to configure a CPX8216-T based RTP Media Portal as a cluster - or a BladeCenter-T based RTP Media Portal as a non-cluster)

Once set, this alarm condition remains set until the causing condition(s) is/are rectified and the RTP Media Portal is restarted..

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	RTP Media Portal Configuration/Initialization Error
Event type:	CONFIG_OR_CUSTOMIZATION_ERROR
Severity:	Critical
Clear condition:	Correct the configuration issue and restart the RTP Media Portal.

Format

The format for log report RTP 804 is as follows:

```
An error occurred during initialization. $1. The RTP
Media Portal is NOT operational.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value.	Description
\$1	Text	Additional text describing the cause of the error condition. Example: An error occurred during initialization. An error occurred while attempting to configure the HA Layer. The RTP Media Portal is NOT operational.

Action

Verify RTP Media Portal configuration.

Contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 805

Log report RTP 805 indicates that the corresponding service node is hosting the Standby Service Instance (ready to become active in the event of a failure).

Once set, this alarm condition remains set until the corresponding blade becomes active or is shutdown.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	RTP Media Portal Blade Standby Message
Event type:	UNSPECIFIED_REASON
Severity:	WARNING
Clear condition:	This alarm is cleared when the blade becomes active.

Format

The format for log report RTP 805 is as follows:

The RTP Media Portal Blade in slot \$1 is in \$2

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value.	Description
\$1	Integer	Slot number in chassis
\$2	String	State – Standby or Standby-Sync

Action

This alarm is informational only. No corrective action is required.

Associated OM registers

This log report is associated with the following register in the HALayer OM group:

standbyInstances (Integer): Meter showing number of standby Service Instances in the Service Cluster.

Additional information

None

RTP 806

Log report RTP 806 indicates that the RTP Media Portal Cluster is in an invalid cluster configuration. The Cluster currently exists in a state different from how it is configured.

Once set, this alarm condition remains set until the cluster nodes are operational.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	HA Layer Invalid Cluster Configuration
Event type:	UNDERLYING_RESOURCE_UNAVAILABLE
Severity:	Critical
Clear condition:	This alarm will clear when all nodes are operational.

Format

The format for log report RTP 806 is as follows:

Cluster is in a \$1+\$2 configuration with \$3 node(s) shutting down and should be in a \$4+\$5 configuration

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value.	Description
\$1	Integer	Number of active nodes present in the cluster
\$2	Integer	Number of standby nodes present in the cluster
\$3	Integer	Number of nodes commanded to shutdown
\$4	Integer	Number of nodes configured to be active
\$5	Integer	Number of nodes configured to be standby

Action

Ensure all nodes within the cluster are operational. If not, you may need to restart the cluster nodes.

Associated OM registers

This log report is associated with the following register in the HALayer OM group:

activeInstances (Integer): Meter showing number of active Service Instances in the Service Cluster.

standbyInstances (Integer): Meter showing number of standby Service Instances in the Service Cluster.

Additional information

None

RTP 815

Log report RTP 815 indicates a change to “Media Portal Cluster” data using a Live Update of Media Portal Cluster Configuration Parameters Data is NOT supported.

If Media Portal Cluster Configuration Parameters Data is changed or deleted from the System Manager Console while the data is in use by any ACTIVE Media Portal(s) in the cluster then this alarm will be raised on all the RTP Media Portal NEs that are using the cluster data.

Once set, this alarm condition remains set until all RTP Media Portal NE's associated with the Service Cluster are restarted.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	RTP Media Portal does NOT support Live MPCluster Configuration
Event type:	CONFIG_OR_CUSTOMIZATION_ERROR
Severity:	Minor
Clear condition:	Restart the RTP Media Portal to clear the alarm.

Format

The format for log report RTP 815 is as follows:

```
Live Update of Media Portal Cluster Configuration  
Parameters Data is NOT supported.
```

Selected field descriptions

This log report has no selected fields.

Action

Restart the RTP Media Portal. MPCluster Configuration Data change will take effect and the alarm will clear when the Media Portal is restarted.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 816

Log report RTP 816 indicates a change to “Media Portal Cluster” data using a Live Update of Media Portal Cluster Fault Tolerance Data is NOT supported.

If Media Portal Cluster Fault Tolerance Data is changed or deleted from the System Manager Console while the data is in use by any ACTIVE Media Portal(s) in the cluster then this alarm will be raised on all the RTP Media Portal NEs that are using the cluster data.

Once set, this alarm condition remains set until all RTP Media Portal NE's associated with the Service Cluster are restarted.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	RTP Media Portal does NOT support Live MPCluster Configuration
Event type:	CONFIG_OR_CUSTOMIZATION_ERROR
Severity:	Minor
Clear condition:	Restart the RTP Media Portal to clear the alarm.

Format

The format for log report RTP 816 is as follows:

```
Live Update of Media Portal Cluster Fault Tolerance  
Data is NOT supported.
```

Selected field descriptions

This log report has no selected fields.

Action

Verify if the Media Portal Cluster Fault Tolerance data change is necessary and correct. If yes, then restart all RTP Media Portal NEs associated with this Service Cluster. If no, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 817

Log report RTP 817 indicates a change to “Media Portal Cluster” data using a Live Update of Media Portal Cluster Gateway Controllers Data is NOT supported.

If Media Portal Cluster Gateway Controllers Data is changed or deleted from the System Manager Console while the data is in use by any ACTIVE Media Portal(s) in the cluster. This alarm will be raised on all the RTP Media Portal NEs that are using the cluster data.

Once set, this alarm condition remains set until all RTP Media Portal NE's associated with the Service Cluster are restarted.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	RTP Media Portal does NOT support Live MPCluster Configuration
Event type:	CONFIG_OR_CUSTOMIZATION_ERROR
Severity:	Minor
Clear condition:	Restart the RTP Media Portal to clear the alarm.

Format

The format for log report RTP 817 is as follows:

```
Live Update of Media Portal Cluster Gateway  
Controllers Data is NOT supported.
```

Selected field descriptions

This log report has no selected fields.

Action

Verify if the MPCluster Gateway Controllers data change is necessary and correct. If yes, then restart all Media Portals in the cluster. If no, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 818

Log report RTP 818 indicates a change to “Media Portal Cluster” data using a Live Update of Media Portal Cluster Session Managers Data is NOT supported.

If Media Portal Cluster Session Managers Data is changed or deleted from the System Manager Console while the data is in use by any ACTIVE Media Portal(s) in the cluster. This alarm will be raised on all the RTP Media Portal NEs that are using the cluster data.

Once set, this alarm condition remains set until all RTP Media Portal NE's associated with the Service Cluster are restarted.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	RTP Media Portal does NOT support Live MPCluster Configuration
Event type:	CONFIG_OR_CUSTOMIZATION_ERROR
Severity:	Minor
Clear condition:	Restart the RTP Media Portal to clear the alarm.

Format

The format for log report RTP 818 is as follows:

```
Live Update of Media Portal Cluster Session Managers  
Data is NOT supported.
```

Selected field descriptions

This log report has no selected fields.

Action

Verify if the MPCluster Session Managers data change is necessary and correct. If yes, then restart all Media Portals in the cluster. If no, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 819

Log report RTP 819 indicates a change to “Media Portal Cluster” data using a Live Update of Media Portal Cluster Static Routes Data is NOT supported.

If Media Portal Cluster Static Routes Data is changed or deleted from the System Manager Console while the data is in use by any ACTIVE Media Portal(s) in the cluster. This alarm will be raised on all the RTP Media Portal NEs that are using the cluster data.

Once set, this alarm condition remains set until all RTP Media Portal NE's associated with the Service Cluster are restarted.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	RTP Media Portal does NOT support Live MPCluster Configuration
Event type:	CONFIG_OR_CUSTOMIZATION_ERROR
Severity:	Minor
Clear condition:	Restart the RTP Media Portal to clear the alarm.

Format

The format for log report RTP 819 is as follows:

```
Live Update of Media Portal Cluster Static Routes  
Data is NOT supported.
```

Selected field descriptions

This log report has no selected fields.

Action

Verify if the MPCluster Static Routes data change is necessary and correct. If yes, then restart all Media Portals in the cluster. If no, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

RTP 820

Log report RTP 820 indicates a change to “Media Portal Cluster” data using a Live Update of Media Portal Cluster Service Instances Data is NOT supported.

If Media Portal Cluster Service Instances Data is changed or deleted from the System Manager Console while the data is in use by any ACTIVE Media Portal(s) in the cluster. This alarm will be raised on all the RTP Media Portal NEs that are using the cluster data.

Once set, this alarm condition remains set until all RTP Media Portal NE's associated with the Service Cluster are restarted.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	RTPB/RTPBLADE
Alarm name:	RTP Media Portal does NOT support Live MPCluster Configuration
Event type:	CONFIG_OR_CUSTOMIZATION_ERROR
Severity:	Minor
Clear condition:	Restart the RTP Media Portal to clear the alarm.

Format

The format for log report RTP 820 is as follows:

```
Live Update of Media Portal Cluster Service Instances  
Data is NOT supported.
```

Selected field descriptions

This log report has no selected fields.

Action

Verify if the MPCluster Service Instances data change is necessary and correct. If yes, then restart all Media Portals in the cluster. If no, contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SEC 820

Log report SEC 820 indicates a certificate in the internal keystore will expire in 89 days or less. The severity of the alarm is based upon thresholds. A minor alarm is raised if the certificate will expire between 60 and 89 days. A major alarm is raised if the certificate will expire between 30 and 59 days. A critical alarm is raised if the certificate will expire in less than 30 days.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SEC/SECURITY
Alarm name:	Key Certificate Expiry
Event type:	ADMINISTRATIVE
Severity:	Minor, Major, or Critical
Clear condition:	Update the keys in the keystore on the server and restart this NEI.

Format

The format for log report SEC 820 is as follows:

```
Secure socket key certificate will expire in  
<remaining-days> days.
```

```
X509 Certificate.
```

```
Version: V<version>
```

```
Subject: <subject>
```

```
Signature Algorithm: <signature-algorithm> OID =  
<oid>
```

```
Validity: [From: <validity-from>,To: <validity-to>]
```

```
Issuer: <issuer>
```

```
Serial Number:  [<serial-number>]
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
remaining-days	0 – 89	The number of days before the certificate will expire.
version	V1	Version of the X509 Certificate
subject	CN=MCS Security, OU=Multimedia Communications Platform, O=Nortel Networks, L=Richardson, ST=TX, C=US	The subject distinguished name of the X509 Certificate.
signature-algorithm	MD5withRSA	The signature algorithm name for the certificate signature algorithm. The algorithm name is determined from the algorithm OID string.
oid	1.2.840.113549.1.1.4	The signature algorithm OID string from the certificate. An OID is represented by a set of nonnegative whole numbers separated by periods. For example, the string "1.2.840.10040.4.3" identifies the SHA-1 with DSA signature algorithm, as per RFC 2459.
validity-from	Day Time Year	The date that the validity period for the certificate begins.
validity-to	Day Time Year	The date that the validity period for the certificate ends.

Field	Value	Description
issuer	CN=MCS Security, OU=Multimedia Communications Platform	The issuer (issuer distinguished name) value from the certificate. The issuer identifies the entity that signed (and issued) the certificate. The issuer field contains an X.500 distinguished name (DN)
serial-number	1093277240	The serialNumber value from the certificate. The serial number is an integer assigned by the certification authority to each certificate. It must be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate).

Action

The certificate in question should be updated with another certificate which has a longer expiry period. After the certificates are updated, the NE instance in question has to be restarted in order for it to begin using the new certificates.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SEC 821

Log report SEC 820 indicates a certificate in the internal truststore will expire in 89 days or less. The severity of the alarm is based upon thresholds. A minor alarm is raised if the certificate will expire between 60 and 89 days. A major alarm is raised if the certificate will expire between 30 and 59 days. A critical alarm is raised if the certificate will expire in less than 30 days.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SEC/SECURITY
Alarm name:	Trusted Certificate Expiry
Event type:	ADMINISTRATIVE
Severity:	Minor, Major, or Critical
Clear condition:	Update the keys in the keystore on the server and restart this NEI.

Format

The format for log report SEC 821 is as follows:

Secure socket key certificate will expire in
<remaining-days> days.

X509 Certificate.

Version: V<version>

Subject: <subject>

Signature Algorithm: <signature-algorithm> OID =
<oid>

Validity: [From: <validity-from>,To: <validity-to>]

Issuer: <issuer>

Serial Number: [<serial-number>]

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
remaining-days	0 – 89	The number of days before the certificate will expire.
version	V1	Version of the X509 Certificate
subject	CN=MCS Security, OU=Multimedia Communications Platform, O=Nortel Networks, L=Richardson, ST=TX, C=US	The subject distinguished name of the X509 Certificate.
signature-algorithm	MD5withRSA	The signature algorithm name for the certificate signature algorithm. The algorithm name is determined from the algorithm OID string.
oid	1.2.840.113549.1.1.4	The signature algorithm OID string from the certificate. An OID is represented by a set of nonnegative whole numbers separated by periods. For example, the string "1.2.840.10040.4.3" identifies the SHA-1 with DSA signature algorithm, as per RFC 2459.
validity-from	Day Time Year	The date that the validity period for the certificate begins.
validity-to	Day Time Year	The date that the validity period for the certificate ends.

Field	Value	Description
issuer	CN=MCS Security, OU=Multimedia Communications Platform	The issuer (issuer distinguished name) value from the certificate. The issuer identifies the entity that signed (and issued) the certificate. The issuer field contains an X.500 distinguished name (DN)
serial-number	1093277240	The serialNumber value from the certificate. The serial number is an integer assigned by the certification authority to each certificate. It must be unique for each certificate issued by a given CA (i.e., the issuer name and serial number identify a unique certificate).

Action

The certificate in question should be updated with another certificate which has a longer expiry period. After the certificates are updated, the NE instance in question has to be restarted in order for it to begin using the new certificates.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SIP 401

Log report SIP 401 indicates a SIP protocol alarm for call failures. This alarm is raised on the crossing of a threshold that is defined for OM group SIP_Inbound_Response_Report. This OM group counts SIP response messages which are received in response to outgoing SIP request messages. One response message in particular, "500 Server Internal Error" is designated as the call failure indication. There are three configurable thresholds for the SIP 500 response for minor, major, and critical alarms. The thresholds specify the 500 responses as a percentage of total responses. For example, if the minor threshold is set to the value 5, a minor alarm will be raised if, in any Office Transfer Period, the number of 500 responses reaches 5% of the total responses. The thresholds are configured in the Configuration Parameters of the network element.

In OM group SIP_Inbound_Response_Report there is one 500 register (and one set of configurable thresholds) for each supported SIP request message (INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PUBLISH, REFER, REGISTER, SUBSCRIBE, and UPDATE). Threshold checking (and resulting alarm generation, modification, or clearing) are performed at the end of each Office Transfer Period. Threshold checking is performed on each transaction type independently of all others. In order to prevent erroneous alarms behavior, threshold checking is subject to a minimum transaction count. There must be at least 100 transactions for threshold checking to be performed. This means that if an alarm is raised in one Office Transfer Period and fewer than 100 transactions occur in a subsequent Office Transfer Period, the alarm will persist regardless of the number of 500 responses.

In addition to the standard alarm fields, the OM threshold alarm will contain a Response Code Dump of recently received 500 response messages, which can be used to determine the source of the 500 responses. The following is an example of a code dump:

```
Response Code [500] Dump:
Queue Depth: 20
Queue Elements: 13
[0] Sat Mar 05 14:31:50 CST 2005 (1110054710931)
***INBOUND***
Source: IPDestination
[INETADDR: <ip_address>] [PORT:5095] [TRNSPRT: UDP]
SIP/2.0 500 Server Internal Error
to: "user 1001"
<sip:9726851001@dt1.com>;tag=666777888
```

```
from: "user 1002" <sip:u1002@dt1.com>;tag=1244863008
call-id:
02746aac3a1d9280316ea896c1883d32577cea3@47.102.117.
7
cseq: 5557 INVITE
via: SIP/2.0/UDP
<ip_address>:5065;branch=z9hG4bK-2a5a2-a57030d-1ad7
fef0
```

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SIP/SIPRTCL
Alarm name:	OM threshold for SIP inbound 500 responses exceeded.
Event type:	THRESHOLD_CROSSED
Severity:	Minor, Major, Critical
Clear condition:	Cleared when the number of 500 Server Internal Error responses falls below the specified percentage for the minor threshold.

Format

The format for log report SIP 401 is as follows:

```
The number of 500 Server Internal Error responses to
SIP <transaction> requests in OM group
SIP_Inbound_Response_Report exceeds the specified
percentage of responses.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
transaction	String	The SIP transaction type for which the 500 response threshold was exceeded, which will be one of the following: INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PUBLISH, REFER, REGISTER, SUBSCRIBE, or UPDATE.

Action

Attached to each alarm report is a Response Code Dump, which contains a list of the most recently received 500 response messages. In each response message, the Source field identifies the source of the 500 response. Specifically, it contains the IP address of the network element which sent the 500 response. A 500 Server Internal Error response message is typically associated with a SWER report on the network element which sent the 500 response, and the SWER report will typically be accompanied by descriptive text indicating what corrective action should be taken. In the absence of such a descriptive text, the operator or craftperson should collect the SWER report and contact the next level of support.

Associated OM registers

SIP_Delay_Report, SIP_Outbound_Response_Report,
SIP_Transaction_Report

Additional information

None

SMCM 101

Log report SMCM 101 indicates an online network element (NE) instance cannot communicate with the System Manager.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SMCM/SMCOMM
Alarm name:	SMComm
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	Connection to System Manager established.

Format

The format for log report SMCM 101 is as follows:

```
Connection to System Manager is down.
```

Selected field descriptions

This log report has no selected fields.

Action

Check network connectivity between the servers running the NE instance and the System Manager.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SRVR 101

Log report SRVR 101 indicates the SNMP agent on the server cannot be contacted.

The Server Monitor queries the SNMP agent on the server for information such as: CPU Occupancy, partition utilization and interface utilization. This information is not available to the Server Monitor if the local agent on the server cannot be contacted.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SRVR/SERVER
Alarm name:	SNMP Agent Communication Failure
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	Communications with the SNMP Agent on the Server is established.

Format

The format for log report SRVR 101 is as follows:

```
SNMP Request Timeout
```

Selected field descriptions

This log report has no selected fields.

Action

Verify that network connectivity between the monitored server and the server running the System Manager exists.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SRVR 102

Log report SRVR 102 indicates the Server Monitor encountered unexpected error responses to the SNMP queries.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SRVR/SERVER
Alarm name:	SNMP Agent Communication Error
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	The communications issue is resolved and the Server Monitor restarted.

Format

The format for log report SRVR 102 is as follows:

```
SNMP Request Error
```

Selected field descriptions

This log report has no selected fields.

Action

Contact next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SRVR 401

Log report SRVR 401 indicates the CPU Occupancy of the monitored Server equals or exceeds the configured threshold.

The Server Monitor computes the average CPU Occupancy of the Server over a 10 second interval using information received from SNMP queries. For a Windows-based server, the average CPU Occupancy is calculated over a 1 minute interval. Finer granularity is not currently supported on a Windows platform.

The Server Monitor provides 3 configurable alarm severity levels: Minor, Major and Critical. Each level is associated with a corresponding CPU Occupancy threshold. The default values are:

- Minor: 80%
- Major: 90%
- Critical: 100%

These values may be changed at any time. A severity level may also be suppressed. The SRVR 401 alarms do not necessarily progress through each defined severity level.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SRVR/SERVER
Alarm name:	CPU Occupancy Threshold
Event type:	THRESHOLD
Severity:	Minor, Major or Critical based on CPU Occupancy threshold configuration
Clear condition:	Sustained CPU Occupancy reduction below the defined threshold level.

Format

The format for log report SRVR 401 is as follows:

CPU Occupancy has reached or exceeded the defined threshold level of <cpu-occupancy>%.

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
cpu-occupancy	10-100 in increments of 10	Configured CPU Occupancy threshold corresponding to the severity.

Action

No action required. Please contact next level of support if the problem persists.

Note that existing SRVR 401 alarms are cleared when the Server Monitor is stopped..

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SRVR 402

Log report SRVR 402 indicates the RAM Utilization of the monitored Server equals or exceeds the configured threshold.

The Server Monitor queries the Server for RAM usage information every 60 seconds. The RAM Utilization value is calculated as the 'used' RAM expressed as a percentage of the 'total' RAM.

The Server Monitor provides 3 configurable alarm severity levels: Minor, Major and Critical. Each level is associated with a corresponding RAM Utilization threshold.

RAM utilization alarms are disabled by default. This configuration may be changed at any time to enable alarms for either all or some severity levels.

The SRVR 402 alarms do not necessarily progress through each defined severity level.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SRVR/SERVER
Alarm name:	Memory Utilization Threshold
Event type:	THRESHOLD
Severity:	Minor, Major or Critical based on RAM Utilization threshold configuration
Clear condition:	Sustained Memory Utilization reduction below the defined threshold level.

Format

The format for log report SRVR 402 is as follows:

```
Memory Utilization has reached or exceeded the
defined threshold level of <ram-threshold>%.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
ram-threshold	10-100 in increments of 10	Configured RAM Utilization threshold corresponding to the severity.

Action

No action required. Please contact next level of support if the problem persists.

Note that existing SRVR 402 alarms are cleared when the Server Monitor is stopped..

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SRVR 403

Log report SRVR 403 indicates the disk space utilization for a partition on the monitored Server equals or exceeds the configured threshold.

The Server Monitor queries the Server for partition usage information every 60 seconds. The partition utilization value is calculated as the 'used' disk space expressed as a percentage of the 'total' disk space for the partition.

The Server Monitor provides 3 configurable alarm severity levels: Minor, Major and Critical. Each level is associated with a corresponding utilization threshold. The default values are:

- Minor: 80%
- Major: 90%
- Critical: 100%

These values may be changed at any time. A severity level may also be suppressed. The SRVR 403 alarms do not necessarily progress through each defined severity level.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SRVR/SERVER
Alarm name:	Partition Utilization Threshold
Event type:	THRESHOLD
Severity:	Minor, Major or Critical based on the disk partition utilization threshold configuration
Clear condition:	Sustained Partition Utilization reduction below the defined threshold level.

Format

The format for log report SRVR 403 is as follows:

```
The defined threshold level of <threshold>% is  
reached or exceeded for partition  
[<partition-name>].
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
threshold	10-100 in increments of 10	Configured partition utilization threshold corresponding to the severity.
partition-name	String	Identifies the partition.

Action

Free up disk space. Consult the next level of support before deleting files.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SRVR 404

Log report SRVR 404 indicates the interface utilization for a physical interface on the monitored Server equals or exceeds the configured threshold.

The Server Monitor queries the Server for interface statistics every 10 seconds. The interface utilization value is calculated as the utilized bandwidth over a 10 second interval expressed as a percentage of the 'total' bandwidth for the interface.

The Server Monitor provides 3 configurable alarm severity levels: Minor, Major and Critical. Each level is associated with a corresponding utilization threshold. The default values are:

- Minor: 80%
- Major: 90%
- Critical: 100%

These values may be changed at any time. A severity level may also be suppressed. The SRVR 404 alarms do not necessarily progress through each defined severity level.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SRVR/SERVER
Alarm name:	Interface Utilization Threshold
Event type:	THRESHOLD
Severity:	Minor, Major or Critical based on interface utilization threshold configuration.
Clear condition:	Sustained Interface Utilization reduction below the defined threshold level.

Format

The format for log report SRVR 404 is as follows:

```
The defined threshold level of <threshold>% is
reached or exceeded for interface [<interface-name>
].
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
threshold	10-100 in increments of 10	Configured interface utilization threshold corresponding to the severity.
interface-name	String	Identifies the interface.

Action

No action required. Please contact next level of support if the problem persists.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SVCA 801

Log report SVCA 801 indicates the service address of System Manager was changed from the Management Console.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SVCA/SMSVCADR
Alarm name:	SM Service Address Changes
Event type:	ADMIN
Severity:	Critical
Clear condition:	System Manager is redeployed.

Format

The format for log report SVCA 801 is as follows:

```
System Manager service address changed.
```

Selected field descriptions

This log report has no selected fields.

Action

If SM service address is changed, SM needs to be redeployed to take the IP Address change. If the administrator cannot login to SM from the Management Console after SM is redeployed, contact next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SYNC 200

Log report SYNC 200 indicates that the configuration data for an NE Instance is out-of-sync.

Various mechanisms are in place on the System Manager to ensure that configuration data is delivered to all NE instances in a reliable manner. If an NE instance cannot be contacted due to network connectivity issues, the System Manager journals the data for delivery when communication with the NE instance is re-established. If connectivity issues persist for long durations, it is conceivable that the journal buffers fill up to capacity

(The journal capacity is determined by engineering parameters on the System Manager). In such an event, the System Manager cannot deliver subsequent events to the NE Instance and consequently marks the NE instance out-of-sync.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SYNC/SYNC
Alarm name:	NESync
Event type:	RESOURCE_AVAILABILITY
Severity:	Major
Clear condition:	Configuration data in sync.

Format

The format for log report SYNC 200 is as follows:

```
<ne-instance>'s configuration data $2 sync.
```


Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
ne-instance	String	Identifies the NE Instance
\$2	“out-of-“ or “in-“	Prefix to the term sync. Either the Network element is out of sync or in-sync

Action

Restart the NE Instance.

Restarting a NE instance may result in service outage. It is recommended to perform any restart during an off-peak maintenance window.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SYS 101

Log report SYS 101

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SYS/SYSTEM
Alarm name:	Peer presumed failed
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	Peer network element instance activity detected.

Format

The format for log report SYS 101 is as follows:

```
Peer network element instance presumed failed.  
Peer control transport address: <peer-TA>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
peer-TA	Dotted IP Address:port	IP address and UDP port of peer instance that is presumed failed.

Action

This is a normal condition if the peer instance has been manually stopped and transitions to OFFLINE. Starting the peer or, if the was peer stopped in order to discontinue its use, removing it from the network configuration will clear the alarm.

If the peer instance is running, check the network connectivity between local and peer network elements.

If the alarm repeatedly raised/cleared, fault tolerant timer values may need to be increased to account for higher than engineered message

transit time between network elements. Content the next level of support in this case.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SYS 102

Log report SYS 102 indicates a fault tolerant Status message was received by a network element instance when no peer is provisioned for that instance.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SYS/SYSTEM
Alarm name:	Status from unprovisioned peer
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	Have not received recent status message from unknown peer instance.

Format

The format for log report SYS 102 is as follows:

```
Received status from network element peer instance  
when none is provisioned.  
Status message TransportAddress: <message-TA>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
message-TA	Dotted IP Address:port	IP Address and UDP port of source of Status message

Action

Locate the network element instance associated with the indicated transport address and determine if it is a valid peer. If not, stop the instance and reconfigure it accordingly. If so, contact the next level of support.

Note that the alarm clears automatically if no status message is received from the unknown peer within instance 60000 msec.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SYS 103

Log report SYS 103 indicates a fault tolerant Status message was received by a network element instance when from a peer whose IP address is different from that of the provisioned peer.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SYS/SYSTEM
Alarm name:	Status from unknown peer
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	Have not received recent status message from unknown peer instance.

Format

The format for log report SYS 103 is as follows:

```
Received status from unknown network element peer
instance.
```

```
    Status message TransportAddress: <message-TA>
    Provisioned peer control TransportAddress:
    <peer-TA>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
message-TA	Dotted IP Address:port	IP Address and UDP port of source of Status message
peer-TA	Dotted IP Address:port	IP Address and UDP port of provisioned peer

Action

Locate the network element instance associated with message's transport address and determine if it is a valid peer. Stop the instance and reconfigure it accordingly. If so, contact the next level of support.

Note that the alarm clears automatically if no status message is received from the unknown peer within instance 60000 msec.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SYS 104

Log report SYS 104 indicates a network element is in a fault tolerant configuration and a peer instance informs an instance that it believes it to be failed. This can happen if there is one way network failure or congestion from the instance to its peer.

This is a normal condition when an instance is started while its peer at least past the INITIALIZING phase of startup. In this case, as the instance initializes, the alarm clears when the instance begins the INITIALIZING phase of startup.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SYS/SYSTEM
Alarm name:	Peer Presumes Failure
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	Peer no longer presumes failure of this instance.

Format

The format for log report SYS 104 is as follows:

```
Peer instance presumes failure of this instance.
```

Selected field descriptions

This log report has no selected fields.

Action

This is a normal condition when an instance is started while its peer has already begun activation or is active. In this case, as the instance initializes, the alarm will clear.

If both the local and peer instance have passed initialization and the alarm persists, there is likely a one way failure or congestion in the network from the direction of the local instance to the peer instance. Verify the network between local and peer network instances and fix if necessary. If the network is functional and the alarm persists, contact the next level of support.

If the alarm repeatedly raised/cleared, fault tolerant timer values may need to be increased to account for higher than engineered message transit time between network elements. Contact the next level of support in this case..

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SYS 105

Log report SYS 105 indicates a network element instance is isolated from the network. This indicates a failure in all network interface cards connected to that network.

Note that delivery of the alarm to the Management Console and the corresponding log to the configured FPM will not be immediately possible without network connectivity. However, using "lights out management", the logs on the isolated machine can be viewed from the spool directory to verify that isolation has occurred.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SYS/SYSTEM
Alarm name:	Network Isolated
Event type:	COMMUNICATION
Severity:	Major
Clear condition:	Network connectivity detected.

Format

The format for log report SYS 105 is as follows:

```
Network isolation detected.
```

Selected field descriptions

This log report has no selected fields.

Action

Ensure the server's network interface cards are connected to the network. If so, contact the next level of support.

When network connectivity is reestablished, the network element instance will restart and the alarm will clear.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SYS 106

Log report SYS 106 indicates an unusual condition where a peer network element instance believes it is network isolated but is still able to communicate the isolation condition to the local instance. This can happen if the peer is isolated only briefly or is cycling between isolation/unisolation. In any case, the peer will restart itself.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SYS/SYSTEM
Alarm name:	Peer Network Isolated
Event type:	COMMUNICATION
Severity:	CRITICAL
Clear condition:	Network connectivity or peer failure detected.

Format

The format for log report SYS 106 is as follows:

```
Peer network isolation detected.  
  Peer control transport address: <peer-TA>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
peer-TA	Dotted IP Address:port	IP Address and UDP port of isolated peer

Action

Ensure the peer server's network interface cards are connected to the network. If so, contact the next level of support.

Note that this alarm will be cleared automatically regardless of network interface card maintenance. If the peer remains isolated, it will stop sending peer Status messages and the local instance will detect peer failure. If/when the peer becomes unisolated, it will restart itself and the local instance will detect the peer failure if it has not already done so.

In either case, this alarm will be cleared and a SYS101 alarm raised in its place.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SYS 703

Log report SYS 703 indicates a network element instance in a fault tolerant configuration when a peer instance is in the ACTIVATING phase but fails to transition to ACTIVE within the time specified by the engineering parameter "FaultTolerance:PeerActivityTransitionTimeout". This normally indicates the peer has encountered a problem and will likely not make the transition at all.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SYS/SYSTEM
Alarm name:	Peer Activating Too Long
Event type:	ABNORMAL
Severity:	Major
Clear condition:	Peer instance presumed failed.

Format

The format for log report SYS 703 is as follows:

```
Peer instance has been activating for at least
<duration> milliseconds and is thus presumed failed.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
duration	Integer > 0	Timeout, in milliseconds, for the ACTIVATING to ACTIVE transition. From the engineering parameter "FaultTolerance:PeerActivityTransition Timeout"

Action

Normal behavior is for the instance to instruct its peer to shutdown. When it does, the peer will be detected as failed and this alarm will be cleared and replaced with a SYS100 alarm.

If this alarm continues to be raised in association with activation of a specific network element instance, contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SYS 704

Log report SYS 704 indicates a network element instance in a fault tolerant configuration when a peer instance is in the DEACTIVATING phase but fails to transition to SHUTDOWN within the time specified by the engineering parameter "FaultTolerance:PeerActivityTransitionTimeout". This normally indicates the peer has encountered a problem and will likely not make the transition at all.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SYS/SYSTEM
Alarm name:	Peer Deactivating Too Long
Event type:	ABNORMAL
Severity:	Major
Clear condition:	Peer instance presumed failed.

Format

The format for log report SYS 704 is as follows:

```
Peer instance has been deactivating for at least
<duration> milliseconds and is thus presumed failed.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
duration	Integer > 0	Timeout, in milliseconds, for the DEACTIVATING to SHUTDOWN transition. From the engineering parameter "FaultTolerance:PeerActivityTransitionTimeout"

Action

Normal behavior is for the instance to instruct its peer to shutdown. When it does, the peer will be detected as failed and this alarm will be cleared and replaced with a SYS100 alarm.

If this alarm continues to be raised in association with deactivation of a specific network element instance, contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

SYS 707

Log report SYS 707 indicates a fault tolerant network element instance requested synchronization from it's peer but was rejected.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	SYS/SYSTEM
Alarm name:	Synchronization request rejected
Event type:	ABNORMAL
Severity:	Major
Clear condition:	Restart network element instance.

Format

The format for log report SYS 707 is as follows:

```
System Manager service address changed
```

Selected field descriptions

This log report has no selected fields.

Action

If problem reoccurs after restart or happens frequently, contact next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

TCF 902

Log report TCF 902 indicates a failure to create all requested TCP servers or UDP based sockets for a particular subsystem.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	TRAN/TRANSPRT
Alarm name:	Socket Configuration Error
Event type:	UNCATEGORIZED
Severity:	Critical
Clear condition:	This component's configuration must be modified and applied in order to clear this condition.

Format

The format for log report TCF 902 is as follows:

```
Allocated <createdTransports> of the  
<requestedTransports> requested transports.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
createdTransports	Integer ≥ 0	Number of successfully created TCP servers or UDP based sockets.
requestedTransports	Integer > 1	Number of requested TCP servers or UDP based sockets.

Action

Verify that IP addresses configured for the server on which the network element instance resides are correct. If so, verify that all network interfaces are properly connected to the Ethernet. Then restart the network element instance.

If problem persists over restarts, contact the next level of support..

Associated OM registers

This log report has no associated OM registers.

Additional information

None

TCF 903

Log report TCF 903 indicates a failure to create a TCP server or UDP based socket.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	TRAN/TRANSPRT
Alarm name:	Socket Allocation Error
Event type:	UNCATEGORIZED
Severity:	Critical
Clear condition:	This component's configuration must be modified and applied in order to clear this condition.

Format

The format for log report TCF 903 is as follows:

```
Could not allocate the <transportType> socket for  
<protocol>.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
transportType	String	Indicates the type of transport, for example TCP, UDP.
protocol	String	Protocol associated with the TCP server or UDP based socket.

Action

Verify that IP addresses configured for the server on which the network element instance resides are correct. If so, verify that all network interfaces are properly connected to the Ethernet. Then restart the network element instance.

If problem persists over restarts, contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

THLD 401

Log report THLD 401 indicates a generic threshold alarm provided by the OM framework. The triggers and threshold values for each alarm are defined by the specific application.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	THLD/THRSHLD
Alarm name:	AboveTHLD
Event type:	THRESHOLD
Severity:	Warning, Minor, Major, or Critical (depending on the application generating it)
Clear condition:	<OM register name> value <OM register value> is below threshold

Format

The format for log report THLD 401 is as follows:

```
<OM register name> value <OM register value> exceeds  
threshold
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OM register name	string	The name of the OM register
OM register value	integer	The value of the OM register

Action

To clear the alarm, the usage indicated by the OM will have to be reduced or the resources associated with the usage will have to be increased or resolved. In the example of closedFileCount OM, the communication channel between the network element and its FPM needs to be up so that the closed files can be sent to FPM and the closedFileCountOM can be reduced.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

THLD 402

Log report THLD 402 indicates a generic threshold alarm provided by the OM framework. The triggers and threshold values for each alarm are defined by the specific application.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	THLD/THRSULD
Alarm name:	belowTHLD
Event type:	THRESHOLD
Severity:	Warning, Minor, Major, or Critical (depending on the application generating it)
Clear condition:	<OM register name> value <OM register value> is above threshold.

Format

The format for log report THLD 402 is as follows:

```
<OM register name> value <OM register value> dropped  
below threshold
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OM register name	String	The name of the OM register
OM register value	integer	The value of the OM register

Action

To clear the alarm, the usage indicated by the OM will have to be increased or the any possible limitation associated with the usage will have to be resolved. In the example of userCount OM, any possible cause of limiting the increase of the users should be looked at.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

TSVR 700

Log report TSVR 700 indicates the failure by the session manager to connect to the terminal server provisioned in the voicemail server configuration page on the provisioning client.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	TSVR/TERMSVR
Alarm name:	TRMSVR_LOGIN
Event type:	ABNORMAL
Severity:	Critical
Clear condition:	Password and username are valid.

Format

The format for log report TSVR 700 is as follows:

```
Password or username is invalid.
```

Selected field descriptions

This log report has no selected fields.

Action

Please check on the voicemail server configuration page, that the username and password entered for the terminal server login is correct.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

TSVR 701

Log report TSVR 701 indicates that the session manager failed to connect to the terminal server on the specified address and port.

This fault raises an alarm in the MCP Management Console alarm browser with the following details:

Alarm family:	TSVR/TERMSVR
Alarm name:	TRMSVR_CONN
Event type:	ABNORMAL
Severity:	Major
Clear condition:	Connected to Terminal Server.

Format

The format for log report TSVR 701 is as follows:

```
Not connected to Terminal Server.
```

Selected field descriptions

This log report has no selected fields.

Action

Please check the IP address and the port configured for the Terminal server in the voicemail server configuration page in the provisioning client.

Associated OM registers

This log report has no associated OM registers.

Additional information

None

AMS300

Log report AMS300 indicates a board reset on the Media Server 2000 node. The IPM-1610 or TP-6310 board was reset.

Format

Reset Board - associated trap is <acBoardEvResettingBoard>

Selected field descriptions

This log report has no selected fields.

Action

There is no corresponding clear SNMP trap. The status stays critical until a reboot and a board started trap occurs. There is no action to be taken.

Probable cause

A user most likely has performed a reset of the media server from the element manager or from the web server interface. This trap is reporting the reset.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS301

Log report AMS301 indicates a fatal error the Media Server 2000 node. The IPM-1610 or TP-6310 board has an un-recoverable run-time error.

Format

Fatal Error - associated trap is <acBoardFatalError>

Selected field descriptions

This log report has no selected fields.

Action

Check alarms and additional logs to determine the reason for the failure. A reboot of the media server is normally required to clear the issue.

Probable cause

An unrecoverable internal software error occurred on the server. This is a run-time error.

Associated OM registers

This log report has no associated OM registers.

Additional information

There is no corresponding clear SNMP trap. The status stays critical until a reboot.

AMS302

Log report AMS302 indicates a configuration error on the Media Server 2000 node. There is an error in the current configuration for the Media Server 2000 Series node.

Format

Configuration Error - associated trap is <acBoardConfigurationError>

Selected field descriptions

This log report has no selected fields.

Action

Check alarms and additional logs to determine the reason for the failure. Fix the configuration error using the appropriate tool: web interface, IEMS or ini file. Save the configuration and if necessary reset the board.

Probable cause

This SNMP trap provides a text string describing the nature of the configuration error. The most likely cause is the entry of a bad configuration parameter, resulting in the media server flagging the condition with this SNMP trap.

Associated OM registers

This log report has no associated OM registers.

Additional information

There is no corresponding clear SNMP trap. The status stays critical until a reboot.

AMS303

Log report AMS303 indicates a temperature alarm. The MS 2000 Series node has a higher than normal temperature condition. This alarm trap is sent from the server when the temperature is above 60 degrees C (140 degrees F).

Format

Temperature Alarm - associated trap is <acBoardTemperatureAlarm>

Selected field descriptions

This log report has no selected fields.

Action

Determine the reason for the high temperature in the Media Server 2000 node. Check the fans on the media server and room temperature where the equipment is located for possible problems.

Probable cause

The operating temperature of the media server is outside the range for operation. This could be caused by a fan failure or the current environment in which the equipment is located is being kept too hot or cold; resulting in the server flagging the out-of-bounds condition.

Associated OM registers

This log report has no associated OM registers.

Additional information

The status stays critical until a corresponding alarm clear is sent when the temperature falls below 55 degrees C (131 degrees F).

AMS304

Log report AMS304 indicates a feature key error on the Media Server 2000 node. The use of a service (such as conferencing, voice prompts) was attempted but a feature key allowing use of the service was not found.

Format

Feature Key Error - associated trap is <acFeatureKeyError>

Selected field descriptions

This log report has no selected fields.

Action

Verify the current feature key setting on the media server web page and contact technical support if new feature functionality is needed.

Probable cause

An attempt was made to use a service on the media server that was not keyed into the feature key for the server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS305

Log report AMS305 indicates board call resource alarm on the Media Server 2000 node. This alarm is raised only in SIP/H.323-based gateway products as a major alarm.

Format

Board Call Resource Alarm - associated trap is
<acBoardCallResourceAlarm>

Selected field descriptions

This log report has no selected fields.

Action

This is a resource issue on the media server. Review the logs and traps from this server to view related issues, for example, lack of resources or fault conditions. A reset of the server may be needed.

Probable cause

This is an internal software error related to call resources.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS306

Log report AMS306 indicates a board controller failure alarm on the Media Server 2000 node. This alarm is raised only in SIP/H.323-based gateway products as a minor alarm.

Format

Board Controller Failure - associated trap is
<acBoardControllerFailureAlarm>

Selected field descriptions

This log report has no selected fields.

Action

Check alarms and additional logs to determine the reason for the failure.

Probable cause

The board controller has a failure.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS307

Log report AMS307 indicates an ethernet link alarm on the Media Server 2000 node. This alarm trap is received when there is a fault on one of the ethernet links which has an alarm status of “major”. If there is a fault on both interfaces, the alarm status is critical and the server is isolated.

Format

Ethernet Link Alarm - associated trap is <acBoardEthernetLinkAlarm>

Selected field descriptions

This log report has no selected fields.

Action

When both link interfaces are restored, an SNMP alarm clear trap is sent and the alarm is cleared.

Probable cause

See the description above. One of the ethernet links was disconnected by a user or went to an out-of-service condition.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS308

Log report AMS308 indicates a board overload on the Media Server 2000 node. This alarm is raised only in SIP/H.323-based gateway products as a major alarm.

Format

Overload Alarm - associated trap is <acBoardOverloadAlarm>

Selected field descriptions

This log report has no selected fields.

Action

Check alarms and additional logs to determine the reason for the failure. There may need to be an additional server added to the network based on the network planning data.

Probable cause

The server is being offered too much work for the board to handle. It is in an overload condition. Please review logs and performance data. It could be the network may not be engineered with a sufficient number of media servers for the traffic in the network. Usage data should be examined and analyzed.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS309

Log report AMS309 indicates an active alarm table overflow on the Media Server 2000 node. During each development cycle, a calculation is made as to the size of the active alarm table that will hold all possible alarms that can be raised at any one time by the board. This alarm will only be seen if there is an error in that calculation.

Format

Active Alarm Table Overflow - associated trap is
<acActiveAlarmTableOverflow>

Selected field descriptions

This log report has no selected fields.

Action

The status stays major until reboot, because it denotes a possible loss of information until the next reboot. No user action can be taken to correct this issue.

Probable cause

This is received when a software table in the media server becomes too full and cannot hold all possible alarms.

Associated OM registers

This log report has no associated OM registers.

Additional information

If an alarm was raised when the table was full, it is possible that the alarm is active, but does not appear in the active alarm table.

AMS310

Log report AMS310 indicates an ATM port alarm on the Media Server 2000 node. This is applicable for the MS2020 server and indicates an ATM port error.

Format

Atm Port Alarm - associated trap is <acAtmPortAlarm>

Selected field descriptions

This log report has no selected fields.

Action

Ensure that the fiber is plugged into the back of the system. Check for damaged fiber. Ensure that network side of the fiber is online.

Probable cause

The alarm will be raised under several link type failures:
LOS (loss of signal): possible fiber cut. AIS (alarm indication signal) soft fault. RDI (remote defect indication): problem on the remote end.

Alarm is raised under these conditions:
LOS condition is present.
AIS condition is present (LOS condition is not present).
RDI condition is present (LOS and AIS conditions are not present).

The alarm is cleared under this condition:
LOS, AIS, and RDI conditions are not present.

Associated OM registers

This log report has no associated OM registers.

Additional information

The status stays critical until the problem is resolved and a reboot occurs.

AMS311

Log report AMS311 indicates an audio provisioning alarm on the Media Server 2000 node. An audio provisioning alarm trap is sent when the AMS times out waiting for audio provisioning from the audio provisioning server.

Format

Audio Provisioning Alarm - associated trap is
<acAudioProvisioningAlarm>

Selected field descriptions

This log report has no selected fields.

Action

Check the APS and status of the node in the APS GUI. Verify the BOARD.ini configuration parameter failure.

Probable cause

The media server times out waiting for successful audio provisioning. The cause for this alarm is that the media server node is disabled in the APS and cannot get audio, the APS is down, or configuration is incorrect with respect to the APS in the Board.ini file for the media server.

Associated OM registers

This log report has no associated OM registers.

Additional information

A clear alarm trap is sent when a successful audio provisioning session occurs.

AMS312

Log report AMS312 indicates an operational state change on the Media Server 2000 node to “disabled”. When the state changes from enabled to disabled, an SNMP traps is sent with a “major” status. If the MS2000 (ATM or IP) fails to initialize the operation state is disabled.

Format

Operational State Change - associated trap is
<acOperationalStateChange>

Selected field descriptions

This log report has no selected fields.

Action

Verify the server can boot from a bootp server or load the CMP load into the server. Check the board.ini file for configuration problems.

Probable cause

This could be caused by a hardware problem or other issue causing the board to not to initialize.

Associated OM registers

This log report has no associated OM registers.

Additional information

A corresponding clear trap is sent when the state changes back to an “enabled” state. In ATM systems, the operational state of the node is also disabled if there are no ATM ports available for use. An ATM port is available for use if it is unlocked and enabled.

AMS314

Log report AMS314 indicates that the NAT placed in front of a device has been identified as a symmetric NAT.

Format

NAT Traversal Alarm - associated trap is <acNATTraversalAlarm>

Selected field descriptions

This log report has no selected fields.

Action

This alarm is cleared when a non-symmetric NAT or no NAT replaces the symmetric one.

Probable cause

When the NAT is placed in the front media server, it is identified as a symmetric NAT, raising this alarm. It is cleared when a non-symmetric NAT or no NAT replaces the symmetric one.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

AMS500

Log report AMS500 indicates a board started condition on the Media Server 2000 node. The IPM-1610 or TP-6310 board was restarted.

Format

Board Started - associated trap is <acBoardEvBoardStarted>

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action. This is an information log.

Associated OM registers

This log report has no associated OM registers.

Probable cause

Someone reset the server or re-applied power to the unit.

Additional information

There is no corresponding clear SNMP trap. This is not an alarm and does not go in the active alarm table. This trap is a signal to clear the entire active alarm table.

AMS501

Log report AMS501 indicates an admin state change on the Media Server 2000 node. The administration state of the MS 2000 Series node changed either to “locked”, “shutting down“, or “unlocked“.

Format

Admin State Change - associated trap is <acgwAdminStateChange>

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action. It is reporting a change in the administrative state of the server (locked to unlocked or unlocked to locked). Locked is an out-of-service condition whereas unlocked is an in-service condition.

Probable cause

User initiated action caused the state changed.

Associated OM registers

This log report has no associated OM registers.

Additional information

An MS 2000 Series node can be locked gracefully, allowing existing calls to complete, before administration (configuration and maintenance) is performed on the node. The MS2000 Series also supports a forced lock which immediately takes down active calls. In both types of locks, the administrative state changes to critical for either a “shutting down” or “locked” state and clears when it transitions to an unlocked state.

AMS600

Log report AMS600 indicates status of board hardware elements being tested.

Format

Enhanced BIT Status - associated trap is <acEnhancedBITStatus>

Selected field descriptions

This log report has no selected fields.

Action

Check the detail of the BIT status log. The log trap may denote the BIT test passed and no correction is needed. The detail in the trap may indicate some failure with the hardware or feature key setting in the media server. Detail should be examined more closely.

Probable cause

This trap provides the status of the BIT (Built-In-Test) on the media server. The information in the trap contains board hardware elements being tested and their status.

Associated OM registers

This log report has no associated OM registers.

Additional information

The board and status appear in the additional info fields.

AMS800

Log report AMS800 indicates that the threshold of a performance monitored object has been crossed.

Format

Performance Monitoring Threshold Crossing - associated trap is
<acPerfomanceMonitoringThresholdCrossing>

Selected field descriptions

This log report has no selected fields.

Action

No immediate corrective action is required. The performance threshold should be monitored for any issues regarding performance of the media server. The analysis of the performance data may warrant the need for additional equipment.

Probable cause

This log trap is sent out each time the threshold of a Performance Monitored object is crossed. The severity field is 'indeterminate' when the crossing is above the threshold and 'cleared' when it goes back under the threshold. The 'source' varbind in the trap indicates the object for which the threshold is being crossed.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CPUM300

Log report CPUM300 is generated when the CPU occupancy level of the Session Server unit reaches a minor, major, or critical level.

Format

The format for log report CPUM300 is as follows:

```
<OFFICE> <severity> CPUM300 MMMDD hh:mm:ss <sequence number> FLT CPUM Fault
Location: <IEMS display name>;<unit IP address>
Notification Id: <NotificationID>
State: Raised
Category: communications
Cause: congestion
Time: Mmm DD hh:mm:ss YYYY
Component Id: <unit hostname>
Specific Problem:
Description: CPU occupancy critical alarm
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	Indicates the office that generated the log report.
severity	* for minor ** for major *** for critical	Indicates the severity of the event based on the number of asterisks.
sequence number	0000-9999	A four-digit sequence number which can be used for lost log detection.
IEMS display name	alphanumeric	The name of the Session Server unit shown as the Display Name in the IEMS GUI. For example, CABSST-Unit-0
unit IP address	IPv4 IP address	The IP address of the Session Server Unit. For example, 10.67.99.67

Field	Value	Description
NotificationID	integer	An integer which can be used to uniquely correlate this alarm's raise and clear for this Session Server unit.
unit hostname	alphanumeric	The hostname of the Session Server unit as per the /etc/hosts file. Example: cablab.ss.unit0

Action

None.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CPUM399

Log report CPUM399 is generated when a CPUM300 alarm is cleared.

Format

The format for log report CPUM399 is as follows:

```
<OFFICE>      CPUM399 MMMDD hh:mm:ss <sequence number> INFO Cleared
Location: <IEMS display name>;<unit IP address>
Notification Id: <NotificationID>
State: Cleared
Time: Mmm DD hh:mm:ss YYYY
Component Id: <unit hostname>
Description: CPU occupancy critical alarm cleared
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	Indicates the office that generated the log report.
sequence number	0000-9999	A four-digit sequence number which can be used for lost log detection.
IEMS display name	alphanumeric	The name of the Session Server unit shown as the Display Name in the IEMS GUI. For example, CABSST-Unit-0
unit IP address	IPv4 IP address	The IP address of the Session Server Unit. For example, 10.67.99.67
NotificationID	integer	An integer which can be used to uniquely correlate this alarm's raise and clear for this Session Server unit.
unit hostname	alphanumeric	The hostname of the Session Server unit as per the /etc/hosts file. Example: cablab.ss.unit0

Action

None.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

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.

DBSE300

Log report [DBSE300](#) is generated any time a change in database connectivity is detected, specifically a loss of connectivity between the Session Server - Trunks 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.

NAM300

Log report NAM300 is generated only under failure conditions. The log appears only when a Session Server Application Maintenance (NAM) process is created and the required parameter specifying a valid, readable, and properly formatted configuration file is not provided.

Format

The format for log report NAM300 is as follows:

```
<OFFICE>      NAM300 MMMDD hh:mm:ss <sequence number> TBL NGSS Application Maintenance Trouble  
[Reason Text : NAM Initialization failure, retrying in 5 seconds]  
[Error Code : 14]
```

Selected field descriptions

The following table explains selected fields in the log report.

Event / Error	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.
Reason Text	text string	Detailed description of the trouble or activity. Example: NAM Initialization failure, retrying in 5 seconds
Error Code	integer	An internal error code used for debugging. Example: 14

Action

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

Associated OM registers

This log report has no associated OM registers.

Additional information

None.

NCAS325

Log report [NCAS325](#) is generated when alarm NCAS325 is raised because the non-call associated signaling (NCAS) link has gone down. Log [NCAS325](#) is also generated when the NCAS link comes up and alarm NCAS325 is cleared.

Format

The format for log report [NCAS325](#) is as follows:

```
<Date> <Time> <DeviceName> alarmd: NCAS325 <AlarmSeverity> TBL <EventLabel>  
<DeviceInfo> <AlarmRaiseLowerText>
```

Example 1 - Log [NCAS325](#) indicating the SCTP connection between the SPCLite and the core has been lost and needs to be restored.

```
Jun 15 12:14:37 rtptngss0-1 alarmd: NCAS206 CRIT TBL NCAS link Down  
NCGL=rtptngss0-1;Unit=1;SCTP Connection Link1 between the SCPLite  
and core is lost
```

Example 2 - Log [NCAS325](#) indicating the SCTP connection between the SPCLite and the core has been restored and the NCAS Link down trouble alarm is lowered.

```
Jun 15 12:14:37 rtptngss0-1 alarmd: NCAS206 NONE TBL NCAS link Down  
NCGL=rtptngss0-1;Unit=1;SCTP Connection Link1 between the SCPLite  
and core is lost - 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
DeviceName	Alphanumeric	The hostname or host id of the unit that generated the log

Field	Value	Description
Log Number	Alphanumeric	The component prefix and number of the log
Severity	CRIT or NONE	This log report is CRIT (Critical) when the NCAS325 alarm is raised, and NONE when the alarm is cleared
Event Type	TBL	The type of trouble or info recorded
Event Label	text	NCAS Link Down
Description	text	This field indicates if the NCAS link between the SCPLite and the core is lost.

Action

Restore the SCTP connection between the SCPLite and the core.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report is associated with Alarm NCAS325. Refer to the originating alarm/log for description details.

NCAS501

Log report NCAS501 is generated by the SIP Gateway application when an out-of-band REFER request is received but does not validate and the request can not be accepted.

Format

The format for log report NCAS501 is as follows:

```
<OFFICE> NCAS501 MMMDD hh:mm:ss <sequence number> TBL OOB REFER REJECTED  
OOB Refer Rejected.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.

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.

NCAS502

Log report NCAS502 is written by the Session Server Trunks application when it cannot communicate to the scplite process.

Format

The raise and clear formats for log report NCAS502 is as follows:

```
<OFFICE> ** NCAS502 MMMDD hh:mm:ss <sequence number> FLT NCAS Fault
  Location: <SST unit Display Name>;<SST unit IP address>
  Notification Id: <NotificationID>
  State: Raised
  Category: communications
  Cause: unspecifiedReason
  Time: Mmm DD hh:mm:ss YYYY
  Component Id: <SST unit hostname>
  Specific Problem:
  Description: <Description>
<OFFICE> NCAS502 MMMDD hh:mm:ss <sequence number> INFO Cleared
  Location: <SST unit Display Name>;<SST unit IP address>
  Notification Id: <NotificationID>
  State: Cleared
  Time: Mmm DD hh:mm:ss YYYY
  Component Id: <SST unit hostname>
  Description: <Description>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.
SST unit Display Name	text string	The name of the Session Server Unit shown for the Display Name in IEMS. For example, RTPO_SST1-Unit-0

Field	Value	Description
SST unit IP address	IPv4 IP address	The IP address of the Session Server Unit. For example, 172.18.164.19
NotificationID	integer	An integer which can be used to uniquely correlate this alarm's raise and clear for this Session Server unit.
SST unit hostname	text string	The hostname of the Session Server unit as per its /etc/hosts file. For example: ngss0
Description	text string	A text string indicating further information about the alarm. For example: No Scplite Connection

Action

This log report requires no action.

Associated OM registers

This log report is not associated with any OM groups.

Additional information

Refer to the originating alarm/log for description details.

NCAS601

Log report NCAS601 is written by the SIP Gateway application when a non-call associated signaling (NCAS) link is configured at the CS 2000 Session Server Manager.

Format

The format for log report NCAS601 is as follows:

```
<OFFICE> NCAS601 MMMDD hh:mm:ss <sequence number> TBL NCAS Link Created  
A new SCTP connection -LINK1 has been established between SCPLite and  
the core
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.

Action

This log report requires no action.

Associated OM registers

This log report is associated with OM groups SIPGW_NCAS and NCAS_LINK. If the link is for out-of-band signaling, then OM group SIPGW_OOB is also associated.

Additional information

Refer to the originating alarm/log for description details.

NMSS115

Log report [NMSS115](#) is generated by the SIP Gateway application when an error occurs while sending NMS TCAP messages to SCTP.

Format

The format for log report [NMSS115](#) is as follows:

```
<Switch ID> NMSS115 <DATE> <TIME> INFO SCTPNMS_ERR_SNT_REPORT  
Error occurred while sending NMS messages over Sctp.
```

Example

```
RSNN08AZ NMSS115 NOV25 09:40:46 INFO SCTPNMS_ERR_SNT_REPORT  
Error occurred while sending NMS messages over Sctp.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Switch ID	Alphanumeric	The switch name or host id of the unit that generated the log
Log Number	Alphanumeric	The component prefix and number of the log
Date	Alphanumeric	The date the log was generated
Time	Numeric	The time the log was generated
Event Type	INFO	The type of trouble or info recorded
Description	Text	This field indicates an error in sending Non-CallP messages to the Sctp

Action

This log provides information regarding a problem in sending Non-CallP messages to the Sctp. It indicates that the MWI service for a subscriber in the Sctp is broken.

Associated OM registers

This log report is generated when the SCTPNMSS OM is not pegged.

Additional information

OM group NMSNCAS provides information on the message traffic for messages sent and received on the NCAS link between the CS2K Core and the Session Server - Trunks.

NMSS116

Log report [NMSS116](#) is generated by the SIP Gateway application when an error occurs while receiving NMS TCAP messages from SCTP.

Format

The format for log report [NMSS116](#) is as follows:

```
<Switch ID> NMSS116 <DATE> <TIME> INFO SCTPNMS_ERR_RCV_REPORT  
Error occurred while receiving NMS messages over SCTP.
```

Example

```
RSNN08AZ NMSS116 NOV25 09:41:25 INFO SCTPNMS_ERR_RCV_REPORT  
Error occurred while receiving NMS messages over SCTP.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Switch ID	Alphanumeric	The switch name or host id of the unit that generated the log
Log Number	Alphanumeric	The component prefix and number of the log
Date	Alphanumeric	The date the log was generated
Time	Numeric	The time the log was generated
Event Type	INFO	The type of trouble or info recorded
Description	Text	This field indicates an error in receiving Non-CallP messages from the SCTP

Action

This log provides information regarding a problem in receiving Non-CallP messages from the SCTP. It indicates that the MWI service for a subscriber in the SCTP is broken. The NMS TCAP message received is corrupted.

Associated OM registers

This log report is generated when the SCTPNMSR OM is not pegged.

Additional information

OM group NMSNCAS provides information on the message traffic for messages sent and received on the NCAS link between the CS2K Core and the Session Server - Trunks.

NMSS117

Log report [NMSS117](#) is generated by the SIP Gateway application when an error occurs while sending REJ messages over SCTP.

Format

The format for log report [NMSS117](#) is as follows:

```
<Switch ID> NMSS117 <DATE> <TIME> INFO SCTPREJ_ERR_SNT_REPORT  
Error occurred while sending REJ messages over SCTP.
```

Example

```
RSNN08AZ NMSS117 NOV25 09:45:23 INFO SCTPREJ_ERR_SNT_REPORT  
Error occurred while sending REJ messages over SCTP.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Switch ID	Alphanumeric	The switch name or host id of the unit that generated the log
Log Number	Alphanumeric	The component prefix and number of the log
Date	Alphanumeric	The date the log was generated
Time	Numeric	The time the log was generated
Event Type	INFO	The type of trouble or info recorded
Description	Text	This field indicates an error in sending REJ messages to the SCTP

Action

This log provides information regarding a problem in sending Non-CallP messages to the SCTP. It indicates that the MWI service for a subscriber in the SCTP is broken.

Associated OM registers

This log report is generated when the SCTPREJS OM is not pegged.

Additional information

OM group NMSNCAS provides information on the message traffic for messages sent and received on the NCAS link between the CS2K Core and the Session Server - Trunks.

NMSS118

Log report [NMSS118](#) is generated by the SIP Gateway application when an error occurs while receiving REJ over messages from Sctp.

Format

The format for log report [NMSS118](#) is as follows:

```
<Switch ID> NMSS118 <DATE> <TIME> INFO SCTPREJ_ERR_RCV_REPORT  
Error occurred while receiving REJ messages over Sctp.
```

Example

```
RSNN08AZ NMSS118 NOV25 09:47:26 INFO SCTPREJ_ERR_RCV_REPORT  
Error occurred while receiving REJ messages over Sctp.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Switch ID	Alphanumeric	The switch name or host id of the unit that generated the log
Log Number	Alphanumeric	The component prefix and number of the log
Date	Alphanumeric	The date the log was generated
Time	Numeric	The time the log was generated
Event Type	INFO	The type of trouble or info recorded
Description	Text	This field indicates an error in receiving REJ messages from the Sctp

Action

This log provides information regarding a problem in receiving Non-CallP messages from the Sctp. It indicates that the MWI service for a subscriber in the Sctp is broken. The REJECT message received is corrupted.

Associated OM registers

This log report is generated when the SCTPREJR OM is not pegged.

Additional information

OM group NMSNCAS provides information on the message traffic for messages sent and received on the NCAS link between the CS2K Core and the Session Server - Trunks.

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.

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 the SIP Gateway application crossing an overload threshold. The logs are used, along with an associated major alarm to indicate overload control status.

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

May  9 13:45:26 rtpfngss1 alarmd: SIPC310 MAJOR TBL  SIP CallP
NCGL=rtpfngss1;Unit=1;SIPC Overload Threshold Reached

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	CRIT, MAJOR, MINOR	The log severity (may be related to alarm severity)
Event Type	TBL or INFO	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 process and the database.

For overload conditions, the SIP Gateway application applies flow control to throttle originations. The percentage of originations allowed to complete is indicated in a related STGW700 log report. Existing calls are not affected.

Associated OM registers

If a major alarm/log is generated, indicating an overload threshold is reached, then the associated SIPGW_CALLP OM group OVRLD_CALLS_REJECTED register is incremented. OM group SIPGW_OVERLOAD is also related.

Additional information

This log report requires no additional information.

SIPC350

Log report SIPC350 is generated by the SIP gateway application when a serious software error such as a segment violation occurs. These severe software errors are called traps. This log displays information which will help understand the process which generated the trap as well as trace back the procedures leading to the procedure which caused the trap.

Format

The format for log report SIPC350 is as follows:

```
Sep 19 00:33:22 comp1-ngss1-unit1 sipgwyappln: SIPC350 NONE
INFO TRAP Process ID : 15219
[0] sipgwyappln(_Z17defaultSigHandleri+0x69) [0x80b1ee1]
[1] /ngss/NGSS_Tools/opt/apps/lib/libpthread.so.0 [0x400748e5]
[2] /ngss/NGSS_Tools/opt/apps/lib/libc.so.6 [0x40367148]
[3] sipgwyap-
pln(_ZN13CSIPProcessor13HandleNewCallEPK16RvSipMsgHandle__PK20
RvSipCallLegHandle__P13CallDataBlock+0x381) [0x8121ec3]
[4] sipgwyap-
pln(_Z26HandleCallLegStateOfferingPK20RvSipCallLegHandle__PK23
RvSipAppCallLegHandle__+0xfb) [0x81441cb]
[5] sipgwyap-
pln(_Z21CallLegStateChangedEvPK20RvSipCallLegHandle__PK23RvSip
AppCallLegHandle__17RvSipCallLegState29RvSipCallLegStateChange
Reason+0x166) [0x81197e0]
[6] sipgwyappln(CallLegCallbackChangeCallStateEv+0x119)
[0x81edc2e]
[7] sipgwyappln(CallLegChangeState+0x144) [0x81fb9d6]
```

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

Field	Value	Description
Log Number	SIPC350	The component prefix and number of the log
Severity	Critical or 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	Alphanumeric	Detailed description of the trouble or activity

Action

A trap indicates serious error condition. Please contact Nortel support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC361

Log report SIPC361 indicates that a duplicate IP address was detected by the SIPGW application when a SIP server was added or modified with an IP address which was already in use by another SIP server.

Format

The format for log report SIPC361 is as follows:

```
Aug 10 21:38:01 compl-ngssl-unit0 SIPgwyappln: SIPC361 NONE INFO  
DATAFILL DUPLICATE IP DETECTED : 172.18.117.3 ADDED FOR SERVER  
CUSSERVER11 IS ALREADY INUSE BY SERVER CUSSERVERA1
```

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	SIPC361	The component prefix and number of the log
Severity	Critical or 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	Alphanumeric	Detailed description of the trouble or activity

Action

If this log is observed, the customer should immediately correct the provisioning to remove the duplicate IP addresses. The duplicated use of IP addresses can result in the incorrect routing of calls.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC370

Log report SIPC370 indicates the statistics of the audit messaging.

Format

The format for log report SIPC370 is as follows:

```
Aug 11 07:27:50 com1-ngss2-unit-0 sipgwyappln: SIPC370 NONE
INFO AUDIT STATS GCPAuditReqSent: 0 GCPAuditRespsRcvd : 0
GCPAuditReqsRcvd: 0 GCPAuditRespsSent: 0 INFOAuditReqSent: 0
INFOAuditRespRcvd: 0 INVITEAuditReqSent: 0 INVITEAuditRespRcvd:
0 NumNegativeResponsesSent: 0 NumExpAuditInvocations: 55
```

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	SIPC370	The component prefix and number of the log
Severity	Critical or 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	Alphanumeric	Detailed description of the trouble or activity

Action

This log provides statistics on the messaging controlled by the call processing audit. No customer action required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC371

Log report SIPC371 indicates that the Call Processing audit has convicted one or more calls because of a timeout of the SIP INFO message since the last audit cycle.

Format

The format for log report SIPC371 is as follows:

```
Aug 11 00:27:49 com1-ngss2-unit-0 sipgwyappln: SIPC371 NONE  
INFO AUDIT SIP CONVICTIONS Reported Since The Last Audit Cycle:19
```

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	SIPC371	The component prefix and number of the log
Severity	Critical or 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	Alphanumeric	Detailed description of the trouble or activity

Action

This log indicates that the SST did not receive a response to the INFO message sent by the call processing audit or the far end sent a 503 Error response stating that the call is not valid. This means that the call

was not valid and the resources on the SST have been cleaned up by the audit. If there are a large number of calls cleaned up, the customer should check the health of the network. Also, if there are a large number of convictions seen in the SIPC371 and SIPC372 logs, action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC372

Log report SIPC372 indicates that the Call Processing audit has convicted one or more calls because of the GCP audit since the last audit cycle.

Format

The format for log report SIPC372 is as follows:

```
Aug 10 15:36:48 com1-ngss2-unit-0 sipgwyappln: SIPC372 NONE  
INFO AUDIT GCP CONVICTIONS Reported since the Last audit cycle: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	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPC372	The component prefix and number of the log
Severity	Critical or 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	Alphanumeric	Detailed description of the trouble or activity

Action

This log indicates that the SST did not receive a response to the GCP audit message sent by the call processing audit to the GWC. This means that the call was not valid and the resources on the SST have

been cleaned up by the audit. If there are a large number of calls cleaned up, the customer should check the health of the CSLAN network and DPT GWCs. Also, if there are a large number of convictions seen in the SIPC371 and SIPC372 logs, action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC550

Log report [SIPC550](#), titled *SIP CallP No Database Connection*, is associated with the generation of the Critical alarm due to a loss of connectivity between the database and the CallP application. A Critical alarm is generated.

A second associated [SIPC550](#) log is labelled *SIP CallP Database Connection Established* when the connection that caused the first SIPC550 log is re-established and the alarm is cleared.

Format

The format for log report [SIPC550](#) is as follows:

```
Nov 12 21:27:48 loopback alarmd:SIPC550 CRIT TBL SIP CallP No Database  
Connection: No Database Connection
```

```
Nov 12 21:29:34 loopback alarmd:SIPC550 NONE TBL SIP CallP Database  
Connection Established: No Database Connection - 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	Alphanumeric, ex. alarmd	Identifies the NGCL or application process unit that generates the report
Log Number	SIPC550	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

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

Action

Establish connectivity between CallP and the Database

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SIPC625

Log report SIPC625 is generated when a remote IP address does not respond to heartbeat messages (OPTIONS).

Note: The SST supports an optional OPTIONS heartbeat to periodically test the signaling path to a remote SIP server.

Format

The format for log report SIPC625 is as follows:

```
Aug  1 11:58:56 SS00 SIPgwyappln: SIPC625 NONE INFO LINKMTC server:
CS2K_GTWJ IP: 172.16.16.99 Connection is not receiving messages,
IP 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	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	SIPC625	The component prefix and number of the log
Severity	Critical or 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	Alphanumeric	Detailed description of the trouble or activity

Action

This log indicates that the SST did not receive the expected responses to the OPTION heartbeat messages. This can be caused by a number of issues. The remote SIP server can be down or the signaling path between the SST and the remote SIP server can be impaired.

A corresponding alarm, SIPC325, is raised when the SST detects a loss of heartbeat to a remote SIP server. The customer should follow the actions identified for the SIPC325 alarm to isolate and address the loss of heartbeat condition.

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 CallIP message send failure
 - Been Terminating too long. Timer Expired.
 - SAM Wait Timer Messaging Timeout
 - SAM/SIP CallIP 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 CallIP created, but not in the requested state
 - SIP CallIP created, but failed to reply to SAM
 - SIP CallIP on the Inactive failed to respond to a request
 - SIP CallIP 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 - Trunks 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 - Trunks 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 - Trunks 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 - Trunks, 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 435

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 - Trunks Security and Administration NTP, NN10346-611* for information about login IDs and user IDs and authorization categories

SIPS300

Log report [SIPS300](#), titled *TLS 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 - Trunks OM group SIPGW_TLS and ensure that the event doesn't continuously recur. If it does recur, use the Session Server - Trunks 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 - Trunks 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 - Trunks OM group SIPGW_TLS. Refer to the Session Server - Trunks 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 - Trunks 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 - Trunks 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 indicates that Transport Level Security (TLS) is disabled. The log is generated when there is a problem encountered during the initialization (unlock) of the SIP Gateway application.

The SIP305 log report is always accompanied by a SIPS310 log. A SIPS305 raise log is cleared by a SIPS305 clear log.

Format

The format for log report SIPS305 when Session Server Trunks is configured to send its alarms northbound via syslog is as follows:

```
Raise:
<OFFICE> *** SIPS305 MMMDD hh:mm:ss <sequence number> TBL TLS is Not
Enabled cablab.ss.unit1 TLS is Not Enabled
Clear:
<OFFICE>      SIPS305 MMMDD hh:mm:ss <sequence number> TBL TLS is Not
Enabled cablab.ss.unit1 Automatically cleared due to alarm generator pro-
cess death
```

The format for log report SIPS305 when Session Server Trunks is configured to send its alarms northbound via SNMP is as follows:

```
Raise:
<OFFICE> *** SIPS305 MMMDD hh:mm:ss <sequence number> FLT SIPS Fault
Location: <SST unit Display Name>;<SST unit IP address>
Notification Id: <NotificationID>
State: Raised
Category: communications
Cause: fileError
Time: Mmm DD hh:mm:ss YYYY
Component Id: <SST unit hostname>
Specific Problem: TLS is Not Enabled
Description: TLS is Not Enabled
Clear:
<OFFICE>      SIPS305 MAR16 11:48:58 3344 INFO Cleared
Location: <SST unit Display Name>;<SST unit IP address>
Notification Id: <NotificationID>
State: Cleared
Time: Mmm DD hh:mm:ss YYYY
Component Id: <SST unit hostname>
Description: Automatically cleared due to alarm generator
process death
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.
SST unit Display Name	text string	The name of the Session Server Unit as per the Display Name in the IEMS GUI. For example, CABSST-Unit-0
SST unit IP address	IPv4 IP address	The IP address of the Session Server Unit. For example, 10.67.99.67
NotificationID	integer	An integer which can be used to uniquely correlate this alarm's raise and clear for this Session Server unit.
SST unit hostname	text string	The hostname of the Session Server unit as per its /etc/hosts file. For example, cablab.ss.unit0

Action

Perform the following activities in the order listed:

1. 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). This location is typically `/opt/base/shared/ssl`.
2. Ensure that the certificate and key files themselves are not corrupted or altered.
3. Ensure that the certificate and key files are meant to be together (by running the **cert_mgnt** tool). If necessary, contact your next level of support or Nortel GNPS for assistance with this activity.
4. Once the problem is resolved, and the SIP Gateway application is initialized (unlocked) again, there will be a SIPS305 clear log indicating problem resolution.

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>.

SIPS310

Log report SIPS310, 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
- TLS Failed Local Certificate Policy

Format

The format for log report SIPS310 is as follows:

```
<OFFICE> *** SIPS310 MMMDD hh:mm:ss <sequence number> INIT TLS  
      <message description>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.
message description	text string	TLS initialization failure reason. For details, refer to the bulleted list in the log summary section.

Action

Perform the following activities in the order listed:

1. 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). This location is typically `/opt/base/shared/ssl`.
2. Ensure that the certificate and key files themselves are not corrupted or altered.
3. Ensure that the certificate and key files are meant to be together (by running the **cert_mgnt** tool). If necessary, contact your next level of support or Nortel GNPS for assistance with this activity.
4. 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. SIPS605 is the clear log for SIPS310.

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 - Trunks OM group SIPGW_TLS and ensure that the event doesn’t continuously recur. If it does recur, use the Session Server - Trunks 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 - Trunks 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 - Trunks.
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 - Trunks OM group SIPGW_TLS. Refer to the Session Server - Trunks 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 effective date and when it 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 Effective: Year=2004, Month = 10, Day = 8

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 a clear log for SIPS310. A SIPS604 log may be generated with this log.

Format

The format for log report SIPS605 is as follows:

```
<OFFICE>      SIPS605 MMMDD hh:mm:ss <sequence number> INFO TLS
               TLS Security Enabled
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.

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 - Trunks). 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 - Trunks 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 - Trunks	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 - Trunks OM group SIPGW_TLS. Refer to the Session Server - Trunks 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 - Trunks 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 - Trunks, 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 - Trunks.

STGW700

Log report [STGW700](#) is an information log that is generated by the SIP Gateway application.

This log may be generated when call processing activity is interrupted or negatively impacted, such as during an 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

May 9 13:45:26 rtpfngss1 alarmd: STGW700 CRIT TBL SIPOVLD
NCGL=rtpfngss1;Unit=1;SIPC CPU occupancy critical alarm

May 9 13:45:26 rtpfngss1 sipgwyappln: STGW700 NONE INFO SIPOVLD
FCR Change OLD FCR: 100 NEW FCR: 90

May 12 10:29:00 rtpfngss1 sipgwyappln: STGW700 NONE INFO SIPOVLD
All babbling node IPs re-enabled due to 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	sipgwyappln or alarmd	Identifies the subsystem that generates the report
Log Number	STGW700	The component prefix and number of the log
Severity	NONE, CRIT, MAJOR	The log severity (may be related to alarm severity)
Event Type	INFO	The type of trouble or info recorded
Label	SIPCALLP, LINKMTC, SIPOVLD	Title label for the log
Description	LogMessage	Detailed description of the messages, refer to section Additional information .

Action

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

Associated OM registers

For log reports with a label of SIPCALLP, OM group SIPGW_CALLP is related. For log reports with a label of SIPOVLD, OM group SIPGW_OVERLOAD is related.

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
- FCR (Flow Control Rate) Change OLD FCR: <0-100> NEW FCR: <0-100>
- Babbling node detected, <server_name> <IP_address>
IP disabled
- Babbling node timeout, <server_name> <IP_address>
IP enabled
- All babbling node IPs re-enabled due to initialization
- CPU occupancy critical alarm (CPU Occupancy reached critical threshold level)
- CPU occupancy major alarm (CPU Occupancy reached major threshold level)
- CPU occupancy minor alarm (CPU Occupancy reached minor threshold level)

STGW700 (INFO AUDIT - 481 Received)

Log report STGW700 (INFO AUDIT - 481 Received) is generated when the SST call audit receives a 481 Unknown Call response for a SIP INFO audit message.

Format

The format for log report STGW700 (INFO AUDIT - 481 Received) is as follows:

```
Aug  2 17:24:57 com1-ngss2-unit-0 SIPgwyappln: STGW700 NONE INFO
SIPCALLP INFO AUDIT - 481 Received - CALL RELEASE SIPCallID:
7c04d304a87012ac13c444d116dfffc3360e7564a94c0498-0088-6145
GcpCallID : 0088.6145-03-01-29-07.49@COMPACT1 GWC :
172.18.112.240 GCP State : 14 SIP State: 7 RemoteServer :
172.18.114.114 Remote Server Name: SPECTRA1
```

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	STGW700	The component prefix and number of the log
Severity	Critical or 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	Alphanumeric	Detailed description of the trouble or activity
SIPCallID	Alphanumeric	SIP CallID for the SIP Session

Field	Value	Description
GcpCallID	Alphanumeric	GCP CallID for the SIP Session
GWC IP	Numeric	IP Address of DPT GWC that is hosting this Session
GCP State	Alphanumeric	GCP State of the SIP Session
SIP State	Numeric	SIP State of the Session
RemoteServer IP	Numeric	IP Address of Remote Server
Remote Server Name	Alphanumeric	Name of the Remote SIP Server

Action

When the SST audit receives a 481 response to a SIP INFO audit, it considers the call to be invalid and it will clear the call. This is a response from the far end device indicating that it is no longer aware of the indicated SIP session.

The customer should track and threshold the number of these logs that are occurring. This log does indicate that an active CS 2000 call has been cleared. The actual threshold value is dependent on a number of factors including the engineering of how quickly the SST audit runs and the performance of the IP network.

A recommended threshold is not provided for this log because the appropriate threshold is customer network dependent. The recommended approach is as follows:

- The customer should monitor each CS 2000 site and collect statistics on the volume of these logs under a normal working condition.
- The customer should establish their threshold for this log based on their network performance.
- The customer should monitor for significant increases over the normal volume of these logs.
- If a significant increase in the volume of these logs is observed, the customer should check the integrity of the IP network and the far end equipment.
- If root cause can not be found and the increased log volume persists, the customer should contact Nortel support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STGW700 (INFO AUDIT - No Response)

Log report STGW700 (INFO AUDIT - No Response) is generated when a response is not received for a SIP INFO audit message sent to a SIP endpoint.

Format

The format for log report STGW700 (INFO AUDIT - No Response) is as follows:

```
STGW700 NONE INFO SIPCALLP INFO AUDIT - No Response - CALL  
RELEASE SIPCallID:  
7c04d304a87012ac13c444d116dfffc3360e7564a94c0498-0088-6145  
GcpCallID : 0088.6145-03-01-29-07.49@COMPACT1 GWC :  
172.18.112.240 GCP State : 14 SIP State: 7 RemoteServer :  
172.18.114.114 Remote Server Name: SPECTRA1
```

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	STGW700	The component prefix and number of the log
Severity	Critical or 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	Alphanumeric	Detailed description of the trouble or activity
SIPCallID	Alphanumeric	SIP CallID for the SIP Session

Field	Value	Description
GcpCallID	Alphanumeric	GCP CallID for the SIP Session
GWC IP	Numeric	IP Address of DPT GWC that is hosting this Session
GCP State	Alphanumeric	GCP State of the SIP Session
SIP State	Numeric	SIP State of the Session
RemoteServer IP	Numeric	IP Address of Remote Server
Remote Server Name	Alphanumeric	Name of the Remote SIP Server

Action

The SST call audit considers the condition where it does not receive a response to a SIP INFO to be a failure condition and it will clear the call. There are a number of events that can trigger this log. The far end device may be unreachable, which would indicate a failure in the SIP signaling path. The far end device may not support the ability to respond to a SIP INFO message.

The customer should track and threshold the number of these logs that are occurring. This log does indicate that an active CS 2000 call has been cleared. The actual threshold value is dependent on a number of factors including the engineering of how quickly the SST audit runs and the performance of the IP network.

A recommended threshold is not provided for this log because the appropriate threshold is customer network dependent. The recommended approach is as follows:

- The customer should monitor each CS 2000 site and collect statistics on the volume of these logs under a normal working condition.
- The customer should establish their threshold for this log based on their network performance.
- The customer should monitor for significant increases over the normal volume of these logs.
- If a significant increase in the volume of these logs is observed, the customer should check the integrity of the IP network and the far end equipment.
- If root cause can not be found and the increased log volume persists, the customer should contact Nortel support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STGW700 (SIP AUDIT - Double Pass Failure)

Log report STGW700 (SIP AUDIT - Double Pass Failure) is generated when the SST call audit fails to audit a SIP endpoint twice on successive audit cycles.

This log is only applicable to the re-INVITE audit. The specific scenario is as follows. When the audit encounters a call that should be audited against the SIP endpoint, the audit will attempt to send a re-INVITE to the SIP endpoint. If the call is in the setup phase of the call, meaning that the call is not answered, then the audit can not send an INVITE to the SIP endpoint. On the next audit cycle, the audit will again attempt to send an INVITE to the SIP endpoint. If the call is still not in the answered state, the audit will again fail to send the re-INVITE. In this scenario, the audit will consider the call to be invalid and it will clear the call and generate this specific STGW700 log. The call is cleared because the audit detected that the call was in the unanswered state for three successive audit cycles. It is not considered to be an expected condition that a call would be in the unanswered state for three successive audit cycles. Even in an expedited mode, the call would need to be in the unanswered state for over 40 seconds.

Format

The format for log report STGW700 (SIP AUDIT - Double Pass Failure) is as follows:

```
Sep 20 10:15:41 RTPOSST1_1 sipgwyappln: STGW700 NONE INFO
SIPCALLP
Location: RTPOSST1_1 IP Address: 172.18.164.24
Time: Wed Sep 20 10:15:41 2006
Component Id: RTPOSST1_1
Unit Number: 1
Description: SIP AUDIT - Double Pass Failure - CALL RELEASE
SipCallID: 34bfb29f-5cba-f6fed080-cc31917f@blade6 GcpCallID :
8683-5440688-2006-9209745@RTPOSST1 GWC : 172.16.144.48 GCP
State : 9 SIP State: 7 RemoteServer IP : 172.18.176.6 Remote
Server Name: HURRICANE06
```

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	STGW700	The component prefix and number of the log
Severity	Critical or 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
Location	character string; IP address	Indicates the display name and IP address of the managed device.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the component ID field.
Unit Number	character string	Indicates the unit number.
Description	character string	Indicates the trap meaning.
SIPCallID	Alphanumeric	SIP CallID for the SIP Session
GcpCallID	Alphanumeric	GCP CallID for the SIP Session
GWC IP	Numeric	IP Address of DPT GWC that is hosting this Session
GCP State	Alphanumeric	GCP State of the SIP Session
SIP State	Numeric	SIP State of the Session

Field	Value	Description
RemoteServer IP	Numeric	IP Address of Remote Server
Remote Server Name	Alphanumeric	Name of the Remote SIP Server

Action

When the SST call audit experiences two consecutive audit failures for the same call, it considers the call to be invalid and it will clear the call.

The customer should track and threshold the number of these logs that are occurring. This log does indicate that an active CS 2000 call has been cleared. The actual threshold value is dependent on a number of factors including the engineering of how quickly the SST audit runs and the performance of the IP network.

A recommended threshold is not provided for this log because the appropriate threshold is customer network dependent. The recommended approach is as follows:

- The customer should monitor each CS 2000 site and collect statistics on the volume of these logs under a normal working condition.
- The customer should establish their threshold for this log based on their network performance.
- The customer should monitor for significant increases over the normal volume of these logs.
- If a significant increase in the volume of these logs is observed, the customer should check the integrity of the IP network and the far end equipment.
- If root cause can not be found and the increased log volume persists, the customer should contact Nortel support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STGW700 (GCP AUDIT - Abnormal Condition--Missing Profile Data)

Log report STGW700 (GCP AUDIT - Abnormal Condition--Missing Profile Data) indicates that the SST call audit detected missing profile data for the call being audited. When a call is initiated through the SST, data provisioned in the profile for the remote SIP server is stored in the call data structures for the call. This log indicates that the audit encountered a call that is missing expected profile data in the call data structures. This is not valid for any call and the audit will clear the call.

Format

The format for log report STGW700 (GCP AUDIT - Abnormal Condition--Missing Profile Data) is as follows:

```
Aug  2 20:37:56 com1-ngss2-unit-0 SIPgwyappln: STGW700 NONE INFO
SIPCALLP GCP AUDIT - Abnormal Condition - Missing Profile Data
- CALL RELEASE SIPCallID:
87988a04a07012ac13c444d17207669b2541da1d6947f898-0053-6150
GcpCallID : 900f-91-2006-0802203216@NGSS2 GWC : 172.18.112.192
GCP State : 5 SIP State: 7 RemoteServer IP : 172.18.112.160
Remote Server Name: NGSS1
```

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	STGW700	The component prefix and number of the log
Severity	Critical or 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

Field	Value	Description
Description	Alphanumeric	Detailed description of the trouble or activity
SIPCallID	Alphanumeric	SIP CallID for the SIP Session
GcpCallID	Alphanumeric	GCP CallID for the SIP Session
GWC IP	Numeric	IP Address of DPT GWC that is hosting this Session
GCP State	Alphanumeric	GCP State of the SIP Session
SIP State	Numeric	SIP State of the Session
RemoteServer IP	Numeric	IP Address of Remote Server
Remote Server Name	Alphanumeric	Name of the Remote SIP Server

Action

The customer should report repeated instances of these logs to Nortel support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STGW700 (GCP AUDIT - Abnormal Condition--Missing Server Data)

Log report STGW700 (GCP AUDIT - Abnormal Condition--Missing Server Data) indicates that the SST call audit detected missing remote SIP server data for the call being audited. When a call is initiated through the SST, data is stored in the call data structures about the specific remote SIP server associated with the call. This log indicates that the audit encountered a call that is missing the expected data that identifies the remote SIP server associated with the call. This is not valid for any call and the audit will clear the call.

Format

The format for log report STGW700 (GCP AUDIT - Abnormal Condition--Missing Server Data) is as follows:

```
Aug  2 20:37:56 com1-ngss2-unit-0 SIPgwyappln: STGW700 NONE INFO
SIPCALLP GCP AUDIT - Abnormal Condition - Missing Server Data -
CALL RELEASE SIPCallID:
87988a04a07012ac13c444d17207669b2541da1d6947f898-0053-6150
GcpCallID : 900f-91-2006-0802203216@NGSS2 GWC : 172.18.112.192
GCP State : 5 SIP State: 7 RemoteServer IP : 172.18.112.160
Remote Server Name: NGSS1
```

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	STGW700	The component prefix and number of the log
Severity	Critical or None	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	Alphanumeric	Detailed description of the trouble or activity
SIPCallID	Alphanumeric	SIP CallID for the SIP Session
GcpCallID	Alphanumeric	GCP CallID for the SIP Session
GWC IP	Numeric	IP Address of DPT GWC that is hosting this Session
GCP State	Alphanumeric	GCP State of the SIP Session
SIP State	Numeric	SIP State of the Session
RemoteServer IP	Numeric	IP Address of Remote Server
Remote Server Name	Alphanumeric	Name of the Remote SIP Server

Action

The customer should report repeated instances of these logs to Nortel support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STGW700 (GCP AUDIT - Double Pass Failure)

The SST call audit sends audit requests to the DPT GWC to ensure that active calls on the SST are still active on the associated DPT GWC. If the SST call audit does not receive a response from the DPT GWC, it considers the timeout to be a first pass failure. On the second audit cycle, the SST call audit will send a second audit request to the DPT GWC for the call. If the second audit message also receives no response, the SST will clear the call and generate this log.

Format

The format for log report STGW700 (GCP AUDIT - Double Pass Failure) is as follows:

```
Sep 20 10:07:10 RTPOSST1_1 sipgwyappln: STGW700 NONE INFO
SIPCALLP
Location: RTPOSST1_1 IP Address: 172.18.164.24
Time: Wed Sep 20 10:07:10 2006
Component Id: RTPOSST1_1
Unit Number: 1
Description: GCP AUDIT - Double Pass Failure - CALL RELEASE
SipCallID: 34bfb2a6-5cba-f6fed080-cc319206@blade6 GcpCallID :
8683-5440703-2006-9209745@RTPOSST1 GWC : 172.16.144.200 GCP
State : 9 SIP State: 7 RemoteServer IP : 172.18.176.6 Remote
Server Name: HURRICANE06
```

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	STGW700	The component prefix and number of the log
Severity	Critical or None	The log severity (may be related to alarm severity)

Field	Value	Description
Event Type	INFO	The type of trouble or info recorded
Label	Alphanumeric	Title label for the log
Location	character string; IP address	Indicates the display name and IP address of the managed device.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the component ID field.
Unit Number	character string	Indicates the unit number.
Description	character string	Indicates the trap meaning.
SIPCallID	Alphanumeric	SIP CallID for the SIP Session
GcpCallID	Alphanumeric	GCP CallID for the SIP Session
GWC IP	Numeric	IP Address of DPT GWC that is hosting this Session
GCP State	Alphanumeric	GCP State of the SIP Session
SIP State	Numeric	SIP State of the Session
RemoteServer IP	Numeric	IP Address of Remote Server
Remote Server Name	Alphanumeric	Name of the Remote SIP Server

Action

This log indicates that the SST call audit has cleared an active call. Call state mismatches can occur during maintenance activities such as a DPT GWC switch of activity, a core restart, or an SST switch of activity. If these logs are observed, the customer should analyze the CS 2000 log stream to see if the logs correspond to a maintenance event. If the logs do not correspond to a maintenance event, or they persist, the customer should contact Nortel support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STGW700 (GCP AUDIT - Force Release)

When the SST call audit takes action to clear an active call, it marks the call with a call clearing action indicator. If the audit detects that the call was not cleared through normal clearing actions, it will perform a force release to clear the call and it will generate this log.

Format

The format for log report STGW700 (GCP AUDIT - Force Release) is as follows:

```
Sep 20 10:28:41 RTPOSST1_1 sipgwyappln: STGW700 NONE INFO SIPCALLP
Location: RTPOSST1_1 IP Address: 172.18.164.24
Time: Wed Sep 20 10:28:41 2006
Component Id: RTPOSST1_1
Unit Number: 1
Description: GCP AUDIT - Force Release - CALL RELEASE SipCallID: 34bfb29f-5cba-f6fed080-
cc31917f@blade6 GcpCallID : 8683-5440688-2006-9209745@RTPOSST1 GWC : 172.16.144.48 G
State : 9 SIP State: 7 RemoteServer IP : 172.18.176.6 Remote Server Name: HURRICANE06
```

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	STGW700	The component prefix and number of the log
Severity	Critical or 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
Location	character string; IP address	Indicates the display name and IP address of the managed device.

Field	Value	Description
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the component ID field.
Unit Number	character string	Indicates the unit number.
Description	character string	Indicates the trap meaning.
SIPCallID	Alphanumeric	SIP CallID for the SIP Session
GcpCallID	Alphanumeric	GCP CallID for the SIP Session
GWC IP	Numeric	IP Address of DPT GWC that is hosting this Session
GCP State	Alphanumeric	GCP State of the SIP Session
SIP State	Numeric	SIP State of the Session
RemoteServer IP	Numeric	IP Address of Remote Server
Remote Server Name	Alphanumeric	Name of the Remote SIP Server

Action

This log indicates that the SST audit required a force release action to clear an active call. If these logs persist, the customer should contact Nortel support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STGW700 (GCPListener Socket RecvFrom Failed)

Log report STGW700 (GCPListener Socket RecvFrom Failed) indicates that a UDP socket read error occurred in the GCPListener task.

This task is used by the SST to receive messages from the DPT GWs.

Format

The format for log report STGW700 (GCPListener Socket RecvFrom Failed) is as follows:

```
Jul 30 21:31:47 compl-ngss1-unit1 SIPgwyappln: STGW700 NONE
INFO SIPCALLP GCPListener Socket RecvFrom Failed. rc = -1, errno
= 4 Interrupted system call, numRcvdFail = 1 0,
recvFailThreshold1 = 5, recvFailThreshold2 = 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	sipgwyappln	Identifies the NGCL or application process unit that generates the report
Log Number	STGW700	The component prefix and number of the log
Severity	Critical or 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	Alphanumeric	Detailed description of the trouble or activity

Field	Value	Description
rc	Numeric	The return code that indicates that the UDP read error failed
errno	Alphanumeric	The error type
numRcvdFail	Numeric	The number of simultaneous errors that have occurred
recvFailThreshold1	Numeric	The threshold set for non-critical UDP read errors (default = 5)
recvFailThreshold2	Numeric	The threshold set for critical UDP read errors (default = 1)

Action

When the GCP Listener task experiences a UDP read error, it will produce the STGW700 SIPCALLP GCPListener Socket RecvFrom Failed log. A SIPC322 alarm will also be raised when the UDP read error is detected. The customer should follow the recommended actions for clearing the SIPC322 alarm. If persistent UDP read errors are reported with this STGW700 log, the customer should report the condition to Nortel support.

When the GCP Listener read error occurs, the SIPC322 alarm will be raised. If the UDP read error is transient, the SST will clear the alarm when a successful UDP read occurs. If the threshold of consecutive UDP read errors is exceeded, the SST will perform an autonomous switch of activity in an attempt to clear the failure condition.

If the UDP read errors persist and the SST can not perform a switch of activity, the SIPC322 alarm will persist to trigger the appropriate customer corrective actions.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STGW700 (SLGTGN digits not stripped)

Log report STGW700 (SLGTGN digits not stripped) is generated when an incoming INVITE contains only prefix digits. In this case, the SLGTGN feature is enabled on the SST. The incoming INVITE contains digits that match a provisioned profile, and the digits that match the provisioned profile are the only digits present. If the prefix digits, which are the digits that match the provisioned profile, are stripped, the call would be offered to the CS 2000 core with no digits. This is not valid for IBNT2 trunks. This log is generated to indicate that the call contained digits that matched a provisioned profile and in this case, the prefix digits are not stripped.

Format

The format for log report STGW700 (SLGTGN digits not stripped) is as follows:

```
Jul 30 21:31:47 comp1-ngss1-unit1 SIPgwyappln: STGW700 NONE
INFO SIPCALLP SLGTGN digits not stripped as they are the only
digits received
```

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	STGW700	The component prefix and number of the log
Severity	Critical or None	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	Alphanumeric	Detailed description of the trouble or activity

Action

Customer must check their networks to see if this is intentional. Calls may not be routing correctly.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STGW700 (WaitThread poll failed)

Log report STGW700 (WaitThread poll failed) indicates that the SST call processing subsystem experienced a failure when trying to poll a UDP socket. The call processing subsystem uses UDP sockets for internal SST signaling. A failure in the UDP sockets used by the call processing subsystem could impact the SST's ability to process calls.

Format

The format for log report STGW700 (WaitThread poll failed) is as follows:

```
Jul 30 21:31:47 compl-ngss1-unit1 SIPgwyappln: STGW700 NONE INFO  
SIPCALLP WaitThread poll failed errno = 4 Interrupted system call
```

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	STGW700	The component prefix and number of the log
Severity	Critical or 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	Alphanumeric	Detailed description of the trouble or activity

Action

If this log is observed, the customer should check the CS 2000 core OM's and the SST OM's to ensure that the SST is still processing calls.

Associated OM registers

TRK OM group in the CS 2000 core provides data on the incoming and outgoing calls for all SIP trunk groups. The SST OM's also provide data on the incoming and outgoing SIP calls.

Additional information

This log report requires no additional information.

STGW800

Log STGW800 indicates that communications to a DPT GWC has been established (Inactive to Active) or that communications to a DPT GWC has been lost (Active to Inactive). The log provides the IP address of the associated DPT GWC.

The SST uses a heartbeat to validate the integrity of signaling to each associated DPT GWC.

Format

The format for log report STGW800 is as follows:

```
Sep 19 20:55:59 RTPOSST1_1 sipgwyappln: STGW800 NONE INFO  
LINKMTC  
Location: RTPOSST1_1 IP Address: 172.18.164.24  
Time: Tue Sep 19 20:55:59 2006  
Component Id: RTPOSST1_1  
Unit Number: 1  
Description: GWC 172.16.145.116 State Changed from Inactive to  
Active
```

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	STGW800	The component prefix and number of the log
Severity	Critical or 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

Field	Value	Description
Location	character string; IP address	Indicates the display name and IP address of the managed device.
Time	character string	Indicates the date and time of the log.
Component Id	character string	Indicates the component ID field.
Unit Number	character string	Indicates the unit number.
Description	character string	Indicates the trap meaning.

Action

A persistent occurrence of these logs could indicate a network issue that is impacting GWC to SST communications. The customer should contact Nortel support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USM300

Log report USM300 is generated when swchecker fails to process and add a parcel file to the SST patching system.

Format

The format for log report USM300 is as follows. The failure example shown would occur if a duplicate patch was delivered to the SST.

NT STD format

```
<OFFICE>      USM300 MMMDD hh:mm:ss <sequence number> FAIL USM Patch Software  
Check Failure File name:<Patch Filename>, Reason:<Failure Reason>
```

Syslog Example

```
Dec 14 11:08:32 rtpf_ngss0 swchecker: USM300 NONE FAIL USM Patch Software  
Check Failure Filename:session_server_i686-91.11.00-001.i386.parcel,  
Reason: Failed adding patch details to the database
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	Indicates the office that generated the log report.
Sequence number	0000 - 9999	Sequential integer which can be used for lost log detection
Severity	None	Log severity
Event Type	FAIL	Failure log
Label	USM Patch Software Check Failure	Log label
Filename	<Patch Parcel Filename>	Lists the patch parcel that failed processing and the reason.
Reason	<Reason for failure>	Provides the reason for the patch parcel failure.

Action

Determine if the patch parcel listed applies to the software load in the SST. If so, attempt to retrieve the patch parcel file again, and rerun **swchecker**.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USM301

Log report USM301 is generated for some patch application failures. Errors with the ngsspatch command syntax do not produce custlogs.

Format

The format for log report USM301 is as follows:

NT STD format

```
<OFFICE>      USM301 MMMDD hh:mm:ss <sequence number> FAIL USM Patch Appli-
cation Failure Patch ID:<Patch ID>, Reason:<Failure Reason>, <Failure
Description>
```

Syslog Example

```
Mar 3 17:29:42 rtpf_unit0 logit: USM301 NONE FAIL USM Patch Application
Failure Patch ID:session_server_i686-91.11.00-002.i386, Reason:Bad job
RC:1, Patch dependency failure, session_server_i686-91.11.00-001 is needed
by session_server_i686-91.11.00-002
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	Indicates the office that generated the log report.
Sequence number	0000 - 9999	Sequential integer which can be used for lost log detection
Severity	None	Log severity
Event Type	FAIL	Failure log
Label	USM Patch Application Failure	Log label
Patch ID	<Patch Name>	Provides the patch name.
Reason	<Reason for failure>	Provides a reason for failure, and available information.

Action

Determine the next course of action based on the reason provided. In the example provided, the application of patch 002 failed as it requires patch 001 which is not installed. Resolution in this case may be to first apply patch 001, and then reattempt applying patch 002.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USM303

Log report USM303 is generated for some patch removal failures. Errors with ngsspatch command syntax do not produce custlogs.

Format

The format for log report USM303 is as follows:

NT STD format

```
<OFFICE>      USM303 MMMDD hh:mm:ss <sequence number> FAIL Patch Removal  
Failure Patch ID:<Patch ID>, Reason:<Failure Reason>, <Failure Description>
```

Syslog Example

```
Mar 7 11:01:14 rtpf_unit0 logit: USM303 NONE FAIL USM Patch Removal Failure  
Patch ID:session_server_i686-91.11.00-001.i386, Reason:Bad job RC:1, Patch  
dependency failure, session_server_i686-91.11.00-001 is needed by  
(installed) session_server_i686-91.11.00-002
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	Indicates the office that generated the log report.
Sequence number	0000 - 9999	Sequential integer which can be used for lost log detection
Severity	None	Log severity
Event Type	FAIL	Failure log
Label	USM Patch Removal Failure	Log label
Patch ID	<Patch Name>	Provides the patch name.
Reason	<Reason for failure and information>	Provides a reason for failure and available information.

Action

Determine the next course of action based on the reason provided. In the example provided, the attempted removal of patch 001 failed as applied patch 002 is dependent on patch 001. If appropriate, the resolution of this case may be to first remove patch 002 and then reattempt removing patch 001.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USM305

Log report USM305 is generated when a miscellaneous error occurs in the SST patching system. The problem may be related to either a patch application or removal attempt.

Format

The format for log report USM305 is as follows:

NT STD format

```
<OFFICE>      USM305 MMMDD hh:mm:ss <sequence number> FAIL USM Patch Command  
Failure Patch ID:<Patch ID>, Error:<Error Description>
```

Syslog Example

```
Dec 2 11:12:30 rtpf_ngss0 agent_controller: USM305 NONE FAIL USM Patch  
Command Failure Patch ID:session_server_i686-91.11.00-001.i386, Error:Add  
job failure
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	Indicates the office that generated the log report.
Sequence number	0000 - 9999	Sequential integer which can be used for lost log detection
Severity	None	Log severity
Event Type	FAIL	Failure log
Label	USM Patch Command Failure	Log label
Patch ID	<Patch Name>	Provides the patch name.
Error	<Error description>	Provides a description of the error encountered.

Action

Contact your Nortel support representative to resolve the software errors reported by USM305.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USM600

Log report USM600 is generated when a parcel file is successfully processed by swchecker and added to the NGSS patching system.

Format

The format for log report USM600 is as follows:

NT STD format

```
<OFFICE>      USM600 MMMDD hh:mm:ss <sequence number> INFO Patch Software Check  
Success Filename:<Patch Filename>
```

Syslog Example

```
Nov 20 20:49:32 rtpf_ngss0 swchecker: USM600 NONE INFO USM Patch Software Check  
Success Filename:session_server_i686-91.11.00-001.i386.parcel
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	Indicates the office that generated the log report.
Sequence number	0000 - 9999	Sequential integer which can be used for lost log detection
Severity	None	Log severity
Event Type	INFO	Information log
Label	USM Patch Software Check Success	Log label
Filename	<Patch Parcel Filename>	Provides the filename of the successfully processed patch parcel.

Action

None.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USM601

Log report USM601 is generated for successful patch application. This log includes the patch ID and new patch state. For applies, the patch state is either of the following:

- Partial, which means the patch has been applied to the unit where the log is generated,
- or
- Applied, which means the patch has been successfully applied to both units.

Format

The format for log report USM601 is as follows:

NT STD format

```
<OFFICE> USM601 MMMDD hh:mm:ss <sequence number> INFO USM Patch  
Application Success Patch ID:<patch ID>, Patch State:<Patch State>
```

Syslog Examples

```
Nov 21 03:31:04 rtpf_ngss0 agent_controller: USM601 NONE INFO USM Patch  
Application Success Patch ID:session_server_i686-91.11.00-001.i386, Patch  
State:Partial
```

```
Nov 21 03:31:04 rtpf_ngss0 agent_controller: USM601 NONE INFO USM Patch  
Application Success Patch ID:session_server_i686-91.11.00-001.i386, Patch  
State:Applied
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	Indicates the office that generated the log report.
Sequence number	0000 - 9999	Sequential integer which can be used for lost log detection
Severity	None	Log severity
Event Type	INFO	Information log

Field	Value	Description
Label	USM Patch Application Success	Log label
Patch ID	<Patch Name>	Provides the patch name and information about system actions required during the patch removal process. In this example, while removing patch 001, it was necessary to restart the SIP Gateway application.
Patch State	<Partial or Applied>	Partial means the patch has been applied to the unit where the log is generated. Applied means the patch has been successfully applied to both units.

Action

None.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USM602

Log report USM602 is generated during a patch application if it is necessary to restart an SST application process. The log contains the patch ID and may include an **slrrc** value that can be used in debugging.

Format

The format for log report USM602 is as follows:

NT STD format

```
<OFFICE>      USM602 MMMDD hh:mm:ss <sequence number> INFO Patch Application  
Info Patch ID:<patch ID>, <information text>
```

Syslog Example

```
Nov 21 16:43:21 rtpf_ngss0 agent_controller: USM602 NONE INFO USM Patch  
Application Info Patch ID:session_server_i686-91.11.00-001.i386, Restarting  
SIP Gateway Application due to slrrc:4
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	Indicates the office that generated the log report.
Sequence number	0000 - 9999	Sequential integer which can be used for lost log detection
Severity	None	Log severity
Event Type	INFO	Information log
Label	USM Patch Application Info	Log label
Patch ID	<Patch Name>	Provides the patch name.
Information text	<Information Text>	Provides information about system actions required during the patch application process. In the example, while applying patch 001, it was necessary to restart the SIP Gateway application.

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USM603

Log report USM603 is generated for successful patch removal. This log includes the patch ID and new patch state. For removes, the patch state is either of the following:

- Partial, which means the patch has been removed only on the unit where the log is generated,
- or
- Available, which means the patch has been successfully removed from both SST units.

Format

The format for log report USM603 is as follows:

NT STD format

```
<OFFICE>      USM603 MMDD hh:mm:ss <sequence number> INFO USM Patch Removal  
Success Patch ID:<Patch ID>, Patch State:<Patch State>
```

Syslog Examples

```
Nov 21 17:13:58 rtpf_ngss0 agent_controller: USM603 NONE INFO USM Patch Removal  
Success Patch ID:session_server_i686-91.11.00-001.i386, Patch State:Partial  
Nov 21 17:13:59 rtpf_ngss0 agent_controller: USM603 NONE INFO USM Patch Removal  
Success Patch ID:session_server_i686-91.11.00-001.i386, Patch State:Available
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	Indicates the office that generated the log report.
Sequence number	0000 - 9999	Sequential integer which can be used for lost log detection
Severity	None	Log severity
Event Type	INFO	Information log
Label	USM Patch Removal Success	Log label

Field	Value	Description
Patch ID	<Patch Name>	Provides the patch name and state.
Patch State	<Partial or Available>	"Partial" indicates the patch has been successfully removed from one SST unit, but it is still applied to the SST mate unit. "Available" indicates the patch has been successfully removed from both SST units.

Action

None.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USM604

Log report USM604 is generated during a patch removal if it is necessary to restart an NGSS application process. The log contains the patch ID and may include an **slrrc** value that can be used in debugging.

Format

The format for log report USM604 is as follows:

NT STD format

```
<OFFICE>      USM604 MMMDD hh:mm:ss <sequence number> INFO USM Patch Removal  
Info Patch ID:<Patch ID>, <information text>
```

Syslog Example

```
Nov 21 16:44:21 rtpf_ngss0 agent_controller: USM604 NONE INFO USM Patch  
Removal Info Patch ID:session_server_i686-91.11.00-001.i386, Restarting SIP  
Gateway Application due to slrrc:4
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	Indicates the office that generated the log report.
Sequence number	0000 - 9999	Sequential integer which can be used for lost log detection
Severity	None	Log severity
Event Type	INFO	Information log
Label	USM Patch Removal Info	Log label
Patch ID	<Patch Name>	Provides the patch name.
Information text	<Information Text>	Provides information about system actions required during the patch removal process. In the example, while removing patch 001, it was necessary to restart the SIP Gateway application.

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USM605

Log report USM605 is generated when the **ngssdeletepatch** command successfully removes a patch from the SST patching system.

Format

The format for log report USM605 is as follows:

```
NT STD format
<OFFICE>      USM605 MMMDD hh:mm:ss <sequence number> INFO USM Patch Deletion
Patch deleted from system: <Patch File>

Syslog Example
Dec 14 11:58:49 rtpf_ngss0 logit: USM605 NONE INFO USM Patch Deletion Patch
deleted from system:session_server_i686-91.11.00-001.i386.parcel
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	Indicates the office that generated the log report.
Sequence number	0000 - 9999	Sequential integer which can be used for lost log detection
Severity	None	Log severity
Event Type	INFO	Information log
Label	USM Patch Deletion	Log label
Patch deleted from system	<Patch Parcel Filename>	Provides the patch parcel file name that was removed from the SST patching system.

Action

None.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

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 - Trunks 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 - Trunks Fault Management*, NN10332-911 for a description of how to monitor the connectivity and network status for both Session Server - Trunks 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 - Trunks 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 - Trunks 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.

XTS302

Log report [XTS302](#) indicates that free space on the root file system is low.

The Session Server or Policy Controller platform generates log report [XTS302](#) in addition to the alarm.

Format

The format for log report [XTS302](#) is as follows:

```
APR17 07:47:46 ngss-1 XTS302 minor FLT Disk/Storage
Unit Number : 0, ACTIVE
Percentage of root free disk space is less than
or equal to 5.00; critical 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	XTS302	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 recorded
Label	Alphanumeric	Title label for the log
Description	Alphanumeric	Detailed description of the trouble

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 disk drive 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 - Trunks 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 rtpsngsslunit1 alarmd: XTS305 MAJOR FLT
NTP Error NCGL=rtpsngsslunit1;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 - Trunks 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 - Trunks 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 - Trunks 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 - Trunks unit* in the Session Server - Trunks 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 - Trunks 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 - Trunks 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 the NCGI platform to monitor the status of CPU and memory related resources for the active Session Server - Trunks 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 - Trunks 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 - Trunks 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 - Trunks or Policy Controller is out of service and the node is not operation in a fault-tolerant mode.

The Session Server - Trunks 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 - Trunks 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 - Trunks or Policy Controller active unit cannot communicate to the mate unit through the ethernet connections.

The Session Server - Trunks 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 - Trunks 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 - Trunks 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 - Trunks 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 - Trunks 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 - Trunks 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 - Trunks or Policy Controller unit is unavailable or status information for the mate unit is unavailable at the maintenance interface.

The Session Server - Trunks 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 - Trunks 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 - Trunks 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 - Trunks 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.

XTS382

Log report XTS382 indicates that one or more sensors on the server chassis is reporting an alarm condition.

The alarm conditions reported by XTS382 are as follows:

- cooling system problem
- processor problem
- threshold crossed
- equipment malfunction

Once raised, the severity of an alarm might escalate if:

- the number of sensors detecting failure increases, or
- the nature of the sensor failure changes (for example, if both minor and major thresholds are crossed)

Format

The format for log report XTS382 when Session Server Trunks is configured to send its alarms northbound via SNMP to IEMS is as follows:

```
<OFFICE> <severity> XTS382 MMMDD hh:mm:ss <sequence number> FLT XTS Fault
Location: <SST unit Display Name>;<SST unit IP address>
Notification Id: <NotificationID>
State: Raised
Category: equipment
Cause: thresholdCrossed
Time: Mmm DD hh:mm:ss YYYY
Component Id: <SST unit hostname>
Specific Problem:
Description: Chassis sensor alarm raised. <# sensor> sensor are
reporting failures.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
severity	* for minor, ** for major, *** for critical	Indicates the severity of the event based on the number of asterisks.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.
SST unit Display Name	text string	The name of the Session Server Unit as per the Display Name in the IEMS GUI. For example, RTPO_SST1-Unit-0
SST unit IP address	IPv4 IP address	The IP address of the Session Server Unit. For example, 172.18.164.19
SST unit hostname	text string	The hostname of the Session Server unit provided in its /etc/hosts file. For example: ngss0
NotificationID	integer	An integer which can be used to uniquely correlate this alarm's raise and clear for this Session Server unit.
# sensors	integer	The number of sensors reporting a failure.

Actions

Reference the Sensor Information page for further sensor data.

If the active unit is affected, consider a manual switch of activity (SWACT) to reduce the risk of loss of service.

Check operational and environmental conditions of the affected unit.

Hardware component replacement might be required to resolve the condition.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

XTS383

Log report XTS383 indicates that a power supply module is reporting an alarm condition.

Once raised, the severity of an alarm might escalate if:

- the number of failed primary or secondary sensors in the group detecting failure increases, or
- the nature of the sensor failure changes (for example, if both minor and major thresholds are crossed)

Format

The format for log report XTS383 when Session Server Trunks is configured to send its alarms northbound via SNMP to IEMS is as follows:

```
<OFFICE> <severity> XTS383 MMMDD hh:mm:ss <sequence number> FLT XTS Fault
Location: <SST unit Display Name>;<SST unit IP address>
Notification Id: <NotificationID>
State: Raised
Category: equipment
Cause: thresholdCrossed
Time: Mmm DD hh:mm:ss YYYY
Component Id: <SST unit hostname>
Specific Problem:
Description: Power supply alarm raised. Module A : Ok.
Module B : <# sensors> sensor are reporting a failure.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
severity	* for minor, ** for major, *** for critical	Indicates the severity of the event based on the number of asterisks.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.

Field	Value	Description
SST unit Display Name	text string	The name of the Session Server Unit as per the Display Name in the IEMS GUI. For example, RTP0_SST1-Unit-0
SST unit IP address	IPv4 IP address	The IP address of the Session Server unit. For example, 172.18.164.19
SST unit hostname	text string	The hostname of the Session Server unit provided in its /etc/hosts file. For example: ngss0
NotificationID	integer	An integer which can be used to uniquely correlate this alarm's raise and clear for this Session Server unit.
# sensors	integer	The number of sensors reporting a failure.

Actions

Reference the Sensor Information page for further sensor data.

If the active unit is affected, consider a manual switch of activity (SWACT) to reduce the risk of loss of service.

Check operational and environmental conditions of the affected unit.

Hardware component replacement might be required to resolve the condition.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires 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 - Trunks 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 - Trunks 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 - Trunks 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 - Trunks 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 - Trunks 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.

XTS638

Log report XTS638 is generated when the switch link (**swlnk**) operation is executed on the LAN links of one unit in a mated pair Session Server Trunks platform.

Format

The format for log report XTS638 is as follows:

```
<OFFICE>      XTS638 MMMDD hh:mm:ss <sequence number> INFO Switch Link Finished
Component Id: <SST unit hostname>
Time: Mmm DD hh:mm:ss YYYY
Unit Number : <Unit Number>, <Unit Activity>
Description : Result: <Result>, Initiator: <Initiator>;
```

Selected field descriptions

The following table explains selected fields in the log report.

Event / Error	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.
SST unit hostname	alphanumeric	The hostname of the Session Server unit as per the /etc/hosts file. Example: cablab.ss.unit0
Unit Number	0 or 1	An integer indicating which Unit this log applies to.
Unit Activity	alphabetic	Specifies the activity state of the SST unit in question. Possible values: ACTIVE or INACTIVE.
Result	alphabetic	Indicates the result of the action taken. Example: Passed
Initiator	alphanumeric	Indicates how the action was initiated. Example: Manual

Action

None.

Associated OM registers

This log report has no associated OM registers.

Additional information

The following is an example of log report XTS638:

```
cablab      XTS638 JAN27 01:38:08 2301 INFO Switch Link Finished
Component Id: cablab.ss.unit0
Time: Jan 27 01:38:08 2006
Unit Number : 0, INACTIVE
Description : Result: Passed, Initiator: Manual;
```

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.

XTS676

Log report XTS676 is generated when a reboot is initiated on a simplex Session Server Trunks platform.

Format

The format for log report XTS676 is as follows:

```
Feb 27 13:41:13 RTPOSST1_1 logman: XTS676 NONE INFO Reboot Initiated  
Component Id: RTPOSST1_1  
Time: Feb 27 13:41:13 2006  
Description : Result: Passed, Initiator: Manual;
```

Selected field descriptions

The following table explains selected fields in the log report.

Event / Error	Value	Description
hostname	variable	Contains the server host name where the alarm was raised.
process name	logman	the system process responsible for generating the customer log
severity	NONE	The log severity (may be related to alarm severity)
event type	INFO	The type of trouble recorded
label	Reboot Initiated	Title label for the log

Actions

Monitor completion of the reboot on the affected unit.

Confirm that the affected services have resumed and are operating properly.

Associated OM registers

This log report has no associated OM registers.

Additional information

ATTENTION

Application services are unavailable until successful completion of the reboot.

XTS677

Log report XTS677 is generated when a mate reboot is initiated on the standby unit in a mated pair Session Server Trunks platform.

Format

The format for log report XTS677 is as follows:

```
<OFFICE>      XTS677 MMMDD hh:mm:ss <sequence number> INFO Reboot Mate Initiated
Component Id: <SST unit hostname>
Time: Mmm DD hh:mm:ss YYYY
Unit Number : <Unit Number>, <Unit Activity>
Description : Result: <Result>, Initiator: <Initiator>;
```

Selected field descriptions

The following table explains selected fields in the log report.

Event / Error	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.
SST unit hostname	alphanumeric	The hostname of the Session Server unit as per the /etc/hosts file. Example: cablab.ss.unit0
Unit Number	0 or 1	An integer indicating which Unit this log applies to.
Unit Activity	alphabetic	Specifies the activity state of the SST unit in question. Possible values: ACTIVE or INACTIVE.
Result	alphabetic	Indicates the result of the action taken. Example: Passed
Initiator	alphanumeric	Indicates how the action was initiated. Example: Manual

Actions

Monitor completion of the reboot on the affected unit.

Confirm that the affected services have resumed and are operating properly.

Associated OM registers

This log report has no associated OM registers.

Additional information

The following is an example of log report XTS677:

```
cablab      XTS677 JAN27 01:41:51 2334 INFO Reboot Mate Initiated
Component Id: cablab.ss.unit1
Time: Jan 27 01:41:51 2006
Unit Number : 1, ACTIVE
Description : Result: Passed, Initiator: Manual;
```

XTS678

Log report XTS678 is generated when the **Halt** command is executed on a simplex Session Server Trunks platform.

Format

The format for log report XTS678 is as follows:

```
<OFFICE>      XTS678 MMMDD hh:mm:ss <sequence number> INFO Halt Initiated
Component Id: <SST unit hostname>
Time: Mmm DD hh:mm:ss YYYY
Unit Number : <Unit Number>, <Unit Activity>
Description : Result: <Result>, Initiator: <Initiator>;
```

Selected field descriptions

The following table explains selected fields in the log report.

Event / Error	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.
SST unit hostname	alphanumeric	The hostname of the Session Server unit as per the /etc/hosts file. Example: cablab.ss.unit0
Unit Number	0 or 1	An integer indicating which Unit this log applies to.
Unit Activity	alphabetic	Specifies the activity state of the SST unit in question. Possible values: ACTIVE or INACTIVE.
Result	alphabetic	Indicates the result of the action taken. Example: Passed
Initiator	alphanumeric	Indicates how the action was initiated. Example: Manual

Action

Monitor the completion of halt on the affected unit.

Associated OM registers

This log report has no associated OM registers.

Additional information

ATTENTION

Halting the last unit leaves the Session Server platform in a total server outage.

The following is an example of log report XTS678:

```
cablab      XTS678 JAN27 01:59:51 2534 INFO Halt Initiated
            Component Id: cablab.ss.unit1
            Time: Jan 27 01:59:51 2006
            Unit Number : 1, ACTIVE
            Description : Result: Passed, Initiator: Manual;
```

XTS679

Log report XTS679 is generated when the **halt mate** command is executed on the Session Server Trunks platform. The **halt mate** command stops operation of the standby unit.

Format

The format for log report XTS679 is as follows:

```
<OFFICE>      XTS679 MMMDD hh:mm:ss <sequence number> INFO Halt Mate Initiated
Component Id: <SST unit hostname>
Time: Mmm DD hh:mm:ss YYYY
Unit Number : <Unit Number>, <Unit Activity>
Description : Result: <Result>, Initiator: <Initiator>;
```

Selected field descriptions

The following table explains selected fields in the log report.

Event / Error	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.
SST unit hostname	alphanumeric	The hostname of the Session Server unit as per the /etc/hosts file. Example: cablab.ss.unit0
Unit Number	0 or 1	An integer indicating which Unit this log applies to.
Unit Activity	alphabetic	Specifies the activity state of the SST unit in question. Possible values: ACTIVE or INACTIVE.
Result	alphabetic	Indicates the result of the action taken. Example: Passed
Initiator	alphanumeric	Indicates how the action was initiated. Example: Manual

Action

Monitor the completion of halt on the affected unit.

Associated OM registers

This log report has no associated OM registers.

Additional information

ATTENTION

Execution of the halt mate command leaves the Session Server platform without a standby unit until the affected mate unit returns to service.

ATTENTION

Prolonged operation in simplex mode is not recommended. Encountering a single failure on the active unit could lead to a service outage.

The following is an example of log report XTS679:

```
cablab      XTS679 JAN27 01:50:34 2421 INFO Halt Mate Initiated
Component Id: cablab.ss.unit1
Time: Jan 27 01:50:34 2006
Unit Number : 1, ACTIVE
Description : Result: Passed, Initiator: Manual;
```

XTS682

Log report XTS682 is written by the NGCL operating system when a sensor alarm for the server chassis is cleared.

Format

The format for log report XTS682 when Session Server Trunks is configured to send its alarms northbound via SNMP to IEMS is as follows:

```
<OFFICE>      XTS682 MMMDD hh:mm:ss <sequence number> INFO Cleared
Location: <SST unit Display Name>;<SST unit IP address>
Notification Id: <NotificationID>
State: Cleared
Time: Mmm DD hh:mm:ss YYYY
Component Id: <SST unit hostname>
Description: Chassis sensor alarm raised. <# sensors> sensor are
reporting failures.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
severity	* for minor, ** for major, *** for critical	Indicates the severity of the event based on the number of asterisks.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.
SST unit Display Name	text string	The name of the Session Server Unit as per the Display Name in the IEMS GUI. For example, RTP0_SST1-Unit-0
SST unit IP address	IPv4 IP address	The IP address of the Session Server Unit. For example, 172.18.164.19
SST unit hostname	text string	The hostname of the Session Server unit provided in its /etc/hosts file. For example: ngss0

Field	Value	Description
NotificationID	integer	An integer which can be used to uniquely correlate this alarm's raise and clear for this Session Server unit.
# sensors	integer	The number of sensors reporting a failure.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

XTS683

Log report XTS683 is written by the NGCL operating system when a sensor alarm for a power supply module is cleared.

Format

The format for log report XTS683 when Session Server Trunks is configured to send its alarms northbound via SNMP to IEMS is as follows:

```
<OFFICE>      XTS683 MMMDD hh:mm:ss <sequence number> INFO Cleared
Location: <SST unit Display Name>;<SST unit IP address>
Notification Id: <NotificationID>
State: Cleared
Time: Mmm DD hh:mm:ss YYYY
Component Id: <SST unit hostname>
Description: Power supply condition cleared. Module A : Ok.
Module B : Ok
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	A string indicating the office that generated the log report.
severity	* for minor, ** for major, *** for critical	Indicates the severity of the event based on the number of asterisks.
sequence number	0000-9999	Four-digit sequence number which can be used for lost log detection.
SST unit Display Name	text string	The name of the Session Server Unit as per the Display Name in the IEMS GUI. For example, RTPO_SST1-Unit-0
SST unit IP address	IPv4 IP address	The IP address of the Session Server Unit. For example, 172.18.164.19
SST unit hostname	text string	The hostname of the Session Server unit provided in its /etc/hosts file. For example: ngss0

Field	Value	Description
NotificationID	integer	An integer which can be used to uniquely correlate this alarm's raise and clear for this Session Server unit.
# sensors	integer	The number of sensors reporting a failure.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires 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.

SPCM300

Log report [SPCM300](#) is a Policy Controller Maintenance Trouble information log. It is generated by the Policy Controller 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 Policy Controller application generates log report [SPCM300](#) in addition to raising the [SPCM300](#) alarm.

Format

The format for log report [SPCM300](#) is as follows:

```
Apr 6 13:24:47 SPC6-Unit1 spcappmtc: SPCM300 NONE TBL SPC Application
Maintenance Trouble
{Reason Text : 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	spcappmtc	Identifies the NGCL or application process unit that generates the report
Log Number	SPCM300	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	SPC 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 Policy Controller CallP message send failure
 - Been Terminating too long. Timer Expired.
 - SAM Wait Timer Messaging Timeout
 - SAM/Policy Controller CallP Audit Messaging Timeout
 - Failed to set the Policy Controller Application state
 - Policy Controller Application process death
 - Failed to start the Policy Controller Application process
 - Failed to set a timer
 - Policy Controller CallP created, but not in the requested state
 - Policy Controller CallP created, but failed to reply to SAM
 - Policy Controller CallP on the Inactive failed to respond to a request

- Policy Controller 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 Policy Controller CallP response
- Swact Precheck Failed due to failure to notify Policy Controller CallP
- Swact Precheck Failed due to timeout waiting on Policy Controller CallP response
- Swact PreSwact Failed due to failure received in Policy Controller CallP response
- Swact PreSwact Failed due to failure to notify Policy Controller CallP
- Swact PreSwact Failed due to timeout waiting on Policy Controller CallP response
- Swact AbortSwact Failed due to failure received in Policy Controller CallP response
- Swact AbortSwact Failed due to failure to notify Policy Controller CallP
- Swact AbortSwact Failed due to timeout waiting on Policy Controller CallP response
- Swact PostSwact Failed due to failure received in Policy Controller CallP response
- Swact PostSwact Failed due to failure to notify Policy Controller CallP
- Swact PostSwact Failed due to timeout waiting on Policy Controller CallP response

- Disable PreCheck Failed due to failure received in Policy Controller CallP response
- Disable PreCheck Failed due to timeout waiting on Policy Controller CallP response
- Disable PreDisable Failed due to failure received in Policy Controller CallP response
- Disable PreDisable Failed due to timeout waiting on Policy Controller CallP response
- Disable AbortDisable Failed due to failure received in Policy Controller CallP response
- Disable AbortDisable Failed due to timeout waiting on Policy Controller CallP response
- Swact PreSwact Failed due to failure to notify Policy Controller CallP
- Disable PreDisable Failed due to failure received from the mate SAM
- Disable PreDisable Failed due to failure to notify Policy Controller 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 Policy Controller 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 Policy Controller 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 Policy Controller 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

SPCM302

Log [SPCM302](#) is generated by a major alarm that is raised when the Policy Controller platform that the Policy Controller Application is running on is in a duplex configuration with both units in an enabled operational state, and the Policy Controller application state goes out of sync between the two Policy Controller units.

This alarm is cleared if the Policy Controller application state becomes sync'ed between the two Policy Controller units and the alarm is cleared.

Format

The format for log report [SPCM302](#) is as follows:

```
Dec 22 16:20:24 PV-SPC6-0 alarmd: SPCM302 MAJOR TBL NGSS App Maintenance  
Sync Trouble Alarm : NCGL=PV-SPC6-0;Unit=0; SPC Application Mtc Out  
Of Sync
```

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	SPCM302	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
Label	NGSS Maintenance Trouble Alarm	Title label for the log

Field	Value	Description
DeviceInfo	Alphanumeric	Info that specifies the device to which the alarm pertains
AlarmRaiseLowerText	Alphanumeric	Text indicating whether the Policy Controller Application Mtc Out Of Sync alarm has been raised or cleared

Action

The Policy Controller application should attempt to sync itself automatically every 30 seconds. If there 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 *Policy Controller Security and Administration NTP, NN10434-611*:

- Perform procedure *Lock the Policy Controller application*
- Perform procedure *Suspend the Policy Controller application*
- Perform procedure *Unsuspend the Policy Controller application*
- Perform procedure *Unlock the Policy Controller 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.

SPCM500

Log report [SPCM500](#) 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 Policy Controller, 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 Policy Controller application generates log report [SPCM500](#) 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 [SPCM500](#) is as follows:

```
Feb 4 11:28:22 spc6-Unit1 spcappmtc: SPCM500 NONE INFO SPC Application
Maintenance State Change [Administrative : Locked -> Locked ]
[Operational : Disabled -> Enabled ] [Control : Suspended -> Not
Suspended ] [Procedural : Not Terminating -> Not Terminating] [User
Requested : No] [Reason : System originated change of state] [Web User
ID : ]
```

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
Process Name	spcappmtc	Identifies the NGCL or application process unit that generates the report

Field	Value	Description
Log Number	SPCM500	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	SPC Maintenance State Change	Title label for the log
Description	Alphanumeric	Detailed description of the trouble or activity; see section: Additional information on page 617

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 *Policy Controller Security and Administration NTP, NNxxxxx-611* for information about login IDs and user IDs and authorization categories

SPCP301

Log report [SPCP301](#) indicates that the Policy Controller application server signaling interface has a communication failure.

Format

The format for log report [SPCP301](#) is as follows:

```
Apr 15 16:12:13 spc1 alarmd: SPCP301 MAJOR TBL AppServer Signaling  
Communication Failure NCGL=spc1;Unit=0;SPCP AppServer 47.153.178.146  
Signaling Communication Failure
```

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	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP301	The component prefix and number of the log
Severity	MAJOR	The log severity (may be related to alarm severity)
Event Type	TBL	This is an informational log
Label	AppServer Signaling Communication Failure	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

Check the application server status and the link to the application server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCM301

Log report [SPCM301](#) generated when its associated critical alarm is raised because the Policy Controller Application has transitioned to a state that indicates it should be in-service, but is actually not, while the active Policy Controller unit running the Policy Controller 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 Policy Controller application is in this state.

The Policy Controller application generates log report [SPCM301](#) in addition to raising or clearing the alarm.

Format

The format for log report [SPCM301](#) is as follows:

```
Dec 22 16:20:24 PV-SPC6-0 alarmd: SPCM301 CRIT TBL NGSS App Maintenance  
Trouble Alarm : NCGL=PV-SPC6-0;Unit=0; SPC Application System Busy
```

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	SPCM301	The component prefix and number of the log

Field	Value	Description
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	NGSS 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 Policy Controller Application System Busy alarm has been raised or cleared

Action

When the Policy Controller Application transitions out of this state (automatically or manually), this alarm is lowered. It is also lowered if the Policy Controller 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 *Policy Controller Security and Administration NTP, NNxxxxx-611*:

- Perform procedure *Lock the Policy Controller application*
- Perform procedure *Unsuspend the Policy Controller application*
- Perform procedure *Unlock the Policy Controller 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.

SPCP302

Log report [SPCP302](#) indicates that the Policy Controller has lost database connection.

Format

The format for log report [SPCP302](#) is as follows:

```
Apr 13 12:13:27 spc1 alarmd: SPCP302 CRIT TBL No Database Connection  
NCGL=spc1;Unit=0;SPCP SPC Processing 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	SPCP302	The component prefix and number of the log
Severity	CRIT	The log severity (may be related to alarm severity)
Event Type	TBL	This is an informational log
Label	No Database Connection	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP303

Log report [SPCP303](#) indicates that the Application server request failure ratio exceeds the predefined threshold value.

Format

The format for log report [SPCP303](#) is as follows:

```
Apr 13 12:23:43 spc1 alarmd: SPCP303 MINOR TBL CAC Request Mass Failure
NCGL=spc1;Unit=0;SPCP CAC Request Failure Exceed Threshold
```

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	SPCP303	The component prefix and number of the log
Severity	MINOR	The log severity (may be related to alarm severity)
Event Type	TBL	This is an informational log
Label	CAC Request Mass Failure	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP304

Log report [SPCP304](#) indicates that the Policy Controller Endpoint Number exceeds the Endpoint Block Size.

Format

The format for log report [SPCP304](#) is as follows:

```
Apr 13 17:26:02 spc1 alarmd: SPCP304 CRIT TBL Exceed Endpoint Block Size
NCGL=spc1;Unit=0;SPCP Endpoint Number Exceed Endpoint Block Size
```

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	SPCP304	The component prefix and number of the log
Severity	CRIT	The log severity (may be related to alarm severity)
Event Type	TBL	This is an informational log
Label	Exceed Endpoint Block Size	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

Obtain a new license to enlarge the endpoint number supported

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP305

Log report [SPCP305](#) indicates that the Policy Controller Endpoint Number exceeds the Endpoint Block Warning Size.

Format

The format for log report [SPCP305](#) is as follows:

```
Apr 14 17:36:02 spc1 alarmd: SPCP305 MAJOR TBL Exceed Endpoint Block  
Warning Size NCGL=spc1;Unit=0;SPCP Endpoint Number Exceed Endpoint Block  
Warning Size
```

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	SPCP305	The component prefix and number of the log
Severity	MAJOR	The log severity (may be related to alarm severity)
Event Type	TBL	This is an informational log
Label	Exceed Endpoint Block Warning Size	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

Obtain a new license to enlarge the endpoint number supported.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP501

Log report [SPCP501](#) indicates that the Policy Controller application has started up.

Format

The format for log report [SPCP501](#) is as follows:

```
APR17 08:04:43 SPC2-Unit1 spccallp: SPCP501 NONE INFO SPC Startup  
SPC start up successfully
```

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	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP501	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	SPC Startup	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP502

Log report [SPCP502](#) indicates that the Policy Controller application has shut down.

Format

The format for log report [SPCP502](#) is as follows:

```
APR17 08:04:43 SPC1-Unit1 spccallp: SPCP501 none INFO SPC Shutdown  
SPC shut down successfully
```

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	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP502	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	SPC Shutdown	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP601

Log report [SPCP601](#) indicates that a Flow Status Audit has completed.

Format

The format for log report [SPCP601](#) is as follows:

```
APR17 08:04:43 SPC2-Unit1 spcallp: SPCP601 none INFO Audit Result  
StatusAck Message is received, Flow 256 still exists
```

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	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP601	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	Audit Result	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

SPCP602

Log report [SPCP602](#) indicates that a CAC request from the application server has been denied.

Format

The format for log report [SPCP602](#) is as follows:

```
APR17 08:04:43 SPC1-Unit1 spccallp: SPCP602 none INFO CAC Request Denied  
Commit Message: Gate 1908 from GWC 47.153.178.146 is not found in SPC
```

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	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP602	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	CAC Request Denied	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

The following OMs are pegged:

- SPC Reservation Request or SPC Commit Request
- CAC Request on Network Segment

Additional information

This log report has no additional information.

SPCP603

Log report [SPCP603](#) indicates that a the Policy Controller callp has accepted a topology change.

Format

The format for log report [SPCP603](#) is as follows:

```
APR17 08:04:43 SPC1-Unit1 spccallp: SPCP603 none INFO Topology Change  
Topology Notify AddNode [NZID: 2] successfully
```

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	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP603	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	Topology Change	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

None

Additional information

This log report has no additional information.

SPCP604

Log report [SPCP604](#) indicates that callP has detected that the Ingress Id of the Network Segment sent in a GateSet message from the GWC is not present in the Policy Controller database. This is an indication that there could be a topology mismatch between the Policy Controller and the GWC/SESM. A summary of the requested problem is included in the free text portion of the report description field.

Format

The format for log report [SPCP604](#) is as follows:

```
APR17 08:04:43 SPC1-Unit1 spccallp: SPCP604 none INFO Topology Mismatch  
Reserve Message: Network Zone 6 from GWC 47.142.130.104 does not exist  
in SPC Topology
```

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	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	SPCP604	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	Topology Mismatch	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

None

Additional information

This log report has no additional information.

TPM301

Log report [TPM301](#) indicates that the Topology Manager has lost database connection.

Format

The format for log report [TPM301](#) is as follows:

```
Apr 14 12:01:59 spc1 alarmd: TPM301 CRIT TBL No Database Connection
NCGL=spc1;Unit=0;TPM Topology Manager 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	TPM301	The component prefix and number of the log
Severity	CRIT	The log severity (may be related to alarm severity)
Event Type	TBL	This is an informational log
Label	No Database Connection	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

TPM501

Log report [TPM501](#) indicates that the Topology Manager application has started up.

Format

The format for log report [TPM501](#) is as follows:

```
APR17 08:04:43 SPC2-Unit1 spctm: TPM501 none INFO TopologyManager startup  
Server Startup
```

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	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	TPM501	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	Topology Manager startup	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

None

Additional information

This log report has no additional information.

TPM502

Log report [TPM502](#) indicates that the Topology Manager application has shut down.

Format

The format for log report [TPM502](#) is as follows:

```
APR17 08:04:43 SPC2-Unit1 spctm: TPM502 none INFO TopologyManager shutdown  
server will exit after receiving RESTART command or signal.
```

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	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	TPM502	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	Topology Manager shutdown	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

None

Additional information

This log report has no additional information.

TPM601

Log report [TPM601](#) indicates that the Topology Manager application has accepted a topology change. A summary of the requested change is included in the free text portion of the report description field.

Format

The format for log report [TPM601](#) is as follows:

```
APR17 08:04:43 SPC2-Unit1 spctm: TPM601 none INFO Topology Change
User(mtc) add NetworkZone(NZID:3 Name:test.1) 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	spccallp	Identifies the NGCL or application process unit that generates the report
Log Number	TPM601	The component prefix and number of the log
Severity	None	The log severity (may be related to alarm severity)
Event Type	INFO	This is an informational log
Label	Topology Change	Title label for the log
Description	Alphanumeric	Text indicating the reason for log generation

Action

None

Associated OM registers

None

Additional information

This log report has no additional information.

RTP101

Log report RTP101 indicates that difficulties (for example, network communication problems, software issues) are encountered when attempting initial communication to setup the Media Blade specified by Blade Name (\$1).

Once set, this alarm condition is checked whenever the RTP Media Portal receives a request for a new connection, and when a timer activated event audits the communication channel with the Media Blades. If communication to a Media Blade fails, or network interface carrier sense fails, then this alarm is generated.

Format

The format for log report RTP101 is as follows:

```
RTP101 SEP21 16:07:34 1835 FLT  Fault
      Location: 47.142.85.137
      Notification Id: 83
      State: Raised
      Category: communications
      Cause: communicationsSubsystemFailure
      Time: Sep 21 16:07:34 2004
      Component Id: Site=MgmtSite;Server=RTP-
prt;System.Sites.MgmtSite.Servers.
      RTPportal0a.Services.bladerun-
ner.BladeRunner_UDP_Factory.blade2_Service Alarm
Specific Problem: RTP;101
Description: severity=CRITICAL;probableCause=com-
munications subsystem failure; addedText=$1
experienced the following problem:
Problem allocating $2 ports for this blade
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	blade1-blade16	Name of the Media Blade experiencing the problem
\$2	Integer	This is the number of media ports configured for the specified Media Blade

Action

Ensure network connectivity between the host and blade, or network connectivity on its other interfaces (link LED(s) lit on blade card). Verify that the Media Blade software is running (Telnet to the suspect Media Blade).

Contact your next level of support

Associated OM registers

RTPMPAvailableBladesMeter (Integer): Meter showing number of blades available to provide service.

Additional information

This log report requires no additional information.

RTP102

Log report RTP102 indicates when an OutOfServiceAlarm is raised. This can occur when a timer-driven event checks availability of currently configured Media Blades. If the full set of configured Media Blades are not available to provide service then this alarm is raised.

Format

The format for log report RTP102 is as follows:

```
RTP102 SEP21 16:07:34 1836 FLT  Fault
      Location: 47.142.85.137
      Notification Id: 84
      State: Raised
      Category: communications
      Cause: resourceAtOrNearingCapacity
      Time: Sep 21 16:07:34 2004
      Component Id: Site=MgmtSite;Server=RTP-
prt;System.Sites.MgmtSite.Servers.
      RTPportal0a.Services.bladerunner.
BladeRunner_UDP_Factory.
RTP_Media_Portal_OutOfServiceAlarm
Specific Problem: RTP;102
Description: severity=MAJOR;probable-
Cause=resource at or nearing capacity;
addedText=Portal has $1 out of $2 blades out of
service;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Integer	The number of configured Media Blades that are not available to provide service
\$2	Integer	The total number of configured Media Blades

Action

Ensure network connectivity between the host and blade, or network connectivity on its other interfaces (link LED is lit on the blade card).

Associated OM registers

RTPMPAvailableBladesMeter (Integer): Meter showing number of blades available to provide service.

Additional information

This log report requires no additional information.

RTP103

Log report RTP103 indicates when a timer-driven event checks the percentage of the configured media ports that are in use and then determines that the current usage level exceeds a configured threshold.

Format

The format for log report 103 is as follows:

```
RTP103 SEP17 15:57:20 9499 FLT  Fault
      Location: 47.142.85.137
      Notification Id: 181
      State: Raised
      Category: communications
      Cause: resourceAtOrNearingCapacity
      Time: Sep 17 15:57:20 2004
      Component Id: Site=MgmtSite;Server=RTP-
prt;System.Sites.MgmtSite.Servers.
      RTPportal0a.Services.bladerun-
ner.BladeRunner_UDP_Factory.PortUsageAlarm
      Specific Problem: RTP;103
      Description: severity=MINOR;probableCause=
resource at or nearing capacity
addedText=Port usage alarm shows $1 ports in use.
There are $2 available ports out of the $3
originally allocated.;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Percent	The percentage of configured media ports that are in use on this RTP Media Portal

Field	Value	Description
\$2	Integer	The number of media ports available to service new session requests
\$3	Integer	The total number of media ports configured on the RTP Media Portal

Action

Ensure that the configured capacity limits (the “ports” configuration parameter) provide adequate capacity to handle session load. This alarm is cleared once occupancy falls below the configured onset threshold.

Contact your next level of support.

Associated OM registers

RTPMPPortUsageMeter (Integer): Meter showing number of ports in use.

Additional information

This log report requires no additional information.

RTP104

Log report RTP104 indicates when a timer-driven event detects a failed status on one of the available host network interfaces. (Note: If both host network interfaces are failed, this alarm will not be displayed because communications with the host card will be lost).

Format

The format for log report RTP104 is as follows:

```
RTP104 SEP21 16:08:02 1865 FLT Fault
      Location: 47.142.85.137
      Notification Id: 94
      State: Raised
      Category: communications
      Cause: communicationsSubsystemFailure
      Time: Sep 21 16:08:02 2004
      Component Id: Site=MgmtSite;Server=RTP-
prt;System.Sites.MgmtSite.Servers.
      RTPportal0a.Services.bladerunner.
BladeRunner_UDP_Factory.HostInterfaceAlarm
Specific Problem: RTP;104
Description: severity=MAJOR;
probableCause=communications subsystem failure
addedText=Portal host shows $1 interface(s)
is(are) down: $2;
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Integer	The number of interfaces experiencing problems
\$2	Integer Name	Listing of interfaces experiencing problems (for example, eth0, eth1)

Action

Ensure network connectivity. Verify interfaces have a good connection to the network (link LED is lit on the host card).

Ensure that IP Failover functionality is enabled on the RTP Media Portal. Verify the host IP failover settings were properly configured during Installation and Commissioning. Verification and configuration of these settings is performed using the "PortalConfig.pl" script on the Host.

This alarm is cleared once both host Network Interfaces exhibit no communications problems.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

RTP105

Log report RTP105 indicates a lost connection with the Last Media Portal.

Format

The format for log report RTP105 is as follows:

```
RTP105 SEP22 08:33:21 2149 FLT Fault
      Location: 47.142.85.137
      Notification Id: 2659
      State: Raised
      Category: communications
      Cause: communicationsSubsystemFailure
      Time: Sep 22 08:33:21 2004
      Component Id: Site=MgmtSite;Server=app2;
System.Sites.MgmtSite.Servers.AppSvr2.
Services.appsvr.BR_Factory.connectionState
Specific Problem: RTP;105
Description: severity=CRITICAL;
probableCause=communications subsystem failure;
addedText=Communication Error : {alarmText};
```

Selected field descriptions

This log report has no selected fields.

Action

Ensure the referenced Media Portal is functional. If not, user may be required to restart the Media Portal.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

RTP106

Log report RTP106 indicates when communication problems (for example, network difficulties) are encountered when attempting to communicate with the Media Blade specified by Blade Name (\$1).

Format

The format for log report RTP106 is as follows:

```
$1 experienced the following problem: Communica-  
tion problem between the host and blade
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Blade1-Blade16	Blade name

Action

Ensure network connectivity between the host and blade, or network connectivity on its other interfaces (link LED(s) lit blade card).

Contact your next level of support.

Associated OM registers

RTPMPAvailableBladesMeter (Integer) - Meter showing number of blades available to provide service.

RTPMPActiveBladesMeter (Integer) - Meter showing number of blades with active connections.

Additional information

This log report requires no additional information.

RTP107

Log report RTP107 indicates when link issues (for example, carrier sense fails) are encountered when attempting to communicate over a problem interface (specified by Interface Name \$2) on the identified Media Blade (specified by Blade Name \$1).

Once set, this alarm condition is checked periodically to determine if the issue is resolved.

Format

The format for log report RTP107 is as follows:

```
$1 experienced the following problem: $2 is showing  
a missing link carrier status.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Blade1-Blade16	Blade name
\$2	eth0-eth1	Network Interface Name

Action

Ensure network connectivity between the host and blade, or network connectivity on its other interfaces (link LED(s) lit on the blade card).

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

RTP108

Log report RTP108 indicates when a Session Manager does not receive responses to requests made to the only available RTP Media Portal in its media resource pool.

When this condition arises, the Session Manager removes this RTP Media Portal from its resource pool. This impacts the Session Manager's ability to process calls that require a RTP Media Portal.

The condition clears when the Session Manager detects a resumption in communications with the affected RTP Media Portal. This causes the Session Manager to add the RTP Media Portal back into its media resource pool.

Format

The format for log report RTP108 is as follows:

```
Communication Error: Lost connection with LAST  
Media Portal at IPAddress: $1.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Dotted IP Address	IP address for control channel messaging (MPCP) that identifies this specific RTP Media Portal

Action

Ensure the referenced RTP Media Portal is accessible over the network and that it is functional.

If it is not functional then you may need to restart the Media Portal. Contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

RTP109

Log report RTP109 indicates when a Session Manager does not receive responses to requests made to an available RTP Media Portal in its media resource pool.

Format

The format for log report RTP109 is as follows:

```
Communication Error: Lost connection with Media  
Portal at IPAddress: $1.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	IP Address	IP address for control channel messaging (MPCP) that identifies this specific RTP Media Portal

Action

Ensure that the referenced RTP Media Portal is accessible over the network and that it is functional.

If it is not functional then you may need to restart the RTP Media Portal. Contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

RTP110

Log report RTP110 indicates a recovery of the RTP Media Portal Host application upon discovery of pre-existing media sessions on a Media Blade.

Format

The format for log report RTP110 is as follows:

```
$1 recovery initiated after comm failure with $2  
pre-existing connections.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Dotted IP Address	IP address that identifies the specific Media Blade recovered
\$2	Integer	Number of pre-existing connections found to be in existence on this Media Blade

Action

None.

Associated OM registers

PreExistingConnections (Integer) - Meter showing the total number of connections the Host found during host recovery.

RecoveryModeFailures (Integer) - Meter showing the number of Media Blades to which control can not be re-established during host recovery.

NumConnsRecovered (Integer) - Meter showing total number of connections reconstructed during last host recovery action.

<bladex>RecoveryPreExistingConns (Integer) - Meter showing the number of connections discovered during the last blade recovery action.

<bladex>RecoveryNumConnsRecovered (Integer) - Meter showing the number of connections reconstructed during last blade recovery action.

Additional information

This log report requires no additional information.

RTP111

Log report RTP111 indicates that the Host was able to re-establish communication with a subtending Media Blade. This log also reports the number of connections over which the Host was able to restore control.

Format

The format for log report RTP111 is as follows:

```
$1 recovery completed after comm failure with $2
connections recovered.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Dotted IP Address	IP address that identifies the specific Media Blade recovered
\$2	Integer	Number of pre-existing connections recovered on this Media Blade

Action

None.

Associated OM registers

PreExistingConnections (Integer) - Meter showing the total number of connections the Host found during host recovery.

RecoveryModeFailures (Integer) - Meter showing the number of Media Blades to which control can not be re-established during host recovery.

NumConnsRecovered (Integer) - Meter showing total number of connections reconstructed during last host recovery action.

<bladex>RecoveryPreExistingConns (Integer) - Meter showing the number of connections discovered during the last blade recovery

action.

<bladex>RecoveryNumConnsRecovered (Integer) - Meter showing the number of connections reconstructed during last blade recovery action.

Additional information

This log report requires no additional information.

RTP112

Log report RTP112 indicates the start of the RTP Media Portal Host application recovery process. This process attempts to reconstitute control over all pre-existing media sessions.

Format

The format for log report RTP112 is as follows:

```
Host Recovery Mode initiated on $1 with $2
pre-existing connections.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Dotted IP Address	IP address that identifies the specific RTP Media Portal undergoing recovery
\$2	Integer	Number of pre-existing connections recovered on this RTP Media Portal

Action

None.

Associated OM registers

PreExistingConnections (Integer) - Meter showing the total number of connections the Host found during host recovery.

RecoveryModeFailures (Integer) - Meter showing the number of Media Blades to which control can not be re-established during host recovery.

NumConnsRecovered (Integer) - Meter showing total number of connections reconstructed during last host recovery action.

<bladex>RecoveryPreExistingConns (Integer) - Meter showing the number of connections discovered during the last blade recovery action.

<bladex>RecoveryNumConnsRecovered (Integer) - Meter showing the number of connections reconstructed during last blade recovery action.

Additional information

This log report requires no additional information.

RTP113

Log report RTP113 indicates the number of connections recovered on a specific Media Blade. This log is produced during the Host recovery process.

Format

The format for log report RTP113 is as follows:

```
Host Recovery Mode completed on $1 showing $2 connections are in use.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Dotted IP Address	IP address that identifies the specific Media Blade recovered
\$2	Integer	Number of pre-existing connections recovered on this Media Blade

Action

None.

Associated OM registers

PreExistingConnections (Integer) - Meter showing the total number of connections the Host found during host recovery.

RecoveryModeFailures (Integer) - Meter showing the number of Media Blades to which control can not be re-established during host recovery.

NumConnsRecovered (Integer) - Meter showing total number of connections reconstructed during last host recovery action.

<bladex>RecoveryPreExistingConns (Integer) - Meter showing the number of connections discovered during the last blade recovery action.

<bladex>RecoveryNumConnsRecovered (Integer) - Meter showing the number of connections reconstructed during last blade recovery action.

Additional information

This log report requires no additional information.

RTP114

Log report RTP114 indicates the number of Media Blades with which the Host failed to establish communications. This log is produced during the Host recovery process.

Format

The format for log report RTP114 is as follows:

```
Host Recovery Mode - failed to reestablish comm  
with $1 blades.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Integer	Reports the number of Media Blades that could not be recovered

Action

No action is required, as a separate alarm is raised for each Media Blade which does not respond.

Associated OM registers

PreExistingConnections (Integer) - Meter showing the total number of connections the Host found during host recovery.

RecoveryModeFailures (Integer) - Meter showing the number of Media Blades to which control can not be re-established during host recovery.

NumConnsRecovered (Integer) - Meter showing total number of connections reconstructed during last host recovery action.

<bladex>RecoveryPreExistingConns (Integer) - Meter showing the number of connections discovered during the last blade recovery action.

<bladex>RecoveryNumConnsRecovered (Integer) - Meter showing

the number of connections reconstructed during last blade recovery action.

Additional information

This log report requires no additional information.

RTP118

Log report RTP118 indicates when an attempt to dispatch an outgoing signal fails.

Format

The format for log report RTP118 is as follows:

```
Unable to dispatch outgoing signal.
```

Selected field descriptions

Not applicable.

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.

RTP200

Log report RTP200 indicates when the RTP Media Portal initializes in a state in which no Media Blade information has been configured.

Format

The format for log report RTP200 is as follows:

```
No Media blades configured.
```

Selected field descriptions

Not applicable.

Action

The RTP Media Portal requires at least one Media Blade in order to provide service. Configure a Media Blade from the System Management Console, and install the Media Blade in order to successfully activate the RTP Media Portal.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

RTP201

Log report RTP201 indicates when a request for reboot of the RTP Media Portal fails due to a software exception.

Format

The format for log report RTP201 is as follows:

```
Unable to reboot due to IO Exception.
```

Selected field descriptions

Not applicable.

Action

Report this log to 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.

RTP202

Log report RTP202 indicates when a request for service is made from an unknown proxy - one which is not configured for this RTP Media Portal.

Format

The format for log report RTP202 is as follows:

```
Unknown proxy - no session established with proxy  
$1.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Dotted IP Address	IP address that identifies the source of the received control message (the IP address of the unknown proxy)

Action

Investigate the source proxy to ensure it is a valid network node. Then either update the configuration to include this node, or secure the control plane.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

RTP203

Log report RTP203 indicates an attempt to send a registration message to one of the configured proxies fails.

Format

The format for log report RTP203 is as follows:

```
Unable to register with proxy $1.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Dotted IP Address	The configured IP address for a proxy

Action

Verify the configuration data represents an existing proxy. Verify that the affected proxy exists and is reachable in the network.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

RTP204

Log report RTP204 indicates that an audit is performed over the Connection Map and a particular connection is not found on the corresponding Media Blade.

Format

The format for log report RTP204 is as follows:

```
Connection not found on $1, endPointID = $2, callID= $3.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	blade1-blade6	Identifies the Media Blade on which the missing connection is expected to be found
\$2	Integer	Identifies the endPointID associated with the missing connection
\$3	Integer	Identifies the CallID associated with the missing connection

Action

Report this log to your next level of support.

Associated OM registers

TotalNumberConnectionsRemovedCount (Integer) - Counter, tracks the total number of connections removed across all audit cycles.

ConnsRemovedLatestCycle (Integer) - Counter, tracks the total number of connections removed (recovered) by the latest idle stream audit cycle.

Additional information

This log report requires no additional information.

RTP205

Log report RTP205 indicates that an audit is performed over the Connection Map and a particular connection is unexpectedly found to be idle on the corresponding Media Blade. The invalidly idle connection is identified in this log.

Format

The format for log report RTP205 is as follows:

```
Idle connection on $1, endPointID = $2, callID = $3.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	blade1-blade6	Identifies the Media Blade on which the mismatched connection is found
\$2	Integer	Identifies the endPointID associated with the mismatched connection
\$3	Integer	Identifies the CallID associated with the mismatched connection

Action

None.

Associated OM registers

TotalNumberConnectionsRemovedCount (Integer) - Counter, tracks the total number of connections removed across all audit cycles.

ConnsRemovedLatestCycle (Integer) - Counter, tracks the total number of connections removed (recovered) by the latest idle stream audit cycle.

Additional information

This log report requires no additional information.

RTP206

Log report RTP206 indicates when an audit is performed over the Connection Map and a particular connection is found on the corresponding Media Blade which exceeds the Long Idle Duration threshold.

Format

The format for log report RTP206 is as follows:

```
Connection on $1, endPointID = $2, callID = $3  
exceeds Long Idle Duration.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	blade1-blade6	Identifies the Media Blade on which the Long Idle Duration connection is found
\$2	Integer	Identifies the endPointID associated with the Long Idle Duration connection
\$3	Integer	Identifies the CallID associated with the Long Idle Duration connection

Action

No action is required (unless this log is generated excessively in which case the Long Idle Duration period could be configured for a longer interval).

Associated OM registers

TotalNumberConnectionsRemovedCount (Integer) - Counter, tracks the total number of connections removed across all audit cycles.

ConnsRemovedLatestCycle (Integer) - Counter, tracks the total number of connections removed (recovered) by the latest idle stream audit cycle.

Additional information

This log report requires no additional information.

RTP207

Log report RTP207 indicates when an audit is performed over the Connection Map and a particular connection is found on the corresponding Media Blade which exceeds the Long Call Duration threshold.

Format

The format for log report RTP207 is as follows:

```
Connection on $1, endPointID = $2, callID = $3  
exceeds Long Call Duration.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	blade1-blade6	Identifies the Media Blade on which the Long Call Duration connection is found
\$2	Integer	Identifies the endPointID associated with the Long Call Duration connection
\$3	Integer	Identifies the CallID associated with the Long Call Duration connection

Action

No action is required (unless this log is generated excessively in which case the Long Call Duration period could be configured for a longer interval).

Associated OM registers

TotalNumberConnectionsRemovedCount (Integer) - Counter, tracks the total number of connections removed across all audit cycles.

ConnsRemovedLatestCycle (Integer) - Counter, tracks the total number of connections removed (recovered) by the latest idle stream audit cycle.

Additional information

This log report requires no additional information.

RTP208

Log report RTP208 indicates a failed attempt to access the interface status file (establish a file handle, read from it, or it does not exist).

Format

The format for log report RTP208 is as follows:

```
Host Interface Status file problem  
(/proc/net/bonding/bond0) .
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
N/A	N/A	N/A

Action

Verify the host IP failover settings were properly configured during Installation and Commissioning. Verification and configuration of these settings is performed using the "PortalConfig.pl" script on the Host.

Report this log to 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.

RTP300

Log report RTP300 indicates when it is necessary for the RTP Media Portal to autonomously increase in the size of the Hash Map used to store connection information.

Format

The format for log report RTP300 is as follows:

```
Demanded exceeded configured portal Call Legs  
capacity. Number of call legs allowed was increased  
from $1to $2.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Integer	Previous Hash Map Size
\$2	Integer	New Hash Map Size

Action

This may indicate a need for additional RTP Media Portal resources.

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.

RTP301

Log report RTP301 indicates a denied request for an increase in the size of the Hash Map.

This log indicates the Hash Map has already increased in size, and prevents unbounded increases in the size of the Connection Map.

Format

The format for log report RTP301 is as follows:

```
Demand exceeded configured portal Call Legs capacity again. Please verify configured Call Legs capacity.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
N/A	N/A	N/A

Action

Report this log to 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.

RTP302

Log report RTP302 indicates a request for an increase in the size of the Hash Map fails due to some unforeseen software issue.

Format

The format for log report RTP302 is as follows:

```
Demand exceeded configured portal Call Legs capacity but failed to increase capacity from $1 to $2.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
\$1	Integer	Previous Hash Map Size
\$2	Integer	New Hash Map Size

Action

Report this log to 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.

RTP801

Log report RTP801 indicates when there is a change made to configuration data for an in-service RTP Media Portal.

The alarm is intended to highlight this data change has not been picked up by the in-service RTP Media Portal because the RTP Media Portal does not support live configuration updates. However, the configuration change is stored persistently so that it can be picked up by the RTP Media Portal on its next initialization. Until that time the run-time data and the persistently stored data are not synchronized.

Format

The format for log report RTP801 is as follows:

```
Live Update of RTP Media Portal Configuration Data
is NOT supported.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
N/A	N/A	N/A

Action

The System Property Portal.Config.BRHOME must be defined for the RTP Media Portal to operate correctly.

Contact your next level of technical support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

RTP802

Log report RTP802 indicates that the RTP Media Portal is not correctly configured.

Format

The format for log report RTP802 is as follows:

```
System Property Portal.Config.BRHOME is NOT  
defined.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
N/A	N/A	N/A

Action

The System Property Portal.Config.BRHOME must be defined for the RTP Media Portal to operate correctly.

Please contact your next level of technical support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

M3UA101

Log report M3UA101 indicates M3UA path status changes.

Format

The format for log report M3UA101 is as follows:

```
TOROONLQCA0 CM M3UA101 MAY26 19:05:10 3237 INFO Path state change  
Path = <path id> has changed to <path status>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
path id	0 to 31	Identifies the path affected by the event
path status	Path Down Path Up Path Active Path Inactive Comm Up Comm Down Cong Enter Cong Exit	Path is down Path is up, but it is not carrying traffic Path is active, and ready to carry traffic Path is inactive, and not ready to carry traffic SCTP association is up SCTP association is down SCTP association enter congestion SCTP association exit congestion

Action

Action is required whenever the path status is not active.

Do the following:

1. Check whether the network is down.
2. Check that the far end endpoint is activated.
3. Check that local endpoint is activated.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

M3UA102

Log report M3UA102 indicates M3UA pathset status changes.

Format

The format for log report M3UA102 is as follows:

```
GDNTRDGD01T  M3UA102 JUL20 08:02:09 03007 INFO Far end node state
State - <far end node status>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
far end node status	Available	Indicates pathset to far end node is available
	Unavailable	Indicates pathset to far end node is unavailable

Action

Action is required when far end node status is unavailable. Refer to M3UA101 log.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

M3UA103

Log report M3UA103 indicates M3UA protocol violation events.

Format

The format for log report M3UA103 is as follows:

```
TOROONLQCA0 CM M3UA103 MAY26 19:05:10 3136 INFO Protocol violation
Reason : <reason test>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<reason text>		Indicates the reason of protocol violation

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.

M3UA104

Log report M3UA104 indicates invalid sctp association establish request.

Format

The format for log report M3UA104 is as follows:

```
TOROONLQCA0 CM M3UA104 MAY26 19:05:10 3136 INFO Invalid Association  
Association : <source port>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<source port>		Indicates the sctp association source port

Action

Do the following:

1. Find which remote endpoint is requesting association establish according to log source port.
2. Check whether path data is mismatched between USP and Core.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

M3UA105

Log report M3UA105 indicates error message received.

Format

The format for log report M3UA105 is as follows:

```
TOROONLQCA0 CM M3UA105 MAY26 19:05:10 3136 INFO Received Error Message
Reason : <error code>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<error code>	Possible error codes include: 0x01 Invalid Version 0x02 Not Used in M3UA 0x03 Unsupported Message Class 0x04 Unsupported Message Type 0x05 Unsupported Traffic Mode Type 0x06 Unexpected Message 0x07 Protocol Error 0x09 Invalid Stream Identifier 0x0d Refused - Management Blocking 0x0e ASP Identifier Required 0x0f Invalid ASP Identifier 0x10 Not Used in M3UA 0x11 Invalid Parameter Value 0x12 Parameter Field Error 0x13 Unexpected Parameter 0x14 Destination Status Unknown 0x15 Invalid Network Appearance 0x16 Missing Parameter 0x17 Not Used in M3UA 0x18 Not Used in M3UA 0x19 Invalid Routing Context 0x1a No Configured AS for ASP	Indicates the received error code

Action

Take action according to the error codes.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

M3UA106

Log report M3UA106 indicates a GWC node as an M3UA signaling link state change to USP.

Format

The format for log report M3UA106 is as follows:

```
GDNTRDGD01T M3UA106 JUL20 08:03:20 4700 INFO Node State Change
Node = <GWC node number> SS7 Signaling State = <link status>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<GWC node number>		Indicates the GWC node number affected by this event
<link status>	available	Indicates that the M3UA signaling link from the GWC to the USP is available
	unavailable	Indicates that the M3UA signaling link from the GWC to the USP is unavailable

Action

Action is required whenever the link status is unavailable

Do the following:

1. Check whether the network is down.
2. Check that the far end endpoint is activated.
3. Check that the local GWC endpoint is activated.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

M3UA107

Log report M3UA107 indicates traffic is discarded because routeset is unavailable.

Format

The format for log report M3UA107 is as follows:

```
GDNTRDGD01T M3UA107 JUL20 08:03:20 4700 INFO Traffic is discarded  
Routeset index<routeset id> is not available
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<routeset id>		Indicates the routeset index affected by this event

Action

Check whether routeset status is correct.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

M3UA108

Log report M3UA108 indicates unexpected message received.

Format

The format for log report M3UA108 is as follows:

```
GDNTRDGD01T   M3UA108 JUL20 08:03:20 4700 INFO Unexpected message
                is received
NA=<node number> Reason=<reason text>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<node number>		Indicates the node number in the m3ua message
<reason text>		Indicates the reason

Action

Do the following:

1. Check whether the data between USP and Core is mismatched.
2. Monitor network traffic if applicable.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USP398

Log report USP398 indicates an alarm raise event in a USP device.

Note: Log report USP398 is related to the Integrated Element Management Server (IEMS).

Format

The format for log report USP398 is as follows:

```
znc0s0jh * USP398 Feb17 01:09:25 0009 FLT USP Fault
Location: 47.142.87.127-Unit-0;47.142.87.127
Notification Id: 1029
State: Raised
Category: communications
Cause: communicationsSubsystemFailure
Time: FEB 17 01:09:25 2006
Component Id: USP=COMP4;Shelf=0;Slot=15;ContextID=0x1010101
Specific Problem:Log GroupID=32;Log Group=Network;Log Number=0
Description: Connectivity lost: 1 1.1.1.1.
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

USP399

Log report USP399 indicates a USP clear event.

Note: Log report USP399 is related to the Integrated Element Management Server (IEMS).

Format

The format for log report USP399 is as follows:

```
znc0s0jh USP399 Feb17 01:10:21 0011 INFO USP Fault
Location: 47.142.87.127-Unit-0;47.142.87.127
Notification Id: 1029
State: Cleared
Time: Feb 17 01:10:21 2006
Component ID: USP=COMP4;Shelf=0;Slot=15;ContextID=0x1010101
Description: netping entry deleted: 1 1.1.1.1.
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.