Copyright © 2006, Nortel Networks Nortel Networks Confidential

Carrier Voice over IP Fault Management Logs Reference Volume 2

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 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 have occurred:

- added SDM 327, 505, 627, and 630 from Volume 3
- added SDMB 360, 615, and 660 from Volume 3
- added SPM 625 and 710 from Volume 3
- moved PM703 from IW SPM to GWC
- CCA331, CCA335 (new)
- CMT303, CMT398 (new)
- CMT304 (added; was missing)
- GWC310 (deleted)
- GWC315, 318 to 322, 601, 603 to 606, 609, 702 (new)
- GWC501 to 503, 507, 600 (modified)
- GWC310 (deleted)
- PM181 (modified)
- SCPL100, 200 (new)
- VOIP800 (new)
- added NODE326 (from Vol 4)

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 2 contains the following Carrier VoIP logs by component:

- Call Agent
- CS 2000
  - CS 2000 Core Manager
  - CS 2000 Management Tools
  - Gateway Controller
  - Interworking Spectrum Peripheral Module ATM
  - Interworking Spectrum Peripheral Module Internet Protocol
  - Services Application Module
  - STORage Management
  - Carrier VoIP Server Platform Foundation Software

The tables associated with each component identify and briefly describe the logs they use. Double-click on the log identifier to see the log details.

Note: CS 2000 Core Manager logs (SDM) also apply to the Core and Billing Manager (CBM) products.

Call Agent

The following table lists the individual logs that the Call Agent generates.

Call Agent logs (Sheet 1 of 3)

Log ID	Description
CCA300	Free space in RAM is low
CCA301	CPU load average has exceeded the threshold
CCA302	Free space on the root file system is low
CCA303	One software process has terminated abnormally
CCA304	One or more of the Network File System (NFS) mounted file systems is inaccessible
CCA305	The platform software lost time synchronization to one or more Network Time Protocol (NTP) servers

Call Agent logs (Sheet 2 of 3)

Log ID	Description
CCA306	CPU utilization has exceeded a threshold
CCA309	The card has a Peripheral Component Interconnect (PCI) bus fault
CCA314	Indicates free memory for the call processing application is low
CCA315	The inactive call processing application is not ready for takeover
CCA316	The call processing application has changed state
CCA322	The inactive call processing application failed an image test.
CCA331	The Call Agent cards cannot communicate to the mate through the ethernet/fiber
CCA335	The Ethernet interface is down
CCA336	One or more Ethernet links are unable to communicate with the network
CCA340	A loss of ATM connectivity has occurred between the Message Controller card and the Message Switch (MS)
CCA344	A trouble condition has occurred on the Message Controller platform
CCA345	A loss of Ethernet connectivity has occurred on the Message Controller card
CCA351	The mate Call Agent unit is unavailable due to several CON and APL alarms
CCA352	An NFS Inactive Indicator Key (NIIKEY) file was detected in one of the /TAPE directories
CCA355	The inactive unit is jammed to prevent a Switch of Activity (SWACT)
CCA362	One or more REx tests has failed
CCA365	System REx has not started for over seven days

Call Agent logs (Sheet 3 of 3)

Log ID	Description
CCA375	The Call Agent cards in the CS 2000 - Compact are of two different hardware types
CCA380	The Call Agent card has a different committed patch file version than another card
CCA390	Indicates a trap from a Linux platform software process
CCA685	Indicates that the CCA disabled the open shortest path firs (OSPF) action in the local Ethernet Routing Switch 8600
CCA686	Indicates that the CCA enabled the open shortest path firs (OSPF) action in the local Ethernet Routing Switch 8600

CS 2000

The following table lists the individual logs that the CS 2000 generates.

CS 2000 logs (Sheet 1 of 2)

Log ID	Description
BOOT200	Indicates whether the out-of-service CEM in an MG4000 successfully loaded a bootstrap protocol (bootp) request made to the CS 2000
BOOT201	Indicate a failure of the CS 2000 to respond to one or more of the bootp requests it has received
ESA120	The CS 2000 successfully generates an MG9000 ESA data file in SFDEV
ESA121	The CS 2000 fails to generate an MG9000 ESA data file in SFDEV
SCAI304	Allows applications running on the CS 2000 to communicate with applications running on the host computer

CS 2000 logs (Sheet 2 of 2)

Log ID	Description
SCPL100	Generated when an NCAS link is established between the CS 2000 Core and the Session Server
SCPL200	Generated when an NCAS link is lost between the CS 2000 Core and the Session Server

CS 2000 Core Manager

The following table lists the individual logs that the CS 2000 Core Manager generates.

Note: CS 2000 Core Manager logs also apply to the Core and Billing Manager (CBM) products.

CS 2000 Core Manager logs (Sheet 1 of 7)

Log ID	Description
SDM267	Indicates a change in the condition of a CBM link
SDM300	Connectivity is not present on a computing module or operating company LAN
SDM301	The maintenance system detects that a logical volume is not mirrored
SDM302	The maintenance system detects that using a system resource exceeds the resource threshold
SDM303	A message indicates that a process is in trouble
SDM304	The Log Delivery application fails to reconnect to a device
SDM306	Table access software versions on the Core side and a SDM node are not compatible
SDM308	An automated incremental backup or a manual system image backup fails on an SDM node
SDM309	The maintenance system on a fault-tolerant SDM hardware detects a fault in a hardware device
SDM314	Generated when a DS512 link is reported down on the SDM

CS 2000 Core Manager logs (Sheet 2 of 7)

Log ID	Description
SDM315	The application detects corruption in the Data Dictionary on the Core during a data dictionary download
SDM317	The DCE detects a problem
SDM318	An OM report is not generated
SDM321	Generated at the start of a split-mode upgrade
SDM325	The connection to a network management component in a given domain has been lost
SDM326	Indicates that the connection was lost between the SDM and the Multiservice Data Manager (MDM) for 5-minute or 30-minute performance measurement data transfer.
SDM327	Generated when a Network Time Protocol (NTP) problem is detected
SDM330	Generated when it detects a communication problem between two mated nodes on a CBM850 HA cluster.
SDM331	Generated when a file in directory /omdata/closedNotSent is deleted by audit to make more than 50% available space in directory /omdata
SDM332	Indicates that the system audit completed with failures.
SDM334	Indicates that a fault was detected on a CBM 800 OC-3 card
SDM335	Indicates a link fault
SDM336	Generated when the core fails to respond to CBM heartbeats or, on the CBM 850, the core responds that it has been homed to another address
SDM500	The SDM node control process has restarted
SDM501	The node control process has updated the run state of the SDM to in-service (InSv)

CS 2000 Core Manager logs (Sheet 3 of 7)

Log ID	Description
SDM502	The SHA process has updated the run state of the SDM to ManB
SDM503	The SDM High Availability (SHA) process has updated the run state of the SDM node to SYSB
SDM504	The high availability (SHA) process updates the run state of the SDM node to TBL
SDM505	Generated when the SuperNode Data Manager high availability process updates the SDM run state to offline
SDM550	A change in the SDM node status occurs
SDM600	The SDM has established connectivity again
SDM601	Mirroring was re-established after a logical volume mirroring failure
SDM602	An SDM system resource threshold is within set limits
SDM603	An SDM303 alarm has been cleared
SDM604	The CM has discarded logs because it does not have enough CPU time to format them
SDM605	Indicates logs for a specific application have been lost
SDM607	Indicates when a process controller starts or restarts a process
SDM608	An I-tape or S-tape process has completed
SDM609	Indicates when the maintenance system detects a hardware device has returned to the in-service (InSv) state
SDM610	Problems with a patch application or transaction
SDM614	Generated when a DS512 link up is reported on the SDM

CS 2000 Core Manager logs (Sheet 4 of 7)

Log ID	Description
SDM615	Generated thresholded logs produced within the preceding 24 h.
SDM616	A TCP/IP connection was refused
SDM617	A DCE problem has been cleared
SDM618	The /var logical volume is 95% full
SDM619	The OM Access Server has detected a corrupt OM group during an OM Schema download
SDM620	Reports current SDM system performance data
SDM621	Generated at the end of a split-mode upgrade
SDM622	The system reaches the maximum size for a file device configured through the Logroute tool
SDM625	The connection to a Network Management component in a given domain has been re-established
SDM626	An information-only log
SDM627	Generated when a Network Time Protocol (NTP) problem is cleared
SDM630	Indicates the SDM Routine EXercise (REX) start and stop time
SDM632	Indicates that the system audit failure reported through log SDM332 has been cleared
SDM633	Indicates a change in the messaging condition of a DS512 or OC-3 link between the SDM or Core and Billing Manager 800 (CBM 800) and the message switch (MS)
SDM634	Indicates that the error condition indicated by log SDM334 has been cleared
SDM635	Indicates that the problem indicated by log SDM335 has been cleared

CS 2000 Core Manager logs (Sheet 5 of 7)

Log ID	Description
SDM636	Indicates that the core heartbeat recovered and the heartbeat alarm has been cleared
SDM650	Indicates a failed link maintenance action
SDM700	Reports a Warm, Cold or Reload restart or a norestartswact on the core
SDM739	Indicates file transfers between the FTP Client and the CORE and shows user log-ins to the CORE
SDMB300	Generated when memory allocation fails
SDMB310	Generated for communication-related problems
SDMB315	Generated for general software-related problems
SDMB316	Generated when you manually kill a billing-related process
SDMB320	Generated for backup-related problems that affect more than one file
SDMB321	Generated for backup-related problems that affect a file
SDMB350	Generated when a billing process reaches a death threshold and makes a request to restart
SDMB355	Generated for problems with disk utilization
SDMB360	Generate when it loses and cannot restore the connection to the Persistent Store System
SDMB365	Generated when a serious problem prevents a named stream from being created
SDMB366	Generated when an error condition exists on the SDM
SDMB367	Generated for selected MIB objects
SDMB370	Generated when the CDR-to-BAF conversion encounters a problem

CS 2000 Core Manager logs (Sheet 6 of 7)

Log ID	Description
SDMB375	Generated by the FTAM responder when a problem occurs during file transfer
SDMB380	Indicates the file transfer mode for the stream has an invalid value
SDMB390	Generated when schedule-related trouble occurs
SDMB400	Generated for every active stream every hour
SDMB530	Generated when there has been a change in the configuration or status of a stream
SDMB531	Generated when there is a successful configuration change for the backup volumes
SDMB550	Generated when the SBA shuts down
SDMB600	Indicates generic information for the overall billing system
SDMB610	Generated when a communications-related problem with billing has been resolved
SDMB615	Generated when a software-related error condition has been resolved
SDMB621	Generated when a new backup file is started
SDMB625	Generated when recovery is started on a backup file
SDMB650	Indicates the SBA is restarting one or more of its processes
SDMB655	Indicates file state changes and disk utilization issues
SDMB660	Generated when a problem involving communications with other SuperNode Billing Application (SBA) features is resolved
SDMB665	Indicates a software problem on the Core
SDMB670	Generated when the CDR-to-BAF conversion process uses default values to create a BAF field

CS 2000 Core Manager logs (Sheet 7 of 7)

Log ID	Description
SDMB675	Generated whenever a problem involving a file transfer is resolved
SDMB680	Generated whenever information not related to the file system or creating links needs to be communicated to the customer
SDMB690	Indicates an SBAIF alarms has cleared
SDMB691	Identifies events related to the scheduled transfer of billing files
SDMB820	Generated when a backup hits a threshold
SDMO375	Indicates that OMDD discovered a problem while performing an outbound file transfer and could not ensure that the OM report was transferred downstream.
SPM625	Generated when crossover message channels are not configured for SPMs
SPM710	Generated when the audit updates the ISDNPROT table

CS 2000 Management Tools

The following table lists the individual logs that the CS 2000 Management Tools generates.

CS 2000 Management Tools logs (Sheet 1 of 3)

Log ID	Description
CMT300	Indicates a data mismatch between the server where the SESM software is installed and the Communication Server 2000
CMT301	Indicates the CS 2000 GWC Manager cannot download data to a GWC on recovery
CMT302	Indicates that the SNMP poller on the CS 2000 Management Tools server cannot communicate with a network device

CS 2000 Management Tools logs (Sheet 2 of 3)

Log ID	Description
CMT303	Indicates that SESM has failed to get available Call Agent IP address from Core
CMT304/CMT399	Indicates that the request from the Gateway Controller (GWC) Manager to the Certificate Manager to retrieve IKE certificates has failed
CMT398	Indicates that the SESM has received a TRAP that does not contain the required info or that the ReportName and ReportNumber are not specified in the value of that info
CMT399	A log from the CMT server has cleared
CMT500	The SESM alarm system is initializing
CMT501	The SESM server application has been shut down
CMT502	The CMT alarm system cannot generate alarm event notifications
DB600	Indicates a database connection error
DB601	Indicates the database connection is closed
DB602	Indicates an invalid password
DB603	Indicates that the threshold for the maximum database sessions has been exceeded
DB604	Indicates that the threshold for the maximum database processes has been exceeded
NPM360	Indicates an alarm has been raised
NPM370	Indicates when an alarm has been cleared
NPM400	Indicates the results of an attempted apply, remove, and audit command
NPM600	Indicates when the NPM server has been started
NPM601	Relates to patch files
NPM603	Indicates problems between the database and the device

CS 2000 Management Tools logs (Sheet 3 of 3)

Log ID	Description
NPM605	Indicates a patch application or removal failed
NPM610	Provides information related to the execution of a task
NPM620	Provides information about system restarts on the GUI
NPM660	Indicates problems when a plan fails to execute
NPM680	Indicates problems when a plan is automatically executed

Gateway Controller

The following table lists the individual logs that the Gateway Controller (GWC) generates.

GWC logs (Sheet 1 of 5)

Log ID	Description
GWC300	Indicates an “Active unit disabled.” Unit Out of Service: Service is not available or Invalid GWC Profile Data
GWC301	Indicates a "Standby unit disabled." Unit Out of Service: Service is not available or Invalid GWC Profile Data
GWC302	Indicates a Major for active unit; Minor for inactive unit. "Core communication lost
GWC303	Indicates a "Mate unit communication lost." No response received to mate heartbeat messages
GWC304	Indicates a gateway has stopped responding to heartbeat
GWC305	Indicates a test alarm is generated from pmdebug interface to log in to the notilog table
GWC306	Indicates a DQoS/COPS connection failure

GWC logs (Sheet 2 of 5)

Log ID	Description
GWC307	Indicates an "Element Manager communication failure." EM indicates provisioned data mismatched in this unit, or EM is not responding, provisioned data loaded from local Flash.
GWC308	Indicates a "Flash memory error." Erase of Flash sector failed
GWC309	Indicates that "Security SAs are nearing capacity."
GWC311	Indicates a Warning. "Provisioned GWC Profile not yet activated."
GWC312	Indicates a Major (partial outage) or Critical (total outage)
GWC313	RMGC is overloaded
GWC314	Indicates a partial outage due to a failed or broken TCP/IP connection to the location recipient
GWC315	Indicates the loss of external host interface signals
GWC318	Indicates that the Gateway Controller initiated an autonomous switch of activity in an attempt to restore communication with its associated media gateways
GWC319	Indicates that the Gateway Controller (GWC) lost communication with all associated media gateways
GWC320	Indicates an IKE/IPSec processing problem
GWC321	Indicates that the auto-negotiation capability is disabled on the Ethernet Routing Switch 8600
GWC322	Indicates that the simple network management protocol message rate exceeded the recommended maximum
GWC399	Clears all other GWC logs
GWC400	An information-only log

GWC logs (Sheet 3 of 5)

Log ID	Description
GWC501	Indicates there has been a connection fault between the GWC and the gateway
GWC502	Indicates service has been restored to the referenced gateway
GWC503	Indicates the gateway has requested that service become interrupted
GWC506	An H.323 GWC unit has lost the connection to an H.323 gateway
GWC507	The connection between a GWC and an H.323 gateway has been restored
GWC600	Generates an information log for an H.323 failure
GWC601	Indicates the change of the Gateway Controller Manager IP address
GWC603	Indicates that a netfail event occurred on the gateway and it was reported to the Gateway Controller
GWC604	Indicates an internal Gateway Controller (GWC) exception. Use this log report for debugging process
GWC605	Indicates that the M3UA Application Server Process (ASP) path audit has detected all the ASP paths in the down state for ten minutes
GWC606	An information log for a Media Proxy (MP) idle or long call detection event
GWC609	Generated when the Gateway Controller detects communication issues with an in-service trunk or large capacity line gateway
GWC702	Generated when the dynamic data download for trunk subgroup data, table TRKSGRP in the CS 2000 Core, fails for a specific tuple
PM180	Generates when the system encounters a software exception

GWC logs (Sheet 4 of 5)

Log ID	Description
PM181	Generates when a specified step occurs in a PM function
PM185	Gives the trace back of the last trap that caused a peripheral to start again
PM703	Records the time an automated PM upgrade task failed
PM720	Produced when an unsolicited maintenance message is received in the Core from a GWC
PM777	Generated when the software detects a hardware defect
V5200	Generates an information report when the BCC fails on a speech link
V5201	Generates information when a V5.2 link BCC request for a speech channel is rejected
V5202	Generates when a V5.2 link BCC audit request is incomplete
V5400	Generates an information report when the V5 CC Audit sends a V5 interface query message
V5401	Generates an information report when a V5 Interface status mismatch occurs between the CM and GPP
V5402	Generates an information report when a V5 link status mismatch occurs between the CM and GPP
V5403	Generates an information report when a C-channel data mismatch occurs between the CM and GPP
V5404	Generates an information report when a data link status mismatch occurs between the CM and GPP

GWC logs (Sheet 5 of 5)

Log ID	Description
IPSec and IKE security logs	Logs associated with the Internet Key Exchange (IKE) system
Kerberos logs	Logs associated with the Kerberos application

Interworking Spectrum Peripheral Module ATM

The following table lists the individual logs that the Interworking Spectrum Peripheral Module ATM Logs (IW SPM ATM) generates.

IW SPM ATM logs (Sheet 1 of 2)

Log ID	Description
BITS300	Indicates that a clock sync critical alarm has been raised
BITS301	Indicates that a clock sync non-critical alarm has been raised
BITS500	Indicates a BITS link state change capturing old/new states
BITS600	Indicates a BITS Fault Report Cleared
BITS601	Indicates a BITS Fault Report Cleared
BITS610	Indicates a BITS timing reference SSM value has changed
BITS612	Indicates a BITS timing reference source switch has occurred
IWBM500	Indicates that one of the following is out-of-service: C-side link, STS3cP carrier, ATM network state, or the ATM address state for the IW bridge software
IWBM501	Indicates the out-of-service item has returned to service
IWBM502	Indicates that a Bsy command was requested for a set of IW SPM bridge terminals
IWBM503	Indicates that an Rts command was requested for a set of IW SPM bridge terminals

IW SPM ATM logs (Sheet 2 of 2)

Log ID	Description
IWBM504	Indicates that an Offl command was requested for a set of IW SPM bridge terminals
IWBM505	Indicates that an Frls command was requested for a set of IW SPM bridge terminals
IWBM600	Indicates the IW bridge receives an invalid terminal ID during an attempt to free a bridge
IWBM601	Indicates an automatic system audit finds a problem and performs a corresponding action
IWBM602	Indicates no IDL bridges are available
IWBM603	Indicates an IWBM audit is being performed
IWBM700	Indicates a maintenance action is being performed
IWBM800	Indicates the number of available IW bridges exceeds the first threshold (70%)
IWBM801	Indicates the number of available IW bridges falls to less than 65%
IWBM802	Indicates the number of available IW bridges exceeds the second threshold (90%)
IWBM803	Indicates the number of available IW bridges falls to less than 85%
SPM313	Indicates a fault in the MIM on an SPM
SYNC202	Indicates a synchronization problem in an office in the base configuration
XNET607	Indicates that an IW SPM interworking bridge was not available for the connection request

Interworking Spectrum Peripheral Module Internet Protocol

The following table lists the individual logs that the Interworking Spectrum Peripheral Module Internet Protocol (IW SPM IP) generates.

IW SPM IP logs

Log ID	Description
NODE300	Generated when a trouble condition is present with the node
NODE303	Indicates the Wrong Application Data on the SPM
NODE323	Generated when a REx request does not execute
NODE326	Indicates a hardware fault
NODE450	Generates to summarize a series of event reports under one log header during a routine exercise (REX) test
NODE500	Indicates a system node state change
NODE600	Indicates an INFO log
VOIP800	Indicates that a network traffic parameter has exceeded the threshold set by data network management personnel in table MNIPPARM

Services Application Module

The following table lists the individual logs that the Services Application Module (SAM21) generates.

SAM21 logs (Sheet 1 of 2)

Log ID	Description
IPOA301	Indicates a loss of cell delineation
IPOA302	Indicates a SONET AIS alarm
IPOA303	Indicates an ATM connection fault
IPOA304	Indicates connection members changed state
IPOA305	Indicates an ATM interface capacity threshold was crossed
IPOA801	Indicates an ATM CRC32 threshold exceeded

SAM21 logs (Sheet 2 of 2)

Log ID	Description
SCU301	Indicates the Extension Bridge in Slot 15/16 is Down/Up
SCU306	Indicates that the NFS Mount, GWC, 3PC, STORM and SAM21 fail
SCU310	Indicates the CPU load is high
SCU315	Indicates problems with temperature or temperature control in a sled
SCU329	Indicates a loss of shelf controller communications
SCU332	Indicates the memory usage is high
SCU335	Indicates problems with power
SCU344	Indicates a lock or unlock request at the CS 2000 SAM21 Manager client has taken longer than 3 minutes to complete
SCU346	Indicates that many processes have abnormally terminated or there is a problem with firmware flashing
SCU348	Indicates that provisioning of the board failed due to some system problem
SCU349	Indicates disk usage is high
SCU356	Indicates a critical fault
SCU398	Indicates a TELCO alarm is raised
SCU399	Indicates that communication between the Shelf Controllers and the CS 2000 SAM21 Manager server application is unavailable
SCU500	Indicates a change in state of a card
SCU501	Indicates an equipment insertion specifying the shelf, card, and slot
SCU502	Indicates equipment removal specifying the shelf, card, and slot

STORage Management

The following table lists the individual logs that the STORage Management (STORM) generates.

STORM logs

Log ID	Description
STM300	Indicate a fault with the fiber channel connection between the STORM cPCI unit and the RAID device
STM301	Indicates a disk related fault
STM302	Indicates a hardware fault
STM800	Indicates the CPU load average exceeds expected levels
STM801	Indicates that memory usage has crossed a threshold
STM802	Indicates that file system usage has crossed a threshold
STM803	Indicates the number of zombie processes has crossed a threshold

Carrier VoIP Server Platform Foundation Software

The following table lists the individual logs that the Carrier VoIP Server Platform Foundation Software (SPFS) generates.

SSPFS logs (Sheet 1 of 2)

Log ID	Description
SOCK525	Indicates that the SOCKS program has been started manually
SOCK526	Indicates that the SOCKS program has been stopped manually
SPFS310	Indicates a loss of network connectivity, log failure, fan failure, disk failure, and high temperature problems
SPFS320	Indicates when an automatic backup has failed and cleared

SSPFS logs (Sheet 2 of 2)

Log ID	Description
SPFS330	Indicates there is no active cluster node
SPFS350	Indicates when the threshold of a file system has been exceeded
SPFS400	Indicates the total number of alarms raised through alarmed

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 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).
- 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*.

CCA300

Log report CCA300 indicates that free space in RAM is low.

The Call Agent generates log report CCA300 in addition to a Memory alarm at the Call Agent Manager.

Format

The format for log report CCA300 is as follows:

```
CCA300 APR17 07:46:06 FLT  Memory
Unit Number : 0, ACTIVE
Description : Available memory is between 125MB and 150MB;
              minor threshold reached.
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA301

Log report CCA301 indicates that the CPU load average for one or more time segments has exceeded the threshold.

The Call Agent generates log report CCA301 in addition to the alarm.

Format

The format for log report CCA301 is as follows:

```
CCA301 APR17 07:49:07 FLT  CPU Load
Unit Number : 0, ACTIVE
Description : 1 minute load average is between 10.00 and 20.
              00; minor threshold reached.
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA302

Log report CCA302 indicates that free space on the root file system is low.

The Call Agent generates log report CCA302 in addition to the alarm.

Format

The format for log report CCA302 is as follows:

```
CCA302 APR17 07:47:46 FLT  Disk
Unit Number : 0, ACTIVE
Description : Percentage of root free disk space is less than
              or equal to 5.00; critical threshold reached.
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA303

Log report CCA303 indicates that at least one software process has terminated abnormally and may retain system resources such as memory space or CPU usage.

The Call Agent generates log report CCA303 in addition to the alarm.

Format

The format for log report CCA303 is as follows:

```
CCA303 APR17 08:06:23 FLT  Zombie Process
Unit Number : 0, ACTIVE
Description : Number of zombie processes is between 5 and 10;
              minor threshold reached.
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA304

Log report CCA304 indicates one or more of the Network File System (NFS) mounted file systems is inaccessible. Each Call Agent mounts three file systems from each STORage Management (STORM) card.

The Call Agent generates log report CCA304 when the alarm clears.

Format

The format for log report CCA304 is as follows:

```
CCA304 APR17 08:04:43 FLT  NFS Mount Not Accessible
Unit Number : 0, ACTIVE
Description : Number of accessible NFS mounts is between 3
              and 5; minor threshold reached.
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA305

Log report CCA305 indicates that the platform software lost time synchronization to one or more Network Time Protocol (NTP) servers, or the drift is excessive.

The Call Agent generates log report CCA305 in addition to the alarm.

Format

The format for log report CCA305 is as follows:

```
CCA305 APR17 08:09:54 FLT  NTP Error
Unit Number : 0, ACTIVE
Description : Host is not communicating with any NTP
              server(s); No. of configured server(s): 2; No.
              of accessible server(s): 0.
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA306

Log report CCA306 indicates that the CPU utilization has exceeded a threshold. A SYS CpuUtl alarm is generated in addition to the log report.

Format

The format for log report CCA306 is as follows:

```
*    CCA306 JUL7 13:23:16 FLT  CPU Utilization
     Unit Number : 0, ACTIVE
     Description : 5 minute percent idle cpu utilization is
                   below 5.00, minor threshold reached.
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA309

Log report CCA309 indicates that the card has a Peripheral Component Interconnect (PCI) bus fault, Error Checking and Correction (ECC) memory fault, or a parity error.

The Call Agent generates log report CCA309 in addition to the alarm.

Format

The format for log report CCA309 is as follows:

```
CCA309 AUG6 08:13:22 FLT  Hardware Fault
Unit Number : 1, INACTIVE
Description : Data parity critical threshold is reached;
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA314

Log report CCA314 indicates that free memory for the call processing application is low. The alarm raised is an APPL Memory alarm. This log report and the APPL Memory alarm are not related to the SYS Memory alarm.

Format

The format for log report CCA314 is as follows:

```
** CCA314 OCT21 11:22:10 FLT  Application Memory
   Unit Number : 1, ACTIVE
   Description : Major memory alarm threshold of 32MB reached
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Description	string	This field indicates if the major threshold of 32MB was reached or if the minor threshold of 48MB was reached.

Action

Contact Nortel Networks support personnel immediately.

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

For major 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 requires no additional information.

CCA315

Log report CCA315 indicates that the call processing application is out of synchronization. The Call Agent generates an APPL simplx alarm in addition to the log report.

The inactive Call Agent is not ready for takeover without an outage. If the mate Call Agent is in-service, and a switch of activity occurs while the APPL simplx alarm is active, the newly active Call Agent triggers a restart reload. A restart reload indicates a complete loss of call processing during the restart and all calls are dropped.

If the APPL simplx alarm persists and a switch of activity does occur, any provisioning or operational data changes that occurred after the loss of synchronization are lost.

Format

The format for log report CCA315 is as follows:

```
**  CCA315 JUL7 01:38:04 FLT  Application Out-of-Sync (simple
    Unit Number : 0, INACTIVE
    Description : The application is Out Of Sync
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA316

Log report CCA316 indicates that the call processing application has changed state.

Format

The format for log report CCA316 is as follows:

```
*   CCA316 MINOR FLT  Application Out-of-Service
    Unit Number : 0, INACTIVE
    Description : The application is Booting.
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA322

Log report CCA322 indicates that the inactive call processing application failed an image test.

The Call Agent generates log report CCA322 in addition to the alarm.

Format

The format for log report CCA322 is as follows:

```
CCA322 AUG6 08:32:10 FLT Image Test Failed
Unit Number : 0, ACTIVE
Description : Result: Failed, Initiator: Manual, Restart
              Type: Warm, Reason: application-related
              non-critical fault;
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA331

Log report CCA331 indicates that the Call Agent cards cannot communicate to the mate through the sparing link. When Geographic Survivability is enabled, the log includes details of monitored connection states. The Call Agent generates log report CCA331 in addition to the alarm.

Format

The formats for log report CCA331 are as follows:

With Geographic Survivability disabled

```
CCA331 JUL25 10:46:48 FLT Mate Connectivity
Unit Number  0, ACTIVE
Description: Link0: INSV, mateCon: AVAIL, netCon: AVAIL;
             Link1: INSV, mateCon: AVAIL, netCon: AVAIL;
             BLink: SYSB, mateCon: UNAVAIL; SL: INSV;
```

With Geographic Survivability enabled

```
CCA331 JUL25 10:46:48 FLT Mate Connectivity
Unit Number: 0, INACTIVE
Description: Link0: INSV, mateCon: BAD (opt:BAD, wan:BAD),
             netCon: OK (local:OK, wanEdge:OK): LINK1:INSV,
             mateCon: BAD (opt:BAD, wan:BAD), netCon: OK
            (local:OK, wanEdge:OK); BLink: SYSB, mateCon:BAD;
             SL: SYSB;
```

The format of associated information log report CCA631 (Mate Connectivity Restored) includes the same details as for CCA331when Geographic Survivability is enabled or disabled. (The field values in CCA631 = OK or INSV.)

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Unit number	0 or 1	The CCA unit number
Activity	ACTIVE or INACTIVE	The activity state of this unit
Description		Description of Geographic Survivability mode connection
Link0:	INSV or SYSB	State of Eth Link 0 connectivity to Ethernet Routing Switch 8600
mateCon:	OK or BAD	Mate connectivity via Eth Link 0
opt	OK or BAD	Mate connectivity via ETH Link 0 and Ether via optical
wan	OK or BAD	Mate connectivity via Eth Link 0 and WAN
netCon:	OK or BAD	Composite network connectivity via ETH Link 0
local	OK or BAD	Network connectivity to local network (Shelf Controller) via Eth Link 0
wanEdge	OK or BAD	Network connectivity to local wan edge router
Link1:	INSV or SYSB	State of Eth Link 1 connectivity to Ethernet Routing Switch 8600
mateCon:	OK or BAD	Mate connectivity via Eth Link 1
opt	OK or BAD	Mate connectivity via ETH Link 1 and Ether via optical
wan	OK or BAD	Mate connectivity via Eth Link 1 and WAN
netCon:	OK or BAD	Composite network connectivity via ETH Link 1
local	OK or BAD	Network connectivity to local network (Shelf Controller) via Eth Link 1

Field	Value	Description
wanEdge	OK or BAD	Network connectivity to local wan edge router
BLink	INSV or SYSB	Backup link state
mateCon	OK or BAD	Mate connectivity via BLink
SL	INSV or SYSB	Sparing-link state

Action

Use the description info in the log or in the corresponding CON alarm to determine the type of connectivity problem. Determine whether this is caused by a maintenance action in progress or by a network connectivity fault.

If a network fault exists, attempt to isolate the connectivity problem. If a maintenance action is in progress, monitor the condition until the maintenance is completed.

For more information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

As of the (I) SN09FF release, the name of the final field in the log changed to SL. Previously, the field name was FC because the sparing link used a fiber channel (FC) interface. The FC interface continues to be supported. In SN09FF, feature A00012478 added a new sparing-link interface, the GigE interface. The user can select the type of sparing-link interface, as explained in *Call Agent Configuration Management*, NN10109-511.

CCA335

Log report CCA335 indicates that the Ethernet interface is down. When Geographic Survivability is enabled, the log includes details of monitored connection states.

The Call Agent generates an Eth alarm at the Call Agent Manager in addition to the log report.

Format

The format for log report CCA335 is as follows:

With Geographic Survivability disabled

```
CCA335 JUL25 13:31:01 FLT  Link Connectivity
Unit Number : 0, UNDETERMINED
Description : Link0: INSV, mateCon: UNAVAIL, netCon: AVAIL;
              Link1: INSV, mateCon: UNAVAIL, netCon: AVAIL;
              BLink: SYSB, mateCon: UNAVAIL; SL: SYSB;
```

With Geographic Survivability enabled

```
CCA335 JUL25 10:46:48 FLT Link Connectivity
Unit Number: 0, INACTIVE
Description: Link0: INSV, mateCon: OK (opt:BAD, wan:OK),
             netCon: OK (local:OK, wanEdge:OK): LINK1:INSV,
             mateCon: OK (opt:BAD, wan:OK), netCon: OK
            (local:OK, wanEdge:OK); BLink: SYSB, mateCon:BAD;
             SL: SYSB
```

The format of associated information log report CCA635 (Link Connectivity Restored) includes the same details as for CCA335 when Geographic Survivability is enabled or disabled. (The field values in CCA635 = OK or INSV.)

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Unit number	0 or 1	The CCA unit number
Activity	ACTIVE or INACTIVE	The activity state of this unit
Description		Description of Geographic Survivability mode connection
Link0:	INSV or SYSB	State of Eth Link 0 connectivity to Ethernet Routing Switch 8600
mateCon:	OK or BAD	Mate connectivity via Eth Link 0
opt	OK or BAD	Mate connectivity via ETH Link 0 and Ether via optical
wan	OK or BAD	Mate connectivity via Eth Link 0 and WAN
netCon:	OK or BAD	Composite network connectivity via ETH Link 0
local	OK or BAD	Network connectivity to local network (Shelf Controller) via Eth Link 0
wanEdge	OK or BAD	Network connectivity to local wan edge router
Link1:	INSV or SYSB	State of Eth Link 1 connectivity to Ethernet Routing Switch 8600
mateCon:	OK or BAD	Mate connectivity via Eth Link 1
opt	OK or BAD	Mate connectivity via ETH Link 1 and Ether via optical
wan	OK or BAD	Mate connectivity via Eth Link 1 and WAN
netCon:	OK or BAD	Composite network connectivity via ETH Link 1
local	OK or BAD	Network connectivity to local network (Shelf Controller) via Eth Link 1

Field	Value	Description
wanEdge	OK or BAD	Network connectivity to local wan edge router
BLink	INSV or SYSB	Backup link state
mateCon	OK or BAD	Mate connectivity via BLink
SL	INSV or SYSB	Sparing-link state

Action

Use the description info in the log or in the corresponding CON alarm to determine the type of connectivity problem. Determine whether this is caused by a maintenance action in progress or by a network connectivity fault.

If a network fault exists, attempt to isolate the connectivity problem. If a maintenance action is in progress, monitor the condition until the maintenance is completed.

For more information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

As of the (I) SN09FF release, the name of the final field in the log changed to SL. Previously, the field name was FC because the sparing link used a fiber channel (FC) interface. The FC interface continues to be supported. In SN09FF, feature A00012478 added a new sparing-link interface, the GigE interface. The user can select the type of sparing-link interface, as explained in *Call Agent Configuration Management*, NN10109-511.

CCA336

Log report CCA336 indicates that one or more Ethernet links are unable to communicate with the network. When Geographic Survivability is enabled, the log includes details of monitored connection states. The Call Agent generates log report CCA336 in addition to the alarm.

Format

The format for log report CCA336 is as follows:

With Geographic Survivability disabled

```
CCA336 APR17 08:58:26 FLT  Network Connectivity
Unit Number : 1, INACTIVE
Description : Link0: INSV, mateCon: AVAIL, netCon: UNAVAIL;
              Link1: INSV, mateCon: AVAIL, netCon: AVAIL;
              BLink: INSV, mateCon: AVAIL; FC: INSV;
```

With Geographic Survivability enabled

```
CCA336 APR17 08:58_26 FLT Network Connectivity
Unit Number: 1, ACTIVE
Description: Link0: INSV, mateCon: BAD (opt:BAD, wan:BAD),
             netCon: OK (local:OK, wanEdge:OK): LINK1:INSV,
             mateCon: BAD (opt:BAD, wan:BAD), netCon: OK
            (local:OK, wanEdge:OK); BLink: SYSB, mateCon:BAD;
             FC: SYSB;
```

The format of associated information log report CCA636 (Network Connectivity Restored) includes the same details as for CCA336 when Geographic Survivability is enabled or disabled. (The field values in CCA636 = OK or INSV.)

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Unit number	0 or 1	The CCA unit number
Activity	ACTIVE or INACTIVE	The activity state of this unit
Description		Description of Geographic Survivability mode connection
Link0:	INSV or SYSB	State of Eth Link 0 connectivity to Ethernet Routing Switch 8600
mateCon:	OK or BAD	Mate connectivity via Eth Link 0
opt	OK or BAD	Mate connectivity via ETH Link 0 and Ether via optical
wan	OK or BAD	Mate connectivity via Eth Link 0 and WAN
netCon:	OK or BAD	Composite network connectivity via ETH Link 0
local	OK or BAD	Network connectivity to local network (Shelf Controller) via Eth Link 0
wanEdge	OK or BAD	Network connectivity to local wan edge router
Link1:	INSV or SYSB	State of Eth Link 1 connectivity to Ethernet Routing Switch 8600
mateCon:	OK or BAD	Mate connectivity via Eth Link 1
opt	OK or BAD	Mate connectivity via ETH Link 1 and Ether via optical
wan	OK or BAD	Mate connectivity via Eth Link 1 and WAN
netCon:	OK or BAD	Composite network connectivity via ETH Link 1
local	OK or BAD	Network connectivity to local network (Shelf Controller) via Eth Link 1

Field	Value	Description
wanEdge	OK or BAD	Network connectivity to local wan edge router
BLink	INSV or SYSB	Backup link state via fiber channel
mateCon	OK or BAD	Mate connectivity via BLink
FC	INSV or SYSB	Fiber channel (FC) state

Action

Use the description info in the log or in the corresponding CON alarm to determine the type of connectivity problem. Determine whether this is caused by a maintenance action in progress or by a network connectivity fault.

If a network fault exists, attempt to isolate the connectivity problem. If a maintenance action is in progress, monitor the condition until the maintenance is completed.

For more information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA340

Log report CCA340 indicates a loss of ATM connectivity between the Message Controller card and the Message Switch (MS).

Format

The format for log report CCA340 is as follows:

```
CCA340 APR17 01:46:00 FLT  MC ATM Connectivity
Unit Number : 0, ACTIVE
Description : MC0 is isolated
```

Selected field descriptions

This log report has no selected fields.

Action

Refer to procedure alarm clearing procedure MC ATM in *Call Agent Fault Management*, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA344

Log report CCA344 indicates a trouble condition on the Message Controller platform. These trouble conditions are related to memory usage, CPU usage, zombie processes, NTP status, and RAMDISK usage.

Format

The format for log report CCA344 is as follows:

```
CCA344 APR17 07:41:57 FLT  MC Trouble
Unit Number : 0, ACTIVE
Description : MC0: 1 minute load average is between 10.00 and
              20.00; minor threshold reached.
```

Selected field descriptions

This log report has no selected fields.

Action

Refer to procedure alarm clearing procedure MC Tbl in *Call Agent Fault Management*, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA345

Log report CCA345 indicates a loss of Ethernet connectivity for the Message Controller card.

Format

The format for log report CCA345 is as follows:

```
CCA345 APR17 01:46:00 FLT  MC Ethernet Connectivity
Unit Number : 0, ACTIVE
Description : 1 ethernet link out-of-service
```

Selected field descriptions

This log report has no selected fields.

Action

Refer to procedure alarm clearing procedure MC Eth in *Call Agent Fault Management*, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA351

Log report CCA351 indicates a response to several CON and APL alarms because the mate Call Agent unit is unavailable. Status information for the mate unit is unavailable at the maintenance interface.

The Call Agent generates log report CCA351 in addition to the alarm.

If a Call Agent card is locked by user action at the CS 2000 SAM21 Manager client, the Call Agent enters the locked-disabled-none state and appears with a hashed outline and a lock icon at the CS 2000 SAM21 Manager client. Duplex operations is restored after unlocking the card at the CS 2000 SAM21 Manager client.

If a Call Agent card experiences a platform software error that prevents the Call Agent from providing service, the Shelf Controller (SC) recovers the Call Agent. As the SC recovers the card, the card icon appearance at the CS 2000 SAM21 Manager client changes. Refer to SAM21 *Shelf Controller Fault Management*, NN10226911 or NN10089911 for more information about SC automatic recovery.

Format

The format for log report CCA351 as follows:

```
CCA351 NOV1 12:21:13 FLT No Mate Communication (simplex)
Unit Number : 0, ACTIVE
Description : Mate unit is unavailable.
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA352

Log report CCA352 indicates that an NFS Inactive Indicator Key (NIIKEY) file was detected in one of the /TAPE directories. The NIIKEY file is used by Nortel Networks personnel during an office conversion from a SuperNode-based switch to a CS 2000 - Compact.

If this log report is generated, contact Nortel Networks support personnel.

Format

The format for log report CCA352 is as follows:

```
*   CCA352 JUL7 13:54:44 FLT  NIIKEY Detected
    Unit Number : 1, INACTIVE
    Description : NIIKEY Detected
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA355

Log report CCA355 indicates the inactive unit is jammed to prevent a Switch of Activity (SWACT).

The Call Agent generates log report CCA355 in addition to the alarm.

Format

The format for log report CCA355 is as follows:

```
CCA355 APR17 08:15:42 FLT  Jam Inactive Unit
Unit Number : 0, ACTIVE
Description : Inactive JAMMED
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA362

Log report CCA362 indicates at what point one or more REx tests has failed.

The Call Agent generates log report CCA362 in addition to the alarm.

Format

The format for log report CCA362 is as follows:

```
CCA362 AUG6 01:36:29 FLT REx Test Failed
Unit Number : 0, ACTIVE
Description:INITIATOR: Application, CLASS: Base, RESULT:
            Failed; REASON: application-related non-critical
            fault encountered; IMGTST PERFORMED: Yes, DIAGS
            PERFORMED: No, RESET PERFORMED: No;
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

For information on how to gather TRAP log reports, SWER log reports, and footprint buffer information, refer to the *Fault Management*, NN10087911.

CCA365

Log report CCA365 indicates System REx has not started for over seven days.

The Call Agent generates log report CCA365 in addition to the alarm.

Format

The format for log report CCA365 is as follows:

```
CCA365 AUG6 08:19:29 FLT RExSch (REx Schedule Failure)
Unit Number : 0, ACTIVE
Description: System REx has not run for at least 7 days;
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA375

Log report CCA375 indicates that the two Call Agent cards in the CS 2000 - Compact are of two different hardware types. This log report is expected during a hardware upgrade of the Call Agent cards.

If this log report is generated, contact Nortel Networks support personnel.

Format

The format for log report CCA375 is as follows:

```
* CCA375 JUL12 10:31:27 FLT  Processor Configuration
  Unit Number : 1, ACTIVE
  Description: CPU Type - Unit 0 has a 7410; Unit 1 has a 750
```

Selected field descriptions

This log report has no selected fields.

Action

If this log report is generated during a hardware upgrade no action is required. If this log report is generated at any other time, contact Nortel Networks support personnel.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA380

Log report CCA380 indicates that one Call Agent card has a different committed patch file version than the other card. This alarm clears when the same patch file version is committed on the second Call Agent card.

The Call Agent generates log report CCA380 to indicate that the committed load mismatch alarm is raised.

Format

The format for log report CCA380 is as follows:

```
CCA380 APR17 09:12:43 FLT  Committed Loads Not Equal
Unit Number : 1, INACTIVE
Description : Unable to lock file /patchingB/._6_1_db: commit
              mismatch
```

Selected field descriptions

This log report has no selected fields.

Action

For information on how to clear this alarm, refer to the C*all Agent Fault Management* document, NN10087-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA390

Log report CCA390 indicates a trap from a Linux platform software process. Traps in Linux platform software do not affect call processing. Any process that traps and exits is automatically restarted.

In previous releases, traps were generated during platform patching and manual platform software process restarts due to the method that platform software processes were stopped. Traps generated during platform patching and manual process restarts for software releases older than SN07 may be ignored.

If this log report is generated, contact Nortel Networks support personnel.

Format

The format for log report CCA390 is as follows:

```
*** CCA390 JUL6 16:15:53 TRAP  TRAP
    SWMON process just received signal SIGSEGV. Exiting now.
```

Selected field descriptions

This log report has no selected fields.

Action

Record the log report, and copy the `3pc.statlog and 3pc.designlog` files from the `/var/log` directory to a safe location. A datadump with a traceback for the process that trapped is written to the 3pc.statlog file. Ensure that the correct log files are saved. 3pc.statlog is the active file for today, 3pc.statlog.1 is from yesterday, and 3pc.statlog.2 is from two days ago. Only the most recent seven days are retained. 3pc.designlog file naming is designed the same way.

Contact Nortel Networks support personnel with the log report and the log files.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CCA685

Log report CCA685 applies to offices with the Geographic Survivability feature enabled. The log indicates that the Open Shortest Path First (OSPF) routing is disabled on the local Ethernet Routing Switch 8600.

This happens only on the inactive unit when Ethernet connectivity or the optical ring goes out of service between sites. The action improves the ability of outside nodes to route to the remaining active Call Agent site.

Format

The format for log report CC685 is as follows:

```
** CCA685 JAN11 12:38:05 INFO OSPF Disabled
   Unit Number: 1, INACTIVE
   Description: Open Shortest Path First routing protocol
            disabled on the local default gateway.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Unit number	0 or 1	The CCA unit number
Activity	ACTIVE or INACTIVE	The activity state of this unit

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.

CCA686

Log report CCA686 applies to offices with the Geographic Survivability feature enabled. The log indicates that the Open Shortest Path First (OSPF) routing is enabled on the local Ethernet Routing Switch 8600.

Format

The format for log report CCA686 is as follows:

```
** CCA686 JAN11 14:26:05 INFO OSPF Enabled
   Unit Number: 0, ACTIVE
   Description: Open Shortest Path First routing protocol
            enabled on the local default gateway.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Unit number	0 or 1	The CCA unit number
Activity	ACTIVE or INACTIVE	The activity state of this unit

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.

BOOT200

The system issues the BOOT200 log when it responds to a bootp request from an out-of-service common equipment module (CEM) in an MG 4000 in a Carrier Voice over IP network. The log indicates whether the CEM loaded successfully.

The bootstrap protocol (bootp) enables a diskless machine to boot from a network. The diskless machine does not know where to boot from nor what load to use. To obtain that information, it broadcasts a bootp request onto the network. A bootp server, upon receiving the request, responds with enough information to allow the diskless machine to initiate the transfer of a load file from the server to itself.

The CS 2000 can act as a bootp server for out-of-service common equipment modules (CEMs) in MG 4000s. If an out-of service CEM has just been powered up or has been reset manually, and if bootp notification has not been suppressed for the MG 4000, the out-of-service CEM loads by this method.

Note 1: This loading method applies only to out-of service CEMs in the MG 4000. In-service CEMs and all other modules are loaded by way of integrated-node-maintenance (INM) loading methods.

Note 2: If bootp notification has been suppressed for the MG 4000, then you must load out-of-service CEMs by other means. For information, see the material on suppressing bootp notification in *MG 4000 Configuration Management*, NN10098-511.

Format

The format for log report BOOT200 is as follows:

```
BOOT200 mmmdd hh:mm:ss ssdd INFO TFTP BOOT LOG REPORT
     Log Result: <result>
     File Name: <file_name>
     Node Name: <node_name>
     Record Size (byte): <record_size>
     File ID: <file_ID>
     Progress Mark: <progress_mark>
     Total Size (kbytes): <total_size>
     Description: <description>
     Elapsed time: (elapsed_time>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Log Result	PASSED or FAILED	Indicates whether loading succeeded or failed.
File Name	Text	Name of the load file.
Node Name	Text	Node number and unit number of the MG 4000.
Record Size	Integer	File record size in bytes.
File ID	Hexadecimal	Internal file ID.
Progress Mark	Integer	The last progress mark. Each progress mark is one kbyte.
Total Size (kbytes)	Integer	File size in kbytes.
Description	Text	Message indicating successful completion, or an error message.
Elapsed time	Time value	Loading time in the format hh:mm:ss:ttt.

Action

This is an information log and requires no action.

Associated OM registers

This log report has no associated OM registers.

BOOT201

The bootstrap protocol (bootp) enables a diskless machine to boot from a network. The diskless machine does not know where to boot from nor what load to use. To obtain that information, it broadcasts a bootp request onto the network. A bootp server, upon receiving the request, responds with enough information to allow the diskless machine to initiate the transfer of a load file from the server to itself.

The CS 2000 can act as a bootp server for Nortel-provided peripheral modules. If a peripheral module needs to boot, it broadcasts a bootp request. When the bootp request arrives at the CS 2000, software in the XA-Core shelf looks up the peripheral module in the MNCKTPAK data-schema table. If the peripheral module is listed in the table, the CS 2000 sends a response to the peripheral module. The peripheral module then initiates the transfer of a load file from the server to itself.

The CS 2000 issues the BOOT201 log to indicate that it has failed one or more of the bootp requests it has received. If it fails repeated requests from a device, it issues the BOOT201 log at ten-minute intervals as a record of the failures. (The ten-minute interval length is a fixed value. The user cannot change it.)

Format

The format for log report BOOT201 is as follows:

```
BOOT201 mmmdd hh:mm:ss ssdd INFO Bootp log report
Mac Address: <xxxxxxxxxxxx>
     MAC addr to node_id lookup failure: <nn>
     INM permission to boot failure: <nn>
     Core IP address lookup failure: <nn>
     SEND_UDP_MSG failure: <nn>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Mac Address	Alphanumeric string	MAC address of the device sending the failed bootp request or requests.
MAC addr to node_id lookup failure	Numeric	Number of bootp requests that failed for the following reason. The requesting device was not listed in table MNCKTPAK.
INM permission to boot failure	Numeric	Number of bootp requests that failed for the following reason. The proper permissions were not set in the integrated node maintenance (INM) system. (INM is the maintenance system for peripheral modules.)
Core IP address lookup failure	Numeric	Number of bootp requests that failed for the following reason. The software in the XA-Core could not find the IP address of the device that issued the bootp requests.
SEND_UDP_MSG failure	Numeric	Number of bootp requests that failed for the following reason. The message to the requesting device failed.

Action

This is an information log and requires no action.

If you want to find out which device is sending the bootp request or requests, look up the MAC address in the office records. If the MAC address is not that of a device listed in the office records, see Additional information.

Associated OM registers

This log report has no associated OM registers.

Additional information

It may happen that a bootp request from a non-Nortel device finds its way to the CS 2000. If this happens, the CS 2000 fails the bootp request and issues the BOOT201 log. If this happens, the BOOT201 log does not indicate a problem in the CS 2000 nor in a Nortel-provided peripheral module.

ESA120

Log report ESA120 is generated if the CS2000 successfully generates an MG9000 ESA data file in SFDEV. The file generation is initiated every 24 hours or from a manual command.

Format

The format for log report ESA120 is as follows:

```
ESA120 mmmdd hh:mm:ss ssdd INFO ESA DATA GENERATION

ESA120 MAY20 01:00:40 2400 INFO ESA DATA GENERATION
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
ESA DATA GENERATION	constant	Successful generation of file with MG9000 ESA data.

Action

Informational log only. Note that the MG9000 EM must download the ESA data to the MG9000 for it to be used during an emergency stand-alone event.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

ESA121

Log report ESA121 is generated if the CS2000 fails to generate an MG9000 ESA data file in SFDEV. The file generation is initiated every 24 hours or from a manual command.If the MG9000 goes into emergency stand alone, then the last ESA data file successfully downloaded will be used.

Format

The format for log report ESA121 is as follows:

```
ESA121 mmmdd hh:mm:ss ssdd INFO ESA DATA GENERATION FAIL
MG9000 ESA WILL USE PREVIOUS DATA FILE

ESA121 MAY20 01:00:48 3500 INFO ESA DATA GENERATION FAIL
MG9000 ESA WILL USE PREVIOUS DATA FILE
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
ESA DATA GENERATION FAIL	constant	The MG9000 ESA data file ESA_SYSTEM_SD$XML failed to generate on the device specified by OFCENG parameter ESA_GWDATA_DEVICE.
MG9000 ESA WILL USE PREVIOUS DATA FILE	constant	Last file successfully downloaded to the MG9000 EM and MG9000 will be used if an ESA even occurs.

Action

Ensure there is enough room on the device and consider using a disk device instead of SFDEV.

Associated OM registers

This log report has no associated OM registers.

Additional information

The MG9000 EM will continue to use the last valid ESA data file successfully downloaded.

Table DSLIMIT specifies the maximum allowed size of SFDEV in the STOREFS entry. This entry can not be set above 5 million words (10 million bytes).

SCAI304

Switch Computer Application Interface (SCAI) is a messaging link that the CS 2000 provides to a host computer. The information carried across this X.25/TCP-IP link allows applications running on the CS 2000 to communicate with applications running on the host computer.

The PRI User-to-User Signaling (UUS) supplementary service enables a user to send/receive a limited amount of information to/from another user. UUS allows communication of ISDN users by transferring user-to-user information (UUI) within call control messages during the establishment of a call.

If the total size of the outgoing ICM message with UUI exceeds the maximum supported ICM size for X.25 linksets (241 bytes), the UUI is discarded and log SCAI304 is generated.

Format

The format for log report SCAI304 is as follows:

```
RSNN10AG  SCAI304 JAN14 22:30:56 5348 INFO UUIPARM DISCARDED
      MESSAGE   : DV_CALL_QUEUED_U
      LINK ID   : DNA: 000000000000000 PROTOCOL: 1 1 1 1
      DEVICE    : MPC: 0  LINK: 3
      SCAI GROUP: SCAI_GRP1
      LINKSET NAME: X25_LNK1
```

Selected field descriptions

The following table describes the fields in the log report:

Field	Values	Description
INFO	UUIPARM DISCARDED	
MESSAGE	DV_CALL_OFFERED_U, DV_CALL_QUEUED_U, DV_CALL_RECEIVED_C	The ICM message for which the SCAI304 log is generated.
LINK ID	aphanumeric	The link in table SCAICOMS corresponding to the ICM. Subfields are DNA and PROTOCOL.

Field	Values	Description
DEVICE	numeric	The device that generated the ICM message. Subfields are MPC and LINK.
SCAI GROUP	alphanumeric	The SCAI group datafilled in table SCAIGRP with which the extended call management (ECM) session is established.
LINKSET NAME	alphanumeric	The name of the linkset used by the ECM session.

Action

See the following table:

Specific problem Probable cause	Action
Specific problem: Outgoing ICM exceeds 241 bytes Probable cause: Received UUI too long for X.25	No immediate action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

In certain circumstances, the SCAI304 log is generated with LINK ID, DEVICE and LINKSET NAME set as unavailable. This happens when the queue used to transmit the message to the SCAI host is decided at a later stage, that is, after the UUI parameter has been discarded. The queue information is needed to provide details of the LINK ID, DEVICE, and LINKSET NAME.

SCPL100

Log SCPL100 is generated when an NCAS link is established between the CS 2000 Core and the Session Server.

Note: SCPL stands for Service Control Point Link.

Format

The format for log report SCPL100 is as follows:

```
<Switch ID> SCPL100 <Date> <Time> INFO NCAS LINK UP
      NCAS LINK FOR INSTANCE NUMBER <Instance> CAME UP
      DUE TO <Reason>
```

Example:

```
RTP308AS SCPL100 OCT01 12:54:31 INFO NCAS LINK UP
      NCAS LINK FOR INSTANCE NUMBER 1 CAME UP
      DUE TO COMMUP
```

Selected field descriptions

The following table describes the fields in the log report:

Field	Values	Description
Switch ID	alphanumeric	The switch identifier.
Instance	numeric	The instance number, as datafilled in the first field of the tuple in table IPAPPL.
Reason	alphabetic, COMMUP	The establish message received from the Session Server.

Action

See the following table:

Specific problem Probable cause	Action
Specific problem: CS 2000 received establish message from Session Server Probable cause: COMMUP message	No action is necessary; this log is for information only.

Associated OM registers

This log report has no associated OM registers.

Additional information

None.

SCPL200

Log SCPL200 is generated when an NCAS link is lost between the CS 2000 Core and the Session Server.

Note: SCPL stands for Service Control Point Link.

Format

The format for log report SCPL200 is as follows:

```
<Switch ID> SCPL200 <Date> <Time> INFO NCAS LINK DOWN
      NCAS LINK FOR INSTANCE NUMBER <Instance> WENT DOWN
      DUE TO <Reason>
```

Example:

```
RTP308AS SCPL200 OCT01 12:54:31 INFO NCAS LINK DOWN
      NCAS LINK FOR INSTANCE NUMBER 1 WENT DOWN
      DUE TO SENDFAILURENOTIFICATION
```

Selected field descriptions

The following table describes the fields in the log report:

Field	Values	Description
Switch ID	alphanumeric	The switch identifier.
Instance	numeric	The instance number, as datafilled in the first field of the tuple in table IPAPPL.
Reason	alphabetic; STATUSCHG (subfields Status = SCTP_SHUTDOWN_RCVD Event = COMM_DN), COMMLOST, COMMERROR, SENDFAILURENOTIFICATION	The notification message received from the Session Server.

Action

See the following table:

Specific problem Probable cause	Action
Specific problem: CS 2000 received notification message from Session Server Probable cause: see Reason field	1. For a short time no action is necessary. This allows the system to recover automatically. When the system recovers, it generates an SCPL100 log. 2. If the system does not recover, ensure that the Session Server is UP. 3. If the system still does not recover, check for any network problems between the Session Server and the CS 2000 Core.

Associated OM registers

This log report has no associated OM registers.

Additional information

None.

SDM267

CBM custlog log to indicate a change in the condition of a CBM link.

Format

The format for log report SDM267 is as follows:

```
SDM267 NONE INFO SDM LINK CONDITION CHANGE
Link: Domain <domain num> Port <port num>
From: <previous link condition>
To: <new link condition>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Link: Domain	0 or 1	MS number
Link: Port	0	NTL9X63 port number
From:	closed, mtc-open, open	previous link condition
To:	closed, mtc-open, open	new link condition

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.

SDM300

Log report SDM300 generates when connectivity is not present from an SuperNode Data Manager (SDM) node to one of the following:

- computing module (CM)
- operating company LAN

Format

The format for log report SDM300 is as follows:

```
<log_off_id> * SDM300 mmmdd hh:mm:ss ssdd TBL SDM Base
Maintenance
Connection has been lost
Type: <type>
<info>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_off_id	character string (maximum 12 characters)	Specifies the name for office identification in the log output header.
type	CM, or LAN	Indicates where the connectivity has been lost.

Field	Value	Description
info	character string	Indicates why the connectivity to the CM has been lost | For type=CM: CM Link Down:, and one of the following messages: • no heartbeat received from the CM • no heartbeat received by the CM • isolate msg from the CM • connect msg from the CM, no heartbeat received by the CM • restart warm msg from the CM, no heartbeat received by the CM • restart cold msg from the CM, no heartbeat received by the CM • restart reload msg from the CM, no heartbeat received by the CM • norestart swact msg from the CM, no heartbeat received by the CM • CM-SDM node IP address mismatch • heartbeat stopped on the SDM node • ds512 links are all closed For type=LAN: • Host Name: <operating company defined node name as entered when it was commissioned>

Action

Determine the reason the connection has been lost and restore connectivity. If a CM IP mismatch is present, verify that the IP addresses are correct. 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.

SDM301

Log report SDM301 generates when the maintenance system detects that a logical volume is not mirrored.

Format

The format for log report SDM301 is as follows:

```
* SDM301 MAY30 12:42:44 5641 TBL SDM Base Maintenance
Logical volume(s) not mirrored
Volume group name: <volume_group_name>
Status: <volume_group_status>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
volume_group_name	character string	Indicates which logical volume is not mirrored.
volume_group_status	integrating or not mirrored	Indicates the status of the logical volume.

Action

Check hardware faults as mirroring can be lost because of hard disk failure(s) on the SuperNode Data Manager (SDM) hardware. The system replaces a disk and brings this disk back in-service (InSv).

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM302

Log report SDM302 generates when the maintenance system detects that the use of a system resource exceeds the resource threshold. These thresholds include CPU, number of processes, swap space, number of zombie processes, swap queue length, and disk space. This log report shows the format and example of the log as the log appears in the OSS. The custlog file and the maintenance screen for the SuperNode Data Manager (SDM) node show this log. The logs in the custlog file and the maintenance screen have a different format.

Format

The format for log report SDM302 is as follows:

```
* SDM302 mmmdd hh:mm:ss ssdd TBL SDM Base Maintenance
Resource threshold exceeded
Type: <resource type>
Value: <resource value when threshold exceeded>
Threshold: <threshold value>
Name: <resource name>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
resource type	character string	Indicates the resource that exceeds the threshold. The following values can exceed the resource threshold: • CPU • number of processes • swap space • number of zombie processes • swap queue entries • logical volume

Field	Value	Description
resource value when threshold exceeded	integer, followed by a character string	Indicates the value of the threshold when the system generates the log. The following values can exceed the resource threshold, where “xx" is a positive integer: • CPU: “xx" number of queue entries that run • Number of processes: “xx" processes • Number of zombies: “xx" zombies • Number of swap queue entries: “xx" entries • For all other values: “xx" percent full
threshold value	integer, followed by a character string	Indicates the value of the resource at the time the resource exceeds the threshold. The following values are possible, where “xx" is a positive integer: • CPU: “xx" number of run queue entries • Number of processes: “xx" processes • Number of zombies: “xx" zombies • Number of swap queue entries: “xx" entries • For all other values: “xx" percent full
resource name	character string	Indicates the logical volume that exceeds the threshold. This field is present when the system reports on the logical volume resource.

Action

Contact the next level of support. Determine if the threshold is set too low. When the threshold is set too low, use the maintenance menu or the commissioning tool to raise the threshold. When the threshold is not too low, determine the process that overuses the resource and correct the problem. Reboot the SDM node. This action can fix the problem. It is possible that some kernel parameters require adjustment. Refer to the procedure "*Clearing a minor or major APPL SDM alarm*" in the Fault Management documentation for this device.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM303

Log report SDM303 generates when a process fails more than three times in a day. The system generates this log report when a message indicates that a process is in trouble.

Format

The format for log report SDM303 is as follows:

```
* SDM303 mmmdd hh:mm:ss ssdd TBL SDM Base Maintenance
Package: <package_name>
Process: <process_name>
Reason:  <info>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
package_name	character string	Indicates the package that had the failure.
process_name	character string	Indicates which process in the package failed.
info	character string	Indicates why the trouble condition occurred.

Action

Contact the next level of support. Examine the log files under /usr/sdm to determine why the process failed.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM304

Log report SDM304 generates when the Log Delivery application fails to reconnect to a device. This failure occurs after a UNIX file does not open. The osfconfig file contains a configurable value. This value specifies the frequency of reconnect attempts.

Format

The format for log report SDM304 is as follows:

```
<switch_name> SDM304 mmmdd hh:mm:ss ssdd FAIL
  OSF Delivery Service: Cannot establish open device.
Device name: <path name>
Reason: <reasontxt>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
path name	text string (13 characters)	The UNIX file name to which the logs transfer.
reasontxt	text string	Indicates the reason for the failure.

Action

Reinitialize the Log Delivery application to resume delivery. Use the Log Delivery online commissioning tool (logroute) to verify that the device name is present and valid.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM306

Log report SDM306 is generated when table access software versions on the Core side and a SuperNode Data Manager (SDM) node are not compatible. The two sides must have compatible versions of table access software to communicate.

Format

The format for log report SDM306 is as follows:

```
SDM306 mmmdd hh:mm:ss ssdd FLT
Component: SDM Table Access Server
Event: Incompatible Core software release (Layer_Version_Edition):
Action To Be Taken: <text>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
component	SDM Table Access Server	Process that communicates with the Core to determine when the Core software is not compatible with the SDM node software.
layer	integer	Identifies the Core software layer number sent from the Core to the SDM node.
version	integer	Identifies the software version number sent from the Core to the SDM node.
edition	character string	Identifies the software edition number sent from the Core to the SDM node.

Action

Upgrade the Core software to a version that is compatible with the SDM node software.

Note: The SDM node software must never be at a lower release level than Core software.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM308

Log report SDM308 provides information on the status of automated incremental backups (I-tape) and manual or automatic system image backups (S-tape). The system generates the log report when an automated incremental backup or a manual or scheduled system image backup fails on an SDM node.

Format

The format for log report SDM308 is as follows:

```
<log_loff_id> * SDM308 mmmdd hh:mm:ss ssdd TBL SDM Base
Maintenance
<reason>
<info>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_off_id	character string (maximum 12 characters)	Specifies the name for office identification in the log output header
reason	character string	Indicates whether the Automated incremental backup (I-tape) or System image backup (S-tape) failed.
info	character string	Indicates why the backup failed

Action

Determine the cause of the failure. Make sure that the backup tape is inserted. Perform the incremental backup manually to identify any problems. Check the /tmp/I-tape log or the /tmp/S-tape log for system details. If necessary, 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.

SDM309

Log report SDM309 generates when the maintenance system on a fault-tolerant SuperNode Data Manager (SDM) hardware detects a fault in a hardware device. The system also generates this log when a user takes a hardware device out-of-service.

Format

The format for log report SDM309 is as follows:

```
* SDM309 mmmdd hh:mm:ss ssdd TBL SDM Base Maintenance
Hardware device out of service
Device: <device identifier>
Device State: <device state>
Suspected module: <module description>
Location: <module location>
Other devices on module: <other devices>
Fault category: <fault category>
Reason: <text reason>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
device identifier	character string	This field identifies the device that is out of service. It contains a three-letter device symbol, followed by an optional device code and the device domain in parentheses. The different values for the device symbol are as follows: • CPU • FAN • ICM • DSK • DAT • ETH • 512

Field	Value	Description
		Note: There can be two Ethernet devices, ETH1 or ETH2. The device code appears only when the device symbol is DSK and more than one disk pair is present. The device code denotes one of the following disk pairs: • 1 to 9 for disk pairs 1 through 9 • A for the 10th disk pair • B for the 11th disk pair The device domain is either 0 or 1.
device state	character string	This field identifies the state of the device as one of the following: • ISTb (In service trouble) • SysB (System busy) • ManB (Manual busy) • CBsy (C-side busy - failed due to the unavailability of another device) • Fail (Failed)

Field	Value	Description
module description	character string	This field identifies the module that contains the out-of-service device, and the product engineering code (PEC) of the module. The field can identify the following modules: • Fan tray • Interconnect module • CPU set • CPU personality module • Ethernet/SCSI controller module • Ethernet controller module • Ethernet/SCSI I/O personality module • DS512 controller module • DS512 personality module

Field	Value	Description
module location	character string	This field identifies the location of the module that contains the out-of-service device. This field contains the following information: • SDMM, followed by the module name, indicates that the defective device is in the main chassis of the SDM frame • SDME, followed by the module name, indicates that the defective device is in the I/O expansion chassis of the SDM frame. • An integer between 1 and 16 follows the module name and tells the user the module location slot. • The slot number is followed by either “front" or “back". This tells the user that the faulty device is at the front or the back of the chassis.
other devices	character string	This field identifies which other devices are on the module. Field values are the same as those for device identifiers.
fault category	character string	Identifies the source of the failure.
text reason	character string	This field contains additional information about the defect.

Action

Use the QueryPM commands from the MAP display to confirm device status and hardware faults. Replace the defective module. Return the module to service.

If you cannot find the problem, 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.

SDM314

Log report SDM314 is generated when a DS512 link is reported down on the SDM.

Format

The format for log report SDM314 is as follows:

```
SDM314 <mmmdd hh:mm:ss ssdd> TBL SDM BASE MAINTENANCE
   DS512 LINK DOWN
   MODULE LOCATION: <shelf name>, SLOT: <slot number>
   PORT: <port num>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Shelf name	4-character alphanumeric	Indicates the main (SDMM) or expansion (SDME) shelf
Slot number	2-digit alphanumeric	Indicates the slot number of the DS512 module.
Port num	1-digit numeric	Indicates the port number for the link.

Action

Issue the "querypm" commands to check for DS512 hardware faults on the SDM. Issue "trnsl" from the MAP to check the link status. Perform link tests from the SDM local maintenance interface. Check the cabling to the DS512 port.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM315

Log report SDM315 is generated by the Table Access Service application when the application detects corruption in the Data Dictionary on the Core during a data dictionary download.

Format

The format for log report SDM315 is as follows:

```
<office name> SDM * SDM315 <date> <time> <logid> TBL
SDM Data Dictionary
   Core Data Dictionary Corruption Detected
   Type Id <type-id>
    Type Name: <type-name>
   Problem: <problem-description>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
type_id	character string 0 to 32767	Indicates the type id that is corrupted.
type_name	variable character string maximum 32 characters	Indicates the name of the type that is corrupted.
problem	Duplicate AREA Refinement or Duplicate STRING RANGE Field	Describes the corruption of the data dictionary type.

Action

Contact the next level of support with the information provided in the log. The log information contains essential information for identifying the Data Dictionary type that is corrupt.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM317

Log report SDM317 generates when the Distributed Computing Environment (DCE) detects any problem.

Format

The format for log report SDM317 is as follows:

```
<log_off_id> * SDM317 mmmdd hh:mm:ss ssdd TBL SDM Base
Maintenance
DCE problem detected
Reason: <info>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_off_id	character string (maximum 12 characters)	Specifies the name for office identification in the log output header.
info variable	character string	Indicates the cause of the problem.

Action

Contact your next level of support or ETAS to help determine the cause of the failure.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM318

Log report SDM318 is generated when an operational measurements (OM) report is not generated. This event is detected if an OM report fails to complete within one report interval.

Format

The format for log report SDM318 is as follows:

```
MMMdd hh:mm:ss <node name> syslog: SDM318 MAJOR FLT Event:
SDM OM Manager: <text_info: 1> <time_stamp> <text_info:_2>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
node name	alphanumeric character string	Identifies the terminal.
text_info:_1	mandatory, constant character string (maximum 21 characters)	Specifies “OM Report of CM Time:"
time_stamp	mandatory, variable character string (maximum 17 characters)	Indicates the month, day, year, and time on the Core of the OM report that failed to complete within its report interval.
text_info:_2	mandatory, constant character string (maximum 48 characters)	Specifies “incomplete. Action To Be Taken: Contact NORTEL."

Action

Contact Nortel Networks.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM321

Log report SDM321 is generated at the start of a split-mode upgrade. This log identifies the start or completion of a switch of activity (SwAct).

Format

The format for log report SDM321 is as follows:

```
SDM321 MAY12 13:18:34 0212 TBL SDM Base Maintenance
Split-system upgrade in progress
Status: <status>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<status>	One of the following text strings: • SwAct started • SwAct completed • SwAct started for fallback • SwAct completed for fallback	Identifies the current status of the split-mode upgrade

Action

Complete the split-mode upgrade or abort the upgrade by falling back.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM325

Log report SDM325 indicates that the connection to a network management component in a given domain has been lost. Log reports may be lost as a result.

Format

The format for log report SDM325 is as follows:

```
MSH10_I06BR   *  SDM325 JUN11 17:09:08 1820 TBL   Passport Log Streamer
        Connection to 10.102.4.15 has been lost.  Log reports may be lost.

MSH10_I06BR      SDM625 JUN11 17:09:20 1822 INFO Passport Log Streamer
        Connection to 10.102.4.15 has been established.
```

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.

SDM326

Log report SDM326 indicates that the connection was lost between the SDM and the Multiservice Data Manager (MDM) for 5-minute or 30-minute performance measurement data transfer.

Format

The format for log report SDM326 is as follows:

```
* SDM326 FEB22 12:12:55 2571 TBL
   SDM Base Maintenance
   Package: SDM_OMDD.omdd
   Process: odslodm
   Trouble Condition asserted
   Reason: Passport : 30-minute connection to 10.102.15.136
   was lost.
```

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.

SDM327

The subsystem generates log SDM327 when a Network Time Protocol (NTP) problem is detected.

Format

The log report format for SDM327 is as follows:

```
RTP_com4iems ** SDM327 SEP18 11:22:15 1724 TBL SDM
        Base Maintenance
        NTP problem detected
        Reason: NTP is not synchronized.
```

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.

SDM330

The data collection alarmd process generates log report SDM330 when it detects a communication problem between two mated HA SSPFS Platform cluster nodes.

Format

The format for log report SDM330 is as follows:

```
<log office id> <ECORE> *  SDM330 APR28 13:39:17 4668 FLT
Alarm raised or updated.
            <description>
            TimeStamp: <time stamp>
            ComponentID: <component ID>
            Category: <category string>
            Probable Cause: <probable cause string>
            Specific Problem: <specific problem string>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Description	Alarm Data Collection from mate node timed out, or	The alarmd processes on both systems of an HA cluster cannot exchange data because of an inter-system communication error
	Incompatible Payload version from mate node Alarmd	The two nodes in an HA cluster are running different software versions, and the alarmd is unable to understand the messages from its peer because of a protocol change
TimeStamp	variable	Identifies the time the alarm was raised.
ComponentID	<profile>= <clusterName>; NODE= <clusterName> -unit<num>	Identifies the remote node.

Field	Value	Description
Category	variable	Identifies the alarm category.
Probable Cause	variable	Qualifies the probable cause for this alarm.
Specific Problem	variable	Further qualifies the probable cause for this alarm.

Action

The action required is determined by the description field of the alarm.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM331

Log report SDM331 is generated when a file in directory /omdata/closedNotSent is deleted by audit to make more than 50% available space in directory /omdata.

Format

The format for log report SDM331 is as follows:

```
SDM331 MAJOR INFO SDM OM FILE RETENTION
   OMD: The file <filename> from closedNotSent directory
   deleted by audit to free up space in /omdata
```

Selected field descriptions

NA

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.

SDM332

Log report SDM332 indicates that the system audit completed with failures.

Format

The format for log report SDM332 is as follows:

```
** SDM332 SEP03 21:33:02 9120 TBL SDM Base Maintenance
   The system audit completed with failures. Execute
   the 'sysaudit-report' command to display the results.
```

Selected field descriptions

This log report has no selected fields.

Action

Execute the 'sysaudit-report' command to display the results of the system audit.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM334

Log report SDM334 indicates that a fault was detected on a CBM 800 OC-3 card. The log is generated if a signal on receive/transmit fiber to the OC-3 card is faulty or is not present.

Format

The format for log report SDM334 is as follows:

```
** SDM334 JAN07 10:53:33 0017 FLT SDM Base Maintenance
   OC3 Card Fault
   Problem: transmit fault
   Link: domain 0 port 0 (ms 0 link 0)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Problem	receive fault transmit fault	A fiber fault has been detected in the direction indicated.
Link	domain 0 port 0 (ms 0 link 0) domain 0 port 1 (ms 1 link 0) domain 1 port 0 (ms 0 link 1) domain 1 port 1 (ms 1 link 1)	This is the link reporting the problem.

Action

Clear the fiber fault.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM335

Log report SDM335 indicates a link fault. The log is generated on a Core and Billing Manager 800 (CBM 800) if cyclic redundancy code (CRC) errors occur frequently on an OC-3 link between the CBM 800 and the message switch (MS). The log is generated on an SDM if one of various errors occurs frequently on a DS512 link between the SDM and the MS.

Format

The format for log report SDM335 is as follows:

```
* SDM335 OCT22 14:20:26 6027 FLT SDM Base Maintenance
   Link Fault
   Fault: Bad Incoming CRCs
   Link: domain 0 port 0 (ms 0 link 0)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Fault:	Bad Incoming CRCs	(CBM 800 and SDM) This log indicates an abnormally large rate of CRC failures.
	Input Overflows	(SDM)
	Output Overflows	(SDM)
	Code Violations	(SDM) Loss of idle errors
	Bad Outgoing CRCs	(SDM)
	Double Nacks	(SDM)
	Wait for Send Timeouts	(SDM) This is often caused by the lack of fiber connectivity between the SDM and the MS.
	Wait for Ack Timeouts	(SDM)
	Wait for Idle Timeouts	(SDM)
	Wait for Message Timeouts	(SDM)
	dsv0 dsv1	(SDM) There is a problem with the availability of the DS512 card. dsv0 = domain 0 dsv1 = domain 1
Link:	domain 0 port 0 (ms 0 link 0) domain 0 port 1 (ms 1 link 0) domain 1 port 0 (ms 0 link 1) domain 1 port 1 (ms 1 link 1)	The link reporting the fault.

Action

Verify the integrity of the fiber connection between the CBM 800 and the MS. Verify the integrity of the hardware at each end of the fiber.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM336

Log report SDM336 is generated when the core fails to respond to CBM heartbeats or, on the CBM 850, the core responds that it has been homed to another address.

Format

The format for log report SDM336 is as follows:

```
SDM336 <date> <time> <seq #> FLT Alarm raised or updated.
    Heartbeat alarm
    Timestamp: <date> <time> <year>
    ComponentID: CLASS=NET;NETTYPE=CORE
    Category: Communications
    Probable Cause: <variable>
    Specific Problem: <variable>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Probable Cause	configurationOr Customization Errorequipment Malfunction	Corresponds to the loss of heartbeat response. Corresponds to the core homed to a different address (CBM 850).
	configurationOr Customization Error	Corresponds to the core homed to a different address (CBM850).
Specific Problem	No heartbeat response received	The CBM has not received any responses from its polling of the core.
	Core homed on a different cluster/unit address	The CBM 850 has received a response from the core indicating it is configured to communicate with a different CBM (CBM 850).

Action

For "no heartbeat response received":

- CBM 850
  - — Verify that the CBM is connected to the ethernet network.
  - — Verify that the core is running and is connected to the ethernet network.
  - — Verify that the ethernet network is running and configured to allow IP traffic between the three IP addresses associated with a CBM 850 and the core.
- CBM 800
  - — Verify that the OC3 hardware is on line.
  - — Verify that the CBM is datafilled in table SDMINV with a pec code of NTRX51LS.
  - — Verify that the MS cards and ports associated with the CBM 800 are in service.
  - — Verify that the CBM is datafilled and is in a ManB or RTS'd state.
  - — Verify that the OC3 links are in an open or mtc-open condition.

For "Core homed on a different cluster/unit address":

- On the core, use the CI increment "oamppci" to display the current status using the "disp" sub-command.
  - — If the display shows "no heartbeat" for either a node or the cluster, then these can be cleared to allow the cbm to connect to the core by using the subcommand "resetipaddress" followed by a node or cluster address (separated from the subcommand by a space).
  - — If the display shows "heartbeat active" either this CBM or the CBM at the address indicated from the disp subcommand is configured to the wrong core.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM500

The SuperNode Data Manager (SDM) generates log report SDM500 when the SDM node control process restarts. The SDM sends the SDM500 to the operations support system (OSS). The user cannot view this log from the SDM remote maintenance menu. The format and example for the SDM500 report appear in the OSS.

Format

The log report format for SDM500 is as follows:

```
SDM500 mmmdd hh:mm:ss ssdd INFO SDM Base Maintenance
SDM startup
Initial state: <startup_state>
```

Field descriptions

The following table describes each field in the log report:

Field	Value	Description
startup_state	INSV, ManB or OFFL	Indicates the startup state of the SDM.

Action

There is no action required.

Associated OM registers

There are no associated OM registers.

Additional information

There is no additional information.

SDM501

The SuperNode Data Manager (SDM) generates log report SDM501 when the node control process updates the SDM run state to in-service (InSv). The operations support system (OSS) receives this log. The user cannot view this log from the SDM remote maintenance interface (RMI). The format and example for the SDM501 report appear in the OSS.

Format

The log report format for SDM501 is as follows:

```
SDM501 mmmdd hh:mm:ss ssdd RTS SDM Base Maintenance
SDM state change to INSV
From:  <old_state>
```

Field descriptions

The following table describes each field in the log report:

Field	Value	Description
old_state	ManB, SysB or ISTB	Indicates the previous state of the SDM.

Action

There is no action required.

Associated OM registers

There are no associated OM registers.

Additional information

There is no additional information.

SDM502

The system generates log report SDM502 when the SuperNode Data Manager (SDM) high availability (SHA) process updates the run state of the SDM to MANB. The system only send this report to the Operations support system (OSS). The user cannot view SDM502 at the SDM remote maintenance menu. The OSS displays the format and example in the same way as the descriptions that follow. The log that the custlog file stores has a slightly different format.

Format

The log report format for SDM502 is as follows:

```
SDM502 mmmdd hh:mm:ss ssdd MANB SDM Base Maintenance
SDM state change to MANB
From: <old_state>
```

Field descriptions

The following table describes each field in the log report:

Field	Value	Description
old_state	INSV, SYSB ISTB, or OFFL	Indicates the previous state of the SDM.

Action

There is no action required.

Associated OM registers

There are no associated OM registers.

Additional information

There is no additional information.

SDM503

Log report SDM503 is generated when the high availability (SHA) process updates the run state of the SDM node to SYSB. The system only sends this report to the operations support system (OSS). The user cannot view SDM503 at through the node's maintenance interface. The OSS displays the format and example in the same way as the descriptions that follow. The log that the custlog file stores has a slightly different format.

Format

The format for log report SDM503 is as follows:

```
SDM503 mmmdd hh:mm:ss ssdd SYSB SDM Base Maintenance
SDM state change to SYSB
From: <old_state>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
old_state	INSV, MANB, or ISTB	Indicates the previous state of the SDM node.

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.

SDM504

Log report SDM504 is generated when the high availability (SHA) process updates the run state of the SDM node to TBL. The system only sends SDM504 to the operations support system (OSS). The user cannot view this report at the node's remote maintenance menu. The OSS displays the format and example in the same way as the descriptions that follow. The log that the custlog file stores has a slightly different format.

Format

The format for log report SDM504 is as follows:

```
SDM504 mmmdd hh:mm:ss ssdd TBL SDM Base Maintenance
SDM state change to ISTB
From: <old_state>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
old_state	INSV, MANB, or SYSB	Indicates the previous state of the SDM node.

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.

SDM505

The subsystem generates log SDM505 when the SuperNode Data Manager (SDM) high availability (SHA) process updates the SDM run state to offline. The system sends this log to the operations support system (OSS). The user cannot view this report at the SDM remote maintenance menu. The log that the custlog file stores has a slightly different format than the following one.

Format

The log report format for SDM505 is as follows:

```
SDM505 mmmdd hh:mm:ss ssdd OFFL SDM Base Maintenance
SMD state change to OFFL
From: <old_state>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
old_state	MANB	Indicates the previous state of the SDM is MANB.

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.

SDM550

Log report SDM550 generates when a change in the SDM node status occurs. A change in the SDM node status results from state changes to one or more of the following:

- SDM node
- SDM hardware device (fault-tolerant platform only)
- software component
- application

Generation of this log with a critical alarm code (***) occurs for the following conditions:

- all C-side links are out of service
- the SDM node is declared a major or critical babbler
- SDM local node maintenance is not responding to polls from central node maintenance
- SDM local node maintenance is reporting a SysB condition

Generation of this log with a minor alarm code (*) occurs when the state of the SDM node is set to ISTb or ManB.

The ISTb state occurs when:

- the SDM node is declared a minor babbling node
- SDM local node maintenance reports an ISTb condition

Format

The format for log report SDM550 is as follows:

```
<log_off_id> <alarm code> SDM550 mmmdd hh:mm:ss ssdd INFO Node
Status Change
    Node: <node>
    Status: <current status> from <previous status>
    Reason: <reason text>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_off_id	character string (maximum 12 characters)	Specifies the name for office identification in the log output header.
alarm code	***	*** indicates that a critical alarm triggered the log.
	**	** indicates that a major alarm triggered the log.
	*	* indicates that a minor alarm triggered the log.
		indicates that an alarm did not trigger the log.
node	SDM, followed by a number	The SDM node number. The number follows the value SDM.
current status	character string (maximum 13 characters)	Indicates the current state and alarm severity at the SDM level of the RMI alarm banner at the time the log was generated. The state can have the following values: • Uneq (unequipped) • OffL (offline) • ManB (manual busy) • InSv (in service) • ISTb (in-service trouble) • SysB (system busy)

Field	Value	Description
		If there is not communication between the SDM node and the Core, the ManB and SysB states will be replaced by ManB (NA) and SysB (NA). The alarm severity will be ***, **, *, or blank. The severity depends on whether the alarm severity at the SDM level of the RMI is critical, major, minor, or none.
previous state	character string (maximum 13 characters)	Indicates the previous state and alarm severity at the SDM level of the RMI alarm banner before the log was generated. Values are identical to the current status.
reason text	optional character string	Indicates the reason for the SDM node state change. (Optional field.)

Action

To isolate and correct the problem, refer to the *Fault Management* documentation for this node.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM600

The system generates log report SDM600 when SuperNode Data Manager (SDM) establishes connectivity again. The SDM establishes connectivity from one of the following:

- operating company LAN
- computing module (CM)

The heartbeat mechanism reports the CM connectivity. A ping test reports the operating company LAN connectivity to the operating company LAN. The system generates SDM600 after the detection and correction of a failure.

The format and example shown are for the operations support system (OSS) version of the log. The SDM remote maintenance interface (RMI) also displays the log report.

Format

The log report format for SDM600 is as follows:

```
<log_off_id> SDM600 mmmdd hh:mm:ss ssdd INFO SDM Base
Maintenance
Connection has been established
Type: <type>
<info>
```

Field descriptions

The following table describes each field in the log report:

Field	Value	Description
log_off_id	character string (maximum 12 characters)	Specifies the name for office identification in the log output header.

Field	Value	Description
type	CMorLAN	Indicates the point where the SDM establishes connectivity again.
info	character string	Indicates the reason SDM establishes connectivity again. For type=CM: CM Link Up:, and one of the following messages: • CM receives heartbeat • connect msg from the CM • restart warm msg from the CM • restart cold msg from the CM • restart reload msg from the CM • norestart swact msg from the CM • CM-SDM IP address mismatch condition clears • ds512 link(s) open For type=LAN: • Host Name: <node name as operating company defines at commissioning time>

Action

There is no action required.

Associated OM registers

There are no associated OM registers.

Additional information

There is no additional information.

SDM601

The system generates log report SDM601 when the maintenance system detects that mirroring was re-established after a logical volume mirroring failure.

Note: This system does not generate this log for Telecom 05.

Format

The log report format for SDM601 is as follows:

```
SDM601 MAY30 12:42:44 5641 INFO SDM Base Maintenance
Logical volume(s) are mirrored
Volume group name: <volume_group_name>
```

Field descriptions

The following table describes each field in the log report:

Field	Value	Description
volume_group_name	character string	Indicates which logical volume is mirrored.

Action

There is no action required.

Associated OM registers

There are no associated OM registers.

Additional information

There is no additional information.

SDM602

The system generates log report SDM602. The system generates this report when the SuperNode Data Manager (SDM) maintenance system detects that a system resource threshold is within set limits. These limits include CPU, number of processes, swap space, number of zombie processes, swap queue entries, and disk space.

Format

The log report format for SDM602 is as follows:

```
SDM602 mmmdd hh:mm:ss ssdd INFO SDM Base Maintenance
Resource is within set limit
Type: <resource type>
<Name: resource name>
```

Field descriptions

The following table describes each field in the log report:

Field	Value	Description
resource type	character string	Indicates which resource falls below the threshold. The values are as follows: • CPU • number of processes • swap space • number of zombie processes • number of swap queue entries • logical volume
resource_name	character string	Indicates which logical volume exceeds the threshold. This field is only present when the logical volume resource is reported.

Action

There is no action required.

Associated OM registers

There are no associated OM registers.

Additional information

There is no additional information.

SDM603

Log report SDM603 indicates that the SDM303 alarm has been cleared. This log may also indicate a state change has occurred that does not require manual intervention to clear.

Format

The format for log report SDM603 is as follows:

```
MSH10_I06BE      SDM603 APR22 12:21:05 6755 INFO SDM Base Maintenance
       Package: SDM_ETA.eta
       Process: start_eta_server
        Reason: Trouble condition cleared. Service now available
```

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.

SDM604

The SuperNode Data Manager (SDM) Log Delivery application generates log report SDM604. The system generates this report when the computing module (CM) discards logs because it does not have enough CPU time to format the logs. This condition also appears in the following message:

```
— WARNING: 22 REPORTS NOT PRINTED
```

Format

The log report format for SDM604 is as follows:

```
<switch_name> SDM604 mmmdd hh:mm:ss <sequence_number> INFO
    Log Delivery Service: lost logs (CM side): <number_lost>
```

Field descriptions

The following table describes each field in the log report:

Field	Value	Description
sequence_number	four-digit numeric	Specifies the sequence number.
number_lost	five-digit numeric	Indicates the number of logs lost.

Action

The switch discards logs under normal traffic conditions. If a large number of logs are lost, check DLOG for an indication of the problem.

Associated OM registers

There are no associated OM registers.

Additional information

There is no additional information.

SDM605

Log report SDM605 indicates logs for a specific application have been lost.

Format

The format for log report SDM605 is as follows:

```
SDM605 SEP27 14:09:36 5829 INFO
   Log Delivery Service: 5 logs lost for application
   LogAdaptor on host msh mg9k
```

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

The Log Delivery Service will identify the lost logs based on the sequence numbers coming along with the Customer logs. If the sequence number is mismatched with the expected sequence, then there will be a lost log generation.

For example, if the Log delivery application reads a log for an application (e.g. LogAdapter from MG9k) with sequence number 1000, then the next expected sequence number for this particular application is 1001. If Log Delivery reads something greater than 1001, like 1004, it means that there has been loss of 2 logs (sequence number: 1002, 1003). In this case the Log Delivery generates a SDM605 log stating that "2 logs lost for application LogAdapter from MG9K".

This log can be generated during network congestion / outage or during SDM/CBM outages / upgrade.

SDM607

The SuperNode Data Manager (SDM) generates log report SDM607. The system does not send SDM607 to the operations support system (OSS), the report is for SDM internal use only. The user can refer to the SDM607 report from the remote maintenance interface (RMI), when logged on to the SDM. The SDM607 report indicates when a process controller starts or restarts a process. The SDM607 does not have a header.

Note: The SDM607 report does not generate for Telecom 06 and up.

Format

The log report format for SDM607 is as follows:

```
SDM607
Package: <package_name>
Process: <process_name>
State:  <action>
Day mmm dd hh:mm:ss yyyy
```

Field descriptions

The following table describes each field in the log report:

Field	Value	Description
package_name	character string	Indicates which package had the failure.
process_name	character string	Indicates which process in the package has failed.
action	started or restarted	Indicates that a process controller has started or restarted a process.

Action

There is no action required.

Associated OM registers

There are no associated OM registers.

Additional information

There is no additional information.

SDM608

Log report SDM608 indicates that an I-tape or S-tape process has completed.

Format

The format for log report SDM608 is as follows:

```
MSH10_I06BE      SDM608 APR22 12:19:16 6639 INFO SDM Base Maintenance
        SDM Backup status cleared by user.
```

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.

SDM609

The subsystem generates log SDM609 when the maintenance system detects a hardware device has returned to the in-service (InSv) state. The maintenance system is on a fault-tolerant SuperNode Data Manager (SDM).

Format

The log report format for SDM609 is as follows:

```
SDM609 mmmdd hh:mm:ss ssdd INFO SDM Base Maintenance
Hardware device in-service
Device: <device identifier>
```

Field descriptions

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

Field	Value	Description
device identifier	character string	This field identifies the device that is out of service. It contains a three-letter device symbol, followed by an optional device code and the device domain in parentheses. The values for the device symbol are as follows: • CPU • FAN • ICM • DSK • DAT • ETH • 512

Field	Value	Description
		Note: There can be two Ethernet devices, ETH1 or ETH2. The device code appears only when the device symbol is DSK and more than one disk pair is present. The device code denotes one of the following disk pairs: • 1 to 9 for disk pairs 1 through 9 • A for the 10th disk pair • B for the 11th disk pair The device domain is either 0 or 1.

Action

There is no action required.

Associated OM registers

There are no OM registers.

Additional information

There is no additional information.

SDM610

For the SDM610 log, this section numbers each Explanation for a corresponding numbered Format of the log.

Explanation 1

A patch application failed.

Explanation 2

Critical patch failure. Up to five failed patch applications can occur during a single session. If a sixth failed patch application occurs during the same session, the critical alarm is raised and the patching tool exits. No further patching transactions are allowed.

Explanation 3

A reboot or SWACT failed during a patching transaction.

Format

Formats for log report SDM610 follow:

Format 1

```
*SDM610 Software Apply
<patch ID> <failure reason>
cbm850=<node>; NODE=<node>; CLASS=SWIM; SWIMTYPE=Patch;
STATUS=Failed; ID=<patch ID>
<date> <time>
```

Format 2

```
***SDM610 Software Apply
Too many failed patches.
cbm850=<node>; NODE=<node>; CLASS=SWIM; SWIMTYPE=Patch;
STATUS=Notification; ID=Count
<date> <time>
```

Format 3

```
*SDM610 Software Apply
<patching notification reason>
cbm850=<node>; NODE=<node>; CLASS=SWIM; SWIMTYPE=Patch;
STATUS=Notification
<date> <time>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<patch ID>	Variable	Identifies the patch that failed.
<failure reason>	Variable	One of the following reasons for the failure: - "Failed to apply." - "Failed integrity check."
<patching notification reason>	variable	One of the following reasons for the notification: - "Inactive local reboot refused." - "Failed reboot." - "Active node failed reboot." - "Inactive node failed reboot." - "Inactive node failed local reboot." - "SWACT command failed." - "SWACT refused." - "Unexpected SWACT occurred."
<node>	Variable	Identifies the node on which the problem occurred.
<date>	www mmm dd	Date: day of week, month and date
<time>	hh:mm:ss yyyy	Time: hours, minutes, seconds, and year

Action

This section associates an action to be performed in response to each numbered explanation.

Action 1

Contact the next level of support to determine the reason for the patching failure. The alarm will clear upon successful application of the patch (PatchID) specified in the alarm.

Note: Other patching transactions will still be allowed if less than six of these alarms are raised.

Action 2

You must contact the next level of support for assistance since no further patching transactions will be allowed.

Action 3

You must contact the next level of support for assistance since the patches applied before this failure or notification have been compromised.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM614

Log report SDM614 is generated when a DS512 link up is reported on the SDM.

Format

The format for log report SDM614 is as follows:

```
SDM614 <mmmdd hh:mm:ss ssdd> INFO SDM BASE MAINTENANCE
   DS512 LINK UP
   MODULE LOCATION: <shelf name>, SLOT: <slot number>
   PORT: <port num>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Shelf name	4-character alphanumeric	Indicates the main (SDMM) or expansion (SDME) shelf
Slot number	2-digit alphanumeric	Indicates the slot number of the DS512 module.
Port num	1-digit numeric	Indicates the port number for the link.

Action

No action is required for this log.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM615

The SDM Exception Reporting Application generates a warning report at 8:00 a.m. local time when the system generates thresholded logs within the preceding 24 h. The report includes the log types and numbers of all such logs during the reporting period. Thresholding causes the following limitations for SDM Exception Reporting:

- System -level counts are lowered because thresholding reduces the number of logs received by the Exception Reporting Application.
- Component-level counts for C1/C1P logs are affected because component information is lost when logs are thresholded.

Format

The format for log report SDM615 is as follows:

```
<switch name> SDM615 mmmdd hh:mm:ss ssdd INFO
Threshold Conflict
Event: Log Thresholding in effect for logs managed
by Exception Reporting application - Exception
Reports may be inaccurate
Action: Disable thresholding via LOGUTIL for fol-
lowing reports: <Thresholded Log>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Thresholded Log	8 alphanumeric	Indicates a log type and log number thresholded through LOGUTIL which the Exception Reporting Application receives.

Action

Use LOGUTIL to disable thresholding for logs indicated in the report.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM616

The SDM Log Delivery application generates this log report when the following happens:

- a TCPIN device is defined to accept a TCP/IP connection from a remote application, such as an OSS, and
- the TCPIN device has the validate address field set. When the validate address field is set, the Log Delivery application accepts only one connection from the specified hostname, and
- an application that is not authorized tries to connect to a specified port number (An application is not authorized when it does not run on a machine with the same IP address as the address in the validation field.) or
- a second connection attempt occurs after a valid address connection is fully operational

Format

The format for log report SDM616 is as follows:

```
<log_off_id> SDM616 mmmdd hh:mm:ss ssdd INFO Connection
Refused
Event: <event>
Reason: <reason>
Calling Address: <IP_address>
Port:<port_number>
Action:<action>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_off_id	character string (maximum 12 characters)	Specifies the name for office identification in the log output header
event	character string	Indicates that a log delivery connection attempt was rejected

Field	Value	Description
reason	character string"Invalid calling address "or" Connection already established from IP"	Indicates the reason why the log delivery connection failed
IP_address	character string maximum 15 characters	Indicates the IP_address of the remote entity that has been refused connection
port_number	character string maximum 5 characters	Indicates the port number on which the connection has been refused
action	character string "Verify configuration data via logroute utility"	Indicates the suggested action

Action

Verify configuration data using logroute utility.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM617

Log report SDM617 indicates that a DCE problem has been cleared.

Format

The format for log report SDM617 is as follows:

```
MSH10_I06BE      SDM617 APR22 12:20:39 6753 INFO SDM Base Maintenance
        DCE problem cleared
```

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.

SDM618

The system generates log report SDM618 when the size of the /var logical volume reaches 95% on the disk. All log files, from the current day to seven days previous to the current day, are deleted when /var logical volume is 95% full. These log files include trouble logs, state change logs, and information logs.

Format

The format for log report SDM618 is as follows:

```
mmmdd hh:mm:ss <node_name> syslog: SDM618 NONE INFO SDM
Base Maintenance <info1> <disk_percentage_full> <info2>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
node_name	alphanumeric character string	Identifies the terminal.
info1	mandatory character string (maximum 22 characters)	Specifies “Logical volume /var is"
disk_percentage_full	mandatory integer string (maximum 3 digits)	Indicates the disk full percentage. The value is between 95 and 100%.
info2	mandatory character string (maximum 54 characters)	Specifies “percent full. log files in /var/adm have been deleted."

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.

SDM619

The system generates log report SDM619 when theOMAccess Server detects a corrupt operational measurements (OM) Group during an OM Schema download.

A corrupt OM Group can occur if a software error on the computing module (CM) side causes data corruption when the CM defines an OM Group. If the system downloads a corrupt OMGroup to the SDM, the OMAccess Server on the SDM detects the corrupt OM Group. The OM Access Server then generates log report SDM619. The OM Access Server automatically downloads another OM Schema and omits the corrupt OM Group.

Format

The format for log report SDM619 is as follows:

```
SDM619 mmmdd hh:mm:ss <node name> syslog: SDM619 NONE INFO
Event:
OM Access Service detected a possible corrupt OM Group during
schema download. New schema download started excluding
GroupName: <text info> GroupId: <integer>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
node name	alphanumeric character string	Identifies the terminal.
syslog: SDM619	constant	Indicates that the system has generated log report SDM619.
NONE	constant	Indicates the severity of the alarm. Log report SDM619 has no alarm value.
INFO	constant	Indicates that log report SDM619 is an information-only log. No action is required.
Event	constant	Indicates that the OM Access Server detected a corrupt OM Group.

Field	Value	Description
text info	mandatory, variable character string (maximum 8 characters)	Identifies the GroupName of the corrupt OM Group.
integer	mandatory, variable numeric string with value 0 to 999 (maximum 3 digits)	Identifies the GroupId of the corrupt OM Group.

Action

This log report requires no action. The OM Access Server corrects the problem automatically.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDM620

The SDM Maintenance Manager (SMM) generates this log to report current SDM system performance data. The performance data includes CPU usage, number of processes, swap space occupancy, and logical volume occupancies.This log is generated according to a pre-defined time interval.

Format

The format for log report SDM620 is as follows:

```
<log_off_id> SDM620 mmmdd hh:mm:ss <logID> INFO SDM
Performance log
<O/S SI name> <O/S value> <O/S SI name> <O/S value>
...
<LV name> <LV SI value> <LV name> <LV SI value>
...
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_off_id	character string (maximum 12 characters)	Specifies the name for office identification in the log output header
O/S SI name	RunQueueNumProcsNumZombiesSwpSpaceorSwpQueue	Indicates the operating system (OS) status indicator (SI) being reported
O/S value	0-999	Indicates the value of O/S status indicators
LV name	variable character string (maximum 256 characters)	Indicates the name of the logical volume being reported
LV SI value	0-100	Indicates value of the logical volume status indicators

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.

SDM621

Log report SDM621 is generated at the end of a split-mode upgrade.

Format

The format for log report SDM621 is as follows:

```
SDM621 MAY12 13:42:22 0349 INFO SDM Base Maintenance
Split-system upgrade ended.
Status: <status>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<status>	One of the following text strings: • `successfully completed` • `fallback occurred`	Identifies whether the upgrade has successfully completed or a fallback has occurred

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.

SDM622

Log report SDM622 is generated when the system reaches the maximum size for a file device configured through the Logroute tool.

Format

The format for log report SDM622 is as follows:

```
officeid SDM622 mmmdd hh:mm:ss #### INFO
<application name>:<max size action>
   File device name: <filename>
   Reason: <reason>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
officeid	alphanumeric	This field indicates the switch that generated the log.
mmmdd	alphanumeric	This field identifies the month and date the log was generated.
hh:mm:ss	numeric	This field indicates the hour, minutes, and seconds the log was generated.
####	numeric	This variable indicates the sequential number of the log generated.
application name	alphanumeric	This variable indicates the application that generated the log.
max size action	alphanumeric	This variable indicates the action the system takes when the file reaches its maximum size.
filename	alphanumeric	This variable indicates the name of the file device stopped by the system when the file device reaches its maximum size.
reason	alphanumeric	This variable explains why the system performed the action indicated in the max size action field.

Action

When the system generates log report SDM622, there are two possible reasons:

- The operating company personnel did not configure enough space for the file devices.
- There is a software error that is causing the production of a large number of logs.

If the operating company personnel did not configure enough space, change the maximum size (Mbyte) of the file device. Check the maximum size of the file device in the Logroute tool.

If the problem is a software error, contact that next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

Operating company personnel can configure the maximum size of the file device using the Logroute tool. Configure the maximum file size to prevent disk overflow. The maximum size of the file device is a global parameter.

SDM625

Log report SDM625 indicates that the connection to a Network Management component in a given domain has been re-established.

Format

The format for log report SDM625 is as follows:

```
MSH10_I06BR      SDM625 JUN11 17:09:20 1822 INFO Passport Log Streamer
        Connection to 10.102.4.15 has been established.
```

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.

SDM626

Log report SDM626 is an information only log. This log is generated whenever the OMDD application starts and detects that the tuple number option has changed state since the last time the application was launched. This log is used to inform the OSS of the state change which signifies a change in the OMDD CSV files. This log also indicates the new (current) state as being either ACTIVATED or DISABLED.

Format

The format for log report SDM625 is as follows:

```
MSH10_I06BR      SDM626 JUN26 13:46:32 3456 INFO OM Data Delivery -  Tuple
number option has been DISABLED

MSH10_I06BR      SDM626 JUN26 13:49:06 3641 INFO OM Data Delivery -  Tuple
number option has been ACTIVATED
```

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.

SDM627

The subsystem generates log SDM627 when a Network Time Protocol (NTP) problem is cleared.

Format

The SDM format for log report SDM627 is as follows:

```
RTP_com4iems    SDM627 SEP17 20:09:15 5984 INFO SDM
        Base Maintenance
        NTP problem cleared
```

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.

SDM630

The subsystem generates log SDM630 to indicate the SDM Routine EXercise (REX) start and stop time.

Format

The log report formats for SDM630 are as follows:

REX started

```
RTP_com4iems    SDM630 SEP18 11:22:15 1724 NONE INFO
SDM REX started
```

REX complete

```
RTP_com4iems    SDM630 SEP18 11:22:15 1724 NONE INFO
SDM REX complete
```

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.

SDM632

Log report SDM632 indicates that the system audit failure reported through log SDM332 has been cleared.

Format

The format for log report SDM632 is as follows:

```
SDM632 FEB11 03:03:49 9978 INFO SDM Base Maintenance
   SDM System Precheck failure is cleared.
```

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.

SDM633

Log report SDM633 indicates a change in the messaging condition of a DS512 or OC-3 link between the SDM or Core and Billing Manager 800 (CBM 800) and the message switch (MS).

Format

The format for log report SDM633 is as follows:

```
SDM633 DEC03 13:04:49 3811 INFO SDM Base Maintenance
   Link Condition Change
   Link: domain 1 port 0 (ms 0 link 1)
   From: open
   To: closed
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Link:	domain 0 port 0 (ms 0 link 0) domain 0 port 1 (ms 1 link 0) domain 1 port 0 (ms 0 link 1) domain 1 port 1 (ms 1 link 1)	The domain and link of the affected DS512 or OC-3 communication link.
From:	closed mtc-open open	previous link condition
To:	closed mtc-open open	new link condition

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.

SDM634

Log report SDM634 indicates that the error condition indicated by log SDM334 has been cleared. The log is generated if a good signal is restored to the ports of the OC-3 card.

Format

The format for log report SDM634 is as follows:

```
SDM634 OCT22 14:14:26 6027 INFO SDM Base Maintenance
   OC3 Card Fault Cleared
   Link: domain 0 port 0 (ms 0 link 0)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Link	domain 0 port 0 (ms 0 link 0) domain 0 port 1 (ms 1 link 0) domain 1 port 0 (ms 0 link 1) domain 1 port 1 (ms 1 link 1)	The link that had reported the problem.

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.

SDM635

Log report SDM635 indicates that the problem indicated by log SDM335 has been cleared. The log is generated when the link condition problem has cleared.

Format

The format for log report SDM635 is as follows:

```
SDM635 OCT22 14:20:26 6027 INFO SDM Base Maintenance
   Link Fault Cleared
   Link: domain 0 port 0 (ms 0 link 0)
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
link:	domain 0 port 0 (ms 0 link 0) domain 0 port 1 (ms 1 link 0) domain 1 port 0 (ms 0 link 1) domain 1 port 1 (ms 1 link 1)	The link that reported the problem.

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.

SDM636

Log report SDM636 indicates that the core heartbeat recovered and the heartbeat alarm has been cleared.

Format

The format for log report SDM636 is as follows:

```
SDM636 OCT22 14:27:59 6061 INFO Alarm raised or updated.
   Heartbeat alarm
   TimeStamp: Fri Oct 22 14:09:40 2004
   ComponentID: CLASS=NET;NETTYPE=CORE
   Category: Communications
   Probable Cause: noProbableCause
   Specific Problem: Heartbeat response received.
```

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.

SDM650

The subsystem generates log SDM650 when central SuperNode Data Manager (SDM) link maintenance requests that a failed link maintenance action is recorded. The system testing of a link is an example of a link maintenance action. The subsystem generates this log by the fault-tolerant platform only.

Format

The format for log report SDM650 is as follows:

```
BFCC108AJ SDM650 MAY06 16:44:06 4400 INFO SDM Link Report
SDM 0 DOMAIN 1 PORT 0 (MS 0 CARD 15 LINK 1)
Link Mtce Action: Test Request
Link Mtce Result: Fault found on link
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_off_id	character string (maximum 12 characters)	Specifies the name for office identification in the log output header.
link description	character string (maximum 72 characters)	Indicates link connection from the SDM to the CM.

Field	Value	Description
link mtce action	character string (maximum 18 characters)	Indicates a request made to SDM link maintenance. The value can be one of the following: • Open Request • Close Request • Mtce Open Request • Test Request
link mtce result	character string (maximum 24 characters)	Indicates the result of the request made to the SDM link maintenance. The value can be one of the following: • Failed to close link • Fault found on link • Failed to open link • Failed to mtce open link • Failed to test link

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.

SDM700

Log report SDM700 reports a Warm, Cold, or Reload restart or a norestartswact on the core.

Format

The format for log report SDM700 is as follows:

```
SDM700 SEP14 18:01:42 2988 INFO SDM Base Maintenance
WARM Restart occurred on the core
Type: CM
INFO: Check INIT log on the Core

SDM700 SEP14 18:01:42 2988 INFO SDM Base Maintenance
COLD Restart occurred on the core
Type: CM
INFO: Check INIT log on the Core

SDM700 SEP14 18:01:42 0117 INFO SDM Base Maintenance
RELOAD Restart occurred on the core
Type: CM
INFO: Check INIT log on the Core

SDM700 SEP14 18:01:42 3097 INFO SDM Base Maintenance
NORESTARTSWACT occurred on the core
Type: CM
INFO: Check INIT log on the Core
```

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.

SDM739

Log report SDM739 indicates file transfers between the FTP Client and the CORE and shows user log-ins to the CORE.

Format

The format for log report SDM739 is as follows:

```
mmdd hh:mm:ss sspfs_server ftpd[20103]: SDM739 NONE INFO FTS
ftp-user request for file PML successful
```

Selected field descriptions

NA

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.

SDMB300

Log report SDMB300 is generated when memory allocation fails.

Format

The format for log report SDMB300 is as follows:

```
SDMB300 <mmmdd hh:mm:ss ssdd>FLT SDM BILLING SYSTEM
    STREAM= <stream>: <48_character_text_string>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	stream name or “ALL"	Identifies the billing stream affected.
48_character_text_string	Variable	Identifies the billing problem encountered.

Action

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.

SDMB310

Log report SDMB310 is generated for problems related to communications with the Core.

Format

The format for log report SDMB310 is as follows:

```
SDMB310 <mmmdd hh:mm:ss ssdd>FLT SDM BILLING COMMS
STREAM= <stream>: <48_character_text_string>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	stream name or “ALL"	Identifies the billing stream affected
48_character_text_string	Variable	Identifies the billing problem encountered

Action

Determine the reason that the SuperNode Data Manager (SDM) node is not communicating with the Core. Determine if the node and Message Switch (MS) and Frame Transport Bus (FBus) are In Service (InSv) or In-Service Trouble (IsTb). If the node is InSv or IsTb, return the billing stream to service.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB315

Log report SDMB315 is generated for general software-related problems.

Format

The format for log report SDMB315 is as follows:

```
SDMB315 <mmmdd hh:mm:ss ssdd>TBL SDM BILLING SOFT ERROR
    STREAM= <stream>: <48_character_text_string>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	stream name or “ALL"	Identifies the billing stream affected
48_character_text_string	Variable	Identifies the billing problem encountered

Action

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.

SDMB316

Log report SDMB316 is generated when any of the following SBA processes on the CM are manually killed:

- BUFAUDI
- BUFAUDIT
- BUFCABKI
- BUFDEVP
- BUFPROC
- BUFRECI
- SBCPROCI
- SBMTSTRI

Format

The format for log report SDMB316 is as follows:

```
SDMB316 <mmmdd hh:mm:ss ssdd>FLT SDM BILLING PROC DEATH
   STREAM= <stream>: <48_character_text_string>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	stream name or “ALL"	Identifies the billing stream affected.
48_character_text_string	Variable	Identifies the billing problem encountered.

Action

For SDM Billing to work correctly, start the process again.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB320

Log report SDMB320 is generated for backup-related problems that affect more than one file.

Format

The format for log report SDMB320 is as follows:

```
SDMB320 <mmmdd hh:mm:ss ssdd>TBL SDM BILLING BACKUP
    STREAM= <stream>: <48_character_text_string>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	stream name or “ALL"	Identifies the billing stream affected
48_character_text_string	Variable	Identifies the billing problem encountered

Action

You must ensure that backup volumes with enough available space are configured for the stream.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB321

Log report SDMB321 is generated for backup-related problems that affect a file.

Format

The format for log report SDMB321 is as follows:

```
SDMB321 <mmmdd hh:mm:ss ssdd>TBL SDM BILLING BACKUP
    STREAM= <stream>: <48_character_text_string>
    VOLUME= <volume> FILE= <file>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	stream name or “ALL"	Identifies the billing stream affected
48_character_text_string	Variable	Identifies the billing problem encountered
volume	Variable	Identifies the disk volume
file	Variable	Identifies the file on the volume

Action

You must ensure that the backup volume is not busy or full.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB350

Log report SDMB350 is generated when a SuperNode Billing Application (SBA) process reaches a death threshold and makes a request to restart. A death threshold occurs after a process has died more than 3 times less than 1 minute apart.

Format

The format for log report SDMB350 is as follows:

```
SDMB350 AUG19 17:51:24 1234 FLT SDM BILLING CONTROL
STREAM= <stream> : <48_character_text_string>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<text>	The system restarts the SBA after multiple process deaths.	An SBA error recovery algorithm restarts the application if a process dies multiple times within a short time period.
	Excessive process deaths occur in SBA	The system produces this log when processes in the SBA die at a slow rate. Normally the system does not generate other logs. This log indicates that multiple SBA process deaths occurred within the last hour.

Action

Investigate the SBA process death. The SBA will automatically restart itself. Watch logs that indicate that SBA is in normal operation. If the system generates this log more than once, 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.

SDMB355

This section numbers each Explanation and associates it with a corresponding numbered Format.

Explanation 1

Problems writing records (by stream)—The SDMB subsystem generates this log when some disk problem prevents the writing of records. This log is associated with the raising alarm DSKWR.

Explanation 2

Problems writing to disk—The SDMB subsystem generates this log when the Record Client/FileManager is unable to write to the disk.

Explanation 3

Critical disk utilization—The SDMB subsystem generates this log when the disk use has risen above the critical threshold specified in the MIB in parm. This log is associated with the raising alarm LODSK.

Explanation 4

Major disk utilization—The SDMB subsystem generates this log when the disk use has risen above the major threshold. This log is associated with the raising alarm LODSK.

Explanation 5

Minor disk utilization—The SDMB subsystem generates this log when the disk use has risen above the minor threshold. This log is associated with the raising alarm LODSK.

Explanation 6

This log has two possible causes: 1) the disk is full because billing files have not been sent downstream and a large number of the files have accumulated in the closedNotSent directory; the maximum number of files to hold billing records for a billing stream is 15000; 2) a large number of processed files have been retained on the core manager because the billing files are not being purged periodically; common

mis-configurations that greatly accelerate the accumulation of small processed files include:

- an oversized logical volume
- shortest rotation criteria of five minutes, from open to unprocessed, selected
- low billing traffic (BBHCA)

Explanation 7

This log is generated when the SBA can not close or open a file.

Explanation 8

This log indicates that there is some disk problem preventing the writing of records.

Format

Formats for log report SDMB355 follow:

Format 1

```
SDMB355 <date> <time> TBL SDM Billing Disk
     STREAM=<stream>: UNABLE TO WRITE RECORDS TO FILE
```

Format 2

```
SDMB355 <date> <time> TBL SDM Billing Disk
     STREAM=<stream>: DISK WRITE FAILURE: <details>
```

Format 3

```
*** SDMB355 <date> <time> AUG19 17:51:24 TBL SDM Billing Disk
     STREAM=<stream>: CRITICAL: DISK UTILIZATION
```

Format 4

```
** SDMB355 <date> <time> TBL SDM Billing Disk
     STREAM=<stream>: MAJOR: DISK UTILIZATION
```

Format 5

```
* SDMB355 <date> <time> TBL SDM Billing Disk
     STREAM=<stream>: MINOR: DISK UTILIZATION
```

Format 6

```
* SDMB355 <date> <time> TBL SDM Billing Disk
     STREAM=<stream>: Reached limit for disk space or number
                      of files.
```

Format 7

```
* SDMB355 <date> <time> TBL SDM Billing Disk
     STREAM=<stream>: CLOSE AND OPEN FILE FAILED
```

Format 8

```
* SDMB355 <date> <time> TBL SDM Billing Disk
     STREAM=<stream>: FLUSH FILE FAILED
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<date>	mmmdd	Date: month and day
<time>	hh:mm:ss	Time: hours, minutes, and seconds
<stream>	Variable	Identifies the stream where the problem occurred.
<details>	Variable	Additional information on problem

Action

This section associates the Action with each numbered explanation.

Action 1

Check the disk space on the SuperNode Data Manager (SDM) hardware. You may need to FTP files or may need to clean up the disk.

Action 2

Check the disk space on the SDM hardware. You may need to FTP files or may need to clean up the disk.

Action 3

Check to see if files are being sent FTP. If not, set the system up to FTP files or back up the files.

Action 4

Check to see if files are being sent FTP. If not, set the system up to FTP files or back up the files.

Action 5

Check to see if files are being sent FTP. If not, set the system up to FTP files or back up the files.

Action 6

Check to see if files are being sent through FTP. If files are not being sent, set the system up to FTP files or back up the files. If the files are being sent, a MIB value is not properly set and you should contact Nortel technical support for assistance.

Action 7

Check to see if files are being sent FTP. If not, set the system up to FTP files or back up the files. Moreover, check file permissions for the destination directories.

Action 8

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.

SDMB360

The SuperNode Data Manager Billing (SDMB) subsystem generates log SDMB360 when it loses and cannot restore the connection to the Persistent Store System (PSS). This log is associated with the alarm SDM Billing Application Interface (SBAIF).

Format

The log report format for SDMB360 is as follows:

```
SDMB360 mmmdd hh:mm:ss ssdd TBL SDM BILLING COMMS
STREAM=<stream>:
<file transfer mode> - <error msg>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	variable	Identifies the stream where the problem occurred.
file transfer mode	IFT, OFT	Indicates the file transfer mode: Inbound or Outbound.
error msg	constant	Connection to File Client Unavailable

Action

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.

SDMB366

Log report SDMB366 is generated when an error condition exists on the SDM.

Format

The format for log report SDMB366 is as follows:

```
SDMB366 <date> <time> <seq #> TBL SDM BILLING
STREAM=ALL: SBA STARTUP FAILURE: <error msg>
```

Selected field descriptions

NA

Action

Contact your next level of support. If the installed SBA supports multiple stream record formats, you can continue to process streams of the unlogged formats.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB365

Log report SDMB365 is generated when a serious problem prevents creation of the named stream. This log is generated when a new version of the SuperNode Billing Application (SBA) product does not support a stream format on an active stream that was present in a previous load.

Format

The format for log report SDMB365 is as follows:

```
SDMB365 <date> <time> <seq#> TBL SDM BILLING
STREAM= <stream>: <48_character_text_string>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<date>	mmmdd	Date: month and day
<time>	hh:mm:ss	Time: hours, minutes, and seconds
<seq#>	4 digits (ssdd)	Sequence number of log
<stream>	ALL or variable	ALL - for system-wide logs not applicable to a specific stream. <Stream> - a stream that exists on the switch.

Action

Revert to the previous running version of SBA. If you removed the support for the stream format in the new release, turn off the stream before installing the new version. If the new version is supposed to support all existing streams, contact Nortel for the latest appropriate software.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB367

This section numbers each Explanation and associates it with a corresponding numbered Format.

Explanation 1

The SDMB subsystem generates this log when a trappable Management Information Base (MIB) object is set. The modification of some MIB objects provides notification of failures to the system manager by way of a trap. Because there is no system manager, the system logs messages. Consideration for separate streams is not built into the Automatic Accounting Data Networking System (AMADNS) MIB specification.

Note: The MIB associated logs do not accommodate multiple streams.

Explanation 2

The SDMB subsystem generates this log when the maximum bytes by file (rcFileMaxBytesOut), or maximum records by file (rcFileMaxRecsOut), are changed.

Format

Formats for log report SDMB367 follow:

Format 1

```
SDMB367 AUG19 17:51:24 1234 TBL SDM BILLING MIB
STREAM=ALL: WARNING: SET ON MIB OBJECT <OBJECT_NAME>
<SET VALUE>
```

Format 2

```
SDMB367 AUG19 17:51:24 1234 TBL SDM BILLING MIB
STREAM=<stream>: WARNING: SET ON MIB OBJECT
<OBJECT_NAME> <SET VALUE>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<OBJECT NAME>	Name of MIB Object Set	Name of MIB object being set
<SET VALUE>	Set value of Object	Value where you set object
<stream>	ALL or variable	ALL For system-wide logs not applicable to a specific stream. <Stream> The name of the specific stream that is associated with the log.

Action

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.

SDMB370

Log report SDMB370 is generated when the CDR-to-BAF conversion encounters a problem that prevents it from converting CDR to BAF. The SDMB subsystem also raises the critical alarm NOSC because the BAF record was not generated.

The TEXT portion of the log provides the stream name and an explanation of the problem.

Format

The format for log report SDMB370 is as follows:

```
SDMB370 <date> <time> <seq #> TBL SDM BILLING CDR2BAF
   CONVERSION STREAM=<stream>:<specific error>.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Stream	4-character alphanumeric	Identifies the stream on which the problem occurred.
Specific error	Variable length	alphanumeric Provides a brief explanation of the problem.

Action

For the CDRT alarm, the mismatch between the CMCDR Template ID and the CDR MIB CurrentTmpltID must be corrected. If the default fixed template ID of 0 is used, the default CDR MIB value of zero needs to be in the CurrentTmpltID field.

Clear the NOSC alarm.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB375

Log report SDMB375 is generated when a problem occurs during the transfer of a file to the data processing management system (DPMS).

Explanations

This section provides numbered explanations for log report SDMB675. Refer to the corresponding entries in other sections of this report for additional information.

Explanation 1

Log report SDMB375 is associated with problems and alarms related to File Transfer Protocol (FTP).

Explanation 2

Log report SDMB375 is associated with problems and alarms related to Real Time Billing (RTB).

Explanation 3

Log report SDMB375 is associated with problems and alarms related to Automatic File Transfer (AFT).

Explanation 4

Log report SDMB375 is associated with problems and alarms related to Secure File Transfer Protocol (SFTPW).

Formats

This section provides numbered formats for each corresponding Explanation.

Format 1

Format 1 for log report SDMB375 follows:

```
SDMB375 <date> <time> <seq #> TBL SDM BILLING FILE TRANSFER
STREAM=<stream>: <error text>
```

Format 2

Format 2 for log report SDMB375 follows:

```
SDMB375 <date> <time> <seq #> TBL SDM REAL TIME BILLING FILE TRANSFER
STREAM=<stream>: <error text>
```

Format 3

Format 3 for log report SDMB375 follows:

```
SDMB375 <date> <time> <seq #> TBL SDM BILLING FILE TRANSFER
STREAM=<stream>: AFT Alarm Status Change
Session Id: <Session_ID>
Status: <Alarm_level> from <alarm_level>
Reason: <reason>
```

Format 4

Format 4 for log report SDMB375 follows:

```
SDMB375 <date> <time> <seq #> <event type> SDM BILLING FILE TRANSFER
STREAM=<stream>: <destination>: <specific error>
```

Selected field descriptions

This section lists selected field descriptions for each corresponding explanation and format.

Selected field descriptions 1 and 2

The following table lists selected field descriptions

Field	Value	Description
<error text>	variable text	Describes the error that generated the log.

Selected field descriptions 3

The following table lists selected field descriptions

Field	Value	Description
<stream>	variable text	Identifies the billing stream on which the problem occurred
<Session_Id>	variable	Identifies the destination
<Alarm_Level>	variable	Identifies the alarm status
<Reason>	variable	Provides a brief explanation of why the alarm was raised or cleared

Selected field descriptions 4

The following table lists selected field descriptions

Field	Value	Description
<stream>	variable text	Identifies the billing stream on which the problem occurred
<destination>	variable	Identifies the destination
<specific error>	variable	Describes the SFTPW-specific error message and the possible action that should be taken

Action

This section lists recommended actions for each corresponding explanation. If the problem continues after you complete an action, contact the next level of support.

Action 1

The following table lists selected error text and recommended actions. If the table does not list the error text in your log, use the text in the log to troubleshoot the problem or contact the next level of support.

Reason	Action
Can't open ftp connection to downstream DPMS	The DPMS has no ports available for communication. Contact the next level of support.
Error: <error text>. Command: <command>	Make sure FTP is working.
ftp was unable to read from CLOSE state	Clear the FTPW alarm.
ftp was unable to read from OPEN state	Clear the FTPW alarm.
ftp was unable to read from RNTO state	Clear the FTPW alarm.
ftp was unable to read from STOR state	Clear the FTPW alarm.
FTP Error: <null line or text string>	Clear the FTPW alarm.
FTP session failed	Clear the FTPW alarm.
Login incorrect while attempting connection to downstream DPMS	Make sure FTP is working.

Reason	Action
Need account for login to downstream DPMS	Create a UNIX account for this login id on the downstream DPMS or contact the next level of support.
Need ftp account for storing files on downstream DPMS	The DPMS Agent supports the use of UNIX accounts, not FTP-specific accounts. Contact the next level of support.
Not logged in while executing <command>	Make sure FTP is working.
Requested action aborted. <command>. Page type unknown.	Check the version of FTP on the destination system or contact the next level of support.
Requested action not taken: <command>. File name not allowed.	The file name may exist on the downstream with write privileges disabled. Contact the next level of support.
Requested file action not taken: <command>. File unavailable.	The file or directory has been deleted, or read access to the file or directory is deactivated. Contact the next level of support.
Requested file action not taken: <command>. Directory does not exist or not writeable.	The file or directory has been deleted, or read access to the file or directory is deactivated. Contact the next level of support.
Unable to exec ftp process	Make sure FTP is working.

Action 2

The following table lists selected error text and recommended actions. If the table does not list the error text in your log, use the text in the log to troubleshoot the problem or contact the next level of support.

Error text	Action
File Manager Failed to close current active files	Clear the RTBFM alarm.
RTB: Auto-recovery operation is restarting for RTB stream <stream> and destination <destination> due to Network related error: Network Connectivity to destination is down. User intervention may be required.	Check for problems in the network or the network connection with the RTB destination. If necessary, contact your network administrator.
RTB: Auto-recovery operation is restarting for RTB stream <stream> and destination <destination> due to Network related error: Network is very slow or FTP server is not responding properly. User intervention may be required.	Check for problems in the network or the network connection with the FTP server. If necessary, contact your network administrator.
RTB: Auto-recovery of RTB destination can not continue for RTB stream <stream> and destination <destination> since Network Test File is not present.	Check for additional SDMB375 logs that identify the cause of the problem.
RTB: Auto-recovery option is exiting for destination due to non Network related error: Problem spawning or waiting for FTP transfer process. User intervention may be required.	Contact your next level of support.

Error text	Action
RTB: Auto-recovery option is exiting for destination due to non Network related error: Remote File Name not allowed or access permissions not sufficient. User intervention may be required.	Compare the configured information for the directory, as stored in the Schedule tuple of the stream, with the actual directory on the RTB destination. • Make sure the directory exists on the RTB destination. If necessary, enter a valid directory in the Schedule tuple. • Make sure the configured name of the directory matches the actual name of the directory on the RTB destination. If necessary, change the name in the Schedule tuple. • Make sure the permissions on the remote storage directory on the RTB destination allow read and write access. If necessary, contact your network administrator.
RTB: Auto-recovery option is exiting for destination due to non Network related error: Remote File or Remote Storage Directory unavailable or access permissions not sufficient. User intervention may be required.	Compare the configured information for the directory, as stored in the Schedule tuple of the stream, with the actual directory on the RTB destination. • Make sure the directory exists on the RTB destination. If necessary, enter a valid directory in the Schedule tuple. • Make sure the configured name of the directory matches the actual name of the directory on the RTB destination. If necessary, change the name in the Schedule tuple. • Make sure the permissions on the remote storage directory on the RTB destination allow read and write access. If necessary, contact your network administrator.
RTB: Auto-recovery option is exiting for destination due to non Network related error: Remote Login ID incorrect for login. User intervention may be required.	Compare the configured login id for the RTB destination, as stored in the Schedule tuple for the stream, with the valid login ids for the RTB destination. Make sure the configured login id is a valid login. If necessary, change the login id in the Schedule tuple or ask your network administrator to create the login id on the RTB destination.

Error text	Action
RTB: Auto-recovery option is exiting for destination due to non Network related error: Remote Login ID incorrect for storing files. User intervention may be required.	Check the permissions on the remote storage directory on the RTB destination. Make sure the remote login id, as configured in the Schedule tuple for the stream, has permission to write to the remote storage directory. If necessary, change the login id in the Schedule tuple or ask your network administrator to change the permissions on the remote storage directory.
RTB: Auto-recovery option is exiting for destination due to non Network related error: Remote Password incorrect. User intervention may be required.	Make sure the password for the remote login id has not changed. If necessary, change the value for the remote password in the Schedule tuple for the stream or contact your network administrator.
RTB: Auto-recovery option is exiting for destination due to non Network related error: Requested action aborted. Exceeded remote storage allocation (for current directory or dataset). User intervention may be required.	Check the RTB destination for available allocated space for the directory. Remove any unnecessary files or contact your network administrator.
RTB: Auto-recovery option is exiting for destination due to non Network related error: Requested action not taken. Insufficient storage space in the Remote system. User intervention may be required.	Check the RTB destination for available space. Remove any unnecessary files or contact your network administrator.
RTB: Auto-recovery option is exiting for destination due to non Network related error: Requested action not taken. Not logged in. User intervention may be required.	Check the Schedule tuple of the stream. Make sure the location and login information for the RTB destination is correct.
RTB: Auto-recovery option is exiting for destination due to non Network related error: Syntax error in FTP parameters or arguments. User intervention may be required.	Contact your next level of support.

Error text	Action
RTB: Auto-recovery option is exiting for destination due to non Network related error: Syntax error, FTP command unrecognized. User intervention may be required.	Contact your next level of support.
RTB: Auto-recovery option is exiting for destination due to non Network related error: Unable to get FTP return codes. User intervention may be required.	Contact your next level of support.
RTB: Auto-recovery option is exiting for destination due to non Network related error: Unknown. User intervention may be required.	Contact the next level of support.
RTB: Error during retry. RTB moved to SYSB state.	Check for additional SDMB375 logs that identify the cause of the retry error.
RTB: Rename operation of pre-existing.tmp file <file> failed for RTB stream <stream> and destination <destination>.	Check the access permissions for the remote partial file directory on the RTB destination. Make sure the RTB instance has write permission to the directory.
RTB: Stream is not running for RTB stream <stream> and destination <destination>. Transfer of Active billing file will not be possible until stream is activated.	Activate the billing stream.
RTB: Stream is not running for destination. Transfer of Active billing file will not be possible until stream is activated.	Activate the billing stream.
RTB: Unable to change in use file to rtb done due to invalid input. Please move any in use file associated with this stream, destination, and with files that have been transferred downstream.	Remove any in-use file associated with the stream, destination, or any files transferred downstream.
RTB: Unable to check for in use file <filename>.	Contact your next level of support.
RTB: Unable to check for rtb done file <filename without path> in directory <full path excluding filename>.	Contact your next level of support.

Error text	Action
RTB: Unable to check for write active file <filename without path> in directory <full path excluding filename>.	Contact your next level of support.
RTB: Unable to check for write error file <filename>.	Contact your next level of support.
RTB: Unable to clean up Audit file <filename>.	Contact your next level of support.
RTB: Unable to clean up in use files. Please remove file <filename> to ensure correct operation of RTB.	Remove the listed billing file from the RTB destination.
RTB: Unable to clean up in use files due to invalid input. Please remove any in use files associated with this <stream>, <destination>, and with files that have been transferred downstream.	Remove any in-use billing files that are associated with the billing stream, destination, or files transferred downstream.
RTB: Unable to clean up in use files due to invalid input. Please remove any in use files associated with this <stream> and <destination>.	Remove any in-use billing files that are associated with the billing stream or transferred downstream.
RTB: Unable to clean up rtb done files. Please remove file <filename without path> from directory <full path excluding filename> to ensure correct operation of RTB.	Remove the listed billing file.
RTB: Unable to clean up rtb done files due to invalid input. Please remove any rtb done files that are associated with this stream and destination.	Remove any rtb done files associated with this stream and destination.
RTB: Unable to clean up rtb done files due to invalid input. Please remove all but the most recent files that are associated with this stream and destination.	Remove all but the most recent billings files associated with the billing stream and destination.
RTB: Unable to clean up write active file <filename>.	Contact your next level of support.

Error text	Action
RTB: Unable to clean up write active files. Please remove file <filename without path> from directory <full path excluding filename> to ensure correct operation of RTB.	Remove the billing file listed in the log report.
RTB: Unable to clean up write active files due to invalid input. Please remove any write active files that are associated with this <stream> and <closed file>.	Remove any write active files associated with the billing stream.
RTB: Unable to clean up write error file <filename without path> from directory <full path excluding filename>.	Contact your next level of support.
RTB: Unable to clean up write error files. Please remove file <filename> to ensure correct operation of RTB.	Remove the billing file listed in the log report.
RTB: Unable to clean up write error files due to invalid input. Please remove any write error files associated with this <stream> and <closed file>.	Remove any write error files associated with the billing stream.
RTB: Unable to create in use file <filename without path> in directory <full path excluding filename>.	Contact your next level of support.
RTB: Unable to create write active file <filename without path> in directory <full path excluding filename>.	Contact your next level of support.
RTB: Unable to move a write active file to write error. Please move file <filename without path> in directory <full path excluding filename> to <filename without path> in directory <full path excluding filename> to ensure that RTB operates correctly.	Move the file listed in the log report.
RTB: Unable to move an in use file to rtb done. Please move file <filename.InUse> to <filename.RtbDone> to ensure that RTB operates correctly.	Contact the next level of support.
RTB: Unable to touch audit file <filename>.	Contact your next level of support.

Error text	Action
RTB: Warning: Network Test File is not present. Although the RTBautoRecovery option is enabled, Auto-recovery will not be possible in case of a file transfer outage for RTB stream <stream> and destination <destination>.	Re-install SBA or turn auto-recovery off.
RTB Control Process Death Detected. RTB is Halted.	Clear the RTBPD alarm.

Action 3

The following table lists selected error texts and recommended actions. If the table does not list the error text in your log or a recommended action for your log, use the text in the log to troubleshoot the problem or contact the next level of support.

Reason	Action
Connection Loss Detected	Check for related logs and alarms that identify the cause of the loss of connection.
Failed to Open File	AFT could not open a local file.
AFT Time-out On Far End Start-up Protocol	The remote processor did not respond to the AFT start-up protocol before the AFT protocol timer expired.
Connection Closed During Start-up Protocol	The connection closed while AFT was exchanging start-up protocol with the far-end processor.
AFT Data Error	AFT could not read or process data from the file.
Error Sending Start-up Protocol	AFT could not send the start-up protocol over the network connection.
AFT Registration With File System Failed	An AFT registration with the file system failed.
Retry Count Exceeded	The maximum number of file transfer retry attempts for the file was achieved. Contact the next level of support. Manual intervention is required to clear the problem.

Reason	Action
Session Stopped by Command.	No action required.
Session Started by Command	No action required.
Alarm Cancelled From Command	No action required.
Alarm Cancelled by AFT - Connection Restored	No action required.
Out of Sequence Error Detected	The downstream collector received data out of sequence. Contact the next level of support. Manual intervention is required to clear the problem.
Corrupted File	The file size was verified against the number of blocks transferred at the end of the file transfer and a mismatch has resulted.
Maximum Number of Partial Files Reached	The maximum number of partial files has been reached. The session will stop and no more files will be transferred. Contact the next level of support. Manual intervention is required to clear the problem.
Session In Stopped State	Connection was restored while the AFT session was in stopped state.

Action 4

Follow the recommended action shown in the <specific-error> field of the log. If an action is not recommended in the <specific-error> field, use the text in the log to troubleshoot the problem or contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

The system may escalate these logs and minor alarms to critical status when the DPMS transmitter exhausts all possible retries. The MIB parameter SessionFtpMaxConsecRetries specifies the condition.

SDMB380

Log report SDMB380 indicates that the file transfer mode for the stream indicated has an invalid value.

Format

The format for log report SDMB380 is as follows:

```
SDMB380 <date> <time> <seq#> TBL SDM BILLING CONFIG
<48_character_text_string>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<date>	mon:day	Date: month and day
<time>	hrs:mins:secs	Time: hours, minutes, and seconds
<seq#>	4 digits	Sequence number of log

Action

Access the CONFSTRM level of BILLMTC, then update the user by entering OUTBOUND or INBOUND. These are the only valid modes.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB390

Log report SDMB390 is generated when a problem occurs with the scheduled transfer of billing files due to fault in the system. An SBAIF alarm is also raised.

Format

The format for log report SDMB390 is as follows:

```
SDMB390 <date> <time> <seq #> TBL SDM BILLING FILE TRANSFER SCHEDULE
   STREAM= <stream> Unable to initialize file transfer schedule for
   stream <stream>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<date>	mmmdd	Date: month and day
<time>	hh:mm:ss	Time: hours, minutes, and seconds
<seq#>	4 digits	Sequence number of log
<stream>	variable	Identifies the stream where the problem occurred.

Action

Make sure the system is fault free. Perform the procedure to clear an SBAIF alarm in the Fault Management documentation for your release.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB400

Log report SDMB400 is generated for every active stream every hour. This log lists all of the current active alarms.

Format

The format for log report SDMB400 is as follows:

```
SDMB400 <mmmdd hh:mm:ss ssdd> SUMM SDM BILLING CONFIG
STREAM= <stream>: <48_character_text_string>
<level> <stream>: <shorttext>: <alarmtext>
<level> <stream>: <shorttext>: <alarmtext>

...
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	stream name	Identifies the affected billing stream
48_character_text_string	Variable	Identifies the billing problem
level	*, **, or ***	Identifies the alarm level
shorttext	Variable	Identifies the active billing alarm
alarmtext	Variable	Identifies the active billing alarm

Action

You must clear alarms immediately.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB530

Log report SDMB530 is generated when there has been a change in the configuration or status of a stream.

Format

The format for log report SDMB530 is as follows:

```
SDMB530 <mmmdd hh:mm:ss ssdd> INFO SDM BILLING CONFIG
   STREAM= <stream>: <48_character_text_string>
   NEW STATUS= <state> OLD STATUS=<state>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	stream name or “ALL"	Identifies the billing stream affected.
48_character_text_string	Variable	Identifies the billing status or configuration change.
config	Variable	Identifies the change in status or configuration data.

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.

SDMB531

Log report SDMB531 is generated when there is a successful configuration change for the backup volumes.

Format

The format for log report SDMB531 is as follows:

```
SDMB531 <mmdd hh:mm:ss ssdd> INFO SDM BILLING CONFIG
   STREAM=<stream>:
   NEW VOLUMES= <new_volume>
   OLD VOLUMES= <old_volume>
```

Example

```
SDMB531 May06 09:43:32 0500 INFO SDM BILLING CONFIG
   STREAM=SBA0:
   NEW VOLUMES= SD00AMA1 SD00AMA2 SD00AMA3 SD00AMA4 SD00AMA5
   SD00AMA6 SD00AMA7 SD00AMA8 SD00AMA9 SD00AMA10
   SD00AMA11 SD00AMA12 SD00AMA13 SD00AMA14 SD00AMA15
   SD00AMA16 SD00AMA17 SD00AMA18 SD00AMA19 SD00AMA20
   SD00AMA21 SD00AMA22 SD00AMA23 SD00SNS SD00AMA
   SD01AMA1 SD01AMA2 SD01AMA3 SD01AMA4 SD01AMA5 SD01AMA6
   SD01AMA7 SD01AMA8 SD01AMA9 SD01AMA10 SD01AMA11 SD00AMA12
   SD01AMA13 SD01AMA14 SD01AMA15

   OLD VOLUMES= SD00AMA1 SD00AMA2 SD00AMA3 SD00AMA4 SD00AMA5
   SD00AMA6 SD00AMA7 SD00AMA8 SD00AMA9 SD00AMA10
   SD00AMA11 SD00AMA12 SD00AMA13 SD00AMA14 SD00AMA15
   SD00AMA16 SD00AMA17 SD00AMA18 SD00AMA19 SD00AMA20
   SD00AMA21 SD00AMA22 SD00AMA23 SD00SNS SD00AMA
   SD01AMA1 SD01AMA2 SD01AMA3 SD01AMA4 SD01AMA5 SD01AMA6
   SD01AMA7 SD01AMA8 SD01AMA9 SD01AMA10 SD01AMA11 SD00AMA12
   SD01AMA13 SD01AMA14 SD01AMA15 SD01AMA16 SD01AMA17
   SD01AMA18 SD01AMA19 SD01AMA20
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	stream name or “ALL”	Identifies the affected billing stream

Field	Value	Description
New_Volumes	Variable	Identifies the latest set of disk volume(s) configured for the stream
Old_Volumes	Variable	Identifies the old set of disk volume(s) configured for the stream

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.

SDMB550

Log report SDMB550 is generated when the SBA shuts down. This occurs because either the SDM node was busied or the SBA was turned off.

Format

The format for log report SDMB550 is as follows:

```
SDMB550 <mmmdd hh:mm:ss ssdd> INFO SDM BILLING CONTROL
    STREAM= <stream>:<text>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Stream	Variable length text string, or ALL	Identifies the stream affected.
Text	48-character text string	Text describing status of stream

Action

Determine why the SBA is shutting down and ensure that the person who busied the SDM node or turned SBA off is aware of the implications of the shut down.

Associated OM registers

This log report has no associated OM registers.

Additional information

In this mode the SBA cannot receive billing data or send billing files to collectors. The SBA will be in backup mode, with the Core side of SBA recording records to the backup files.

SDMB600

Log report SDMB600 indicates generic information for the overall billing system.

Format

The format for log report SDMB600 is as follows:

```
SDMB600 <mmmdd hh:mm:ss ssdd> INFO SDM BILLING SYSTEM
STREAM= <stream>: <48_character_text_string>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	stream name or “ALL”	Identifies the billing stream affected.
48_character_text_string	Variable	Identifies the billing problem encountered.

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.

SDMB610

Log report SDMB610 is generated when a communications-related problem with billing has been resolved.

Format

The format for log report SDMB610 is as follows:

```
SDMB610 mmmdd hh:mm:ss ssdd INFO SDM BILLING COMMS
   STREAM= <stream>:<status>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Stream	4-character alphanumeric	Identifies the stream to which the log applies.
Status	48-character alphanumeric	Provides status information.

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.

SDMB615

The SuperNode Data Manager Billing (SDMB) subsystem generates log SDMB615 when a software-related error condition has been resolved.

Format

The log report format for SDMB615 is as follows:

```
SDMB615 mmmdd hh:mm:ss ssdd INFO SDM BILLING SOFT
ERROR STREAM=<stream>:<status>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	4-character alphanumeric	Identifies the stream to which the log applies.
status	48-character alphanumeric	Provides status information.

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.

SDMB620

Log report SDMB620 is generated when a backup-related problem with billing has been resolved.

Format

The format for log report SDMB620 is as follows:

```
SDMB620 < mmmdd hh:mm:ss ssdd> INFO SDM BILLING BACKUP
   STREAM= <stream>:<status>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Stream	4-character alphanumeric	Identifies the stream to which the log applies.
Status	48-character alphanumeric	Provides status information.

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.

SDMB621

Log report SDMB621 is generated when a new backup file is started.

Format

The format for log report SDMB621 is as follows:

```
SDMB621 < mmmdd hh:mm:ss ssdd> INFO SDM BILLING BACKUP
   STREAM= <stream>:<status>
   VOLUME= <volume> FILE= <file>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Stream	4-character alphanumeric	Identifies the stream to which the log applies.
Status	48-character alphanumeric	Provides status information.
Volume	8-character alphanumeric	Name of volume on which new file is located.
File	12-character alphanumeric	Name of new backup file.

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.

SDMB625

Log report SDMB625 is generated when recovery is started on a backup file.

Format

The format for log report SDMB625 is as follows:

```
SDMB625 < mmmdd hh:mm:ss ssdd> INFO SDM BILLING BACKUP
   STREAM= <stream>:<status>
   VOLUME= <volume> FILE= <file>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Stream	4-character alphanumeric	Identifies the stream to which the log applies.
Status	48-character alphanumeric	Provides status information.
Volume	8-character alphanumeric	Name of volume on which backup file is located.
File	12-character alphanumeric	Name of backup file on which recovery is being performed.

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.

SDMB650

Log report SDMB650 indicates that the SBA is restarting one or more of its processes.

Format

The format for log report SDMB650 is as follows:

```
SDM650 <date><time> <seq #> INFO SDM BILLING CONTROL
    STREAM= ALL: <text>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Text	48-character alphanumeric string	Status information.

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.

SDMB655

This section numbers each Explanation and associates it with a corresponding numbered Format.

Explanation 1

This log indicates file state changes and disk utilization levels.

Explanation 2

This log indicates that the disk utilization has dropped below a threshold.

Note: The three thresholds are critical, major and minor.

Explanation 3

This log indicates that the SBA can not move a file to the closeSent directory.

Format

Formats for log report SDMB655 follow:

Format 1

```
SDMB655 <date> <time> INFO SDM Billing Disk
STREAM=<stream>: File <filename> has moved from <state> to <new state>
```

Format 2

```
SDMB655 <date> <time> INFO SDM Billing Disk
STREAM=<stream>: BELOW <Threshold> DISK UTILIZATION
```

Format 3

```
SDMB655 <date> <time> INFO SDM Billing Disk
STREAM=<stream>: Failed to move file <filename> to closedSent. Manual
necessary
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<date>	mmmdd	Date: month and day
<time>	hh:mm:ss	Time: hours, minutes, and seconds
<seq#>	4 digits (ssdd)	Sequence number of log
<stream>	variable	Identifies the stream where the problem occurred.
<filename>	variable	Identifies the file that was removed.
<state>	variable	Identifies the state where the problem occurred.

Action

This section associates the Action with each numbered explanation.

Action 1

This is an information only log, no action is required.

Action 2

None

Action 3

None

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB660

The SuperNode Data Manager Billing (SDMB) subsystem generates log SDMB660 when a problem involving communications with other SuperNode Billing Application (SBA) features is resolved. This log is associated with the alarm FTP.

Format

The log report format for SDMB660 is as follows:

```
SDMB660 mmmdd hh:mm:ss ssdd INFO SDM BILLING COMMS
STREAM=<stream>:OFT - <specific resolution>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	variable	Identifies the stream where the problem occurred.
specific resolution	variable	Indicates the resolution of the communication problem.

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.

SDMB665

Log report SDMB665 indicates a software problem on the Core that prevents the synchronization (downloading) of FLEXCDR data at an SDM node.

Format

The format for log report SDMB665 is as follows:

```
SDMB665 <mmmdd hh:mm:ss ssdd>INFO SDM INFO BILLING
     STREAM=<stream>:<status>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Stream	4-character alphanumeric	Identifies the stream on which the problem occurred.
Status	48-character alphanumeric	Status information.

Action

For a status of “Unable to download CM’s FLEXCDR data,” restart the Core with a load that supports the SBA enhancements for CDR on SDM node. If the support for the SBA enhancements for CDR on SDM node was intentionally not installed, CDR event records are generated with their default values. If the Core software is supposed to support the SBA enhancements for CDR on SDM node, contact your next level of support and inform them that the software supplier should be contacted for delivery of the latest appropriate software.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB670

Log report SDMB670 is generated when the CDR-to-BAF conversion process uses default values to create a BAF field because a CDR field is missing. The SDMB subsystem also generates the SDMB670 log when the problem is corrected.

Format

The format for log report SDMB670 is as follows:

```
SDMB670 <date><time><seq#> INFO SDM BILLING CDR2BAF
CONVERSION STREAM=<stream>:<specific error>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Stream	4-character alphanumeric	Identifies the stream on which the problem occurred.
Specific error	Variable length alphanumeric	Provides a brief explanation of the problem.

Action

For the missing CDR field(s), determine which are needed to generate the BAF field. Use the BAF field displayed in the log report and refer to the applicable documentation for a list of the CDR fields associated with each BAF field. Update the CDR to include the missing field.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB675

Log report SDMB675 is an information log that identifies a event related to the transfer of billing files. An event may be a normal operation, a problem, or the resolution of a problem.

Log report SDMB675 supports the following services and applications:

- File transfer protocol (FTP)
- Real Time Billing (RTB)
- Automatic File Transfer (AFT)
- Secure file transfer protocol (SFTPW)

Explanations

This section provides numbered Explanations for each corresponding numbered Format and Action.

Explanation 1

Log report SDMB675 identifies the following events:

- the resolution of a problem related to file transfers
- an error that does not affect the processing of files

Log report SDMB675 may be associated with the following events:

- a problem identified in log report SDMB375 clears
- an FTP or FTPW alarm clears

The text in the log provides details on the error or resolved problem.

Explanation 2

Log report SDMB675 identifies a normal operation, a problem, or the resolution of a problem related to RTB. Log report SDMB675 is associated with the clearing of an RTB alarm.

The text in the log provides details on the condition.

Explanation 3

Log report SDMB675 identifies a normal operation, a problem, or the resolution of a problem related to AFT.

The text in log report SDMB675 identifies the event and the stream, destination, and file affected by the event.

Explanation 4

Log report SDMB675 identifies the following events:

- the resolution of a problem related to file transfers
- an error that does not affect the processing of files

Log report SDMB675 may be associated with the following events:

- a problem identified in log report SDMB375 clears
- an FTP or SFTPW alarm clears

The text in the log provides details on the error or resolved problem.

Formats

This section provides numbered Formats for each corresponding Explanation and Action.

Format 1

Format 1 for log report SDMB675 follows:

```
SDMB675 <date><time><seq #> INFO SDM BILLING FILE TRANSFER
STREAM= <stream>: <specific_resolution>
```

Format 2

Format 2 for log report SDMB675 follows:

```
SDMB675 <date><time><seq #> INFO SDM REAL TIME BILLING FILE TRANSFER
STREAM= <stream>: <specific_resolution>
```

Format 3

Format 3 for SDMB675 follows:

```
SDMB675 <date><time><seq #> INFO SDM BILLING FILE TRANSFER
STREAM= <stream>
Session Id: <Session_ID>
Event: <Event>
File Name: <File_Name>
```

Format 4

Format 4 for log report SDMB675 follows:

```
SDMB675 <date><time><seq #> INFO SDM BILLING FILE TRANSFER
STREAM= <stream>: <specific_resolution>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<date>	mmmdd	Date: month and day
<time>	hh:mm:ss	Time: hours, minutes, and seconds
<seq#>	4 digits (ssdd)	Sequence number of log
<stream>	variable	Identifies the stream where the problem occurred
<specific resolution>	variable	Describes why the log was generated
<Session_ID>	variable	Identifies the destination associated with the log
<Event>	variable	Describes why the log was generated
<File_Name>	variable	Identifies the associated DIRP file

Action

This section provides numbered actions for each Explanation and Format.

Action 1

No action is required.

Action 2

Refer to the text of the log. If the text describes a normal operation, no action is required. If the text describes any other condition, contact the next level of support.

Action 3

Refer to the text of the log. If the text describes a normal operation, no action is required. If the text describes any other condition, contact the next level of support.

Action 4

No action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB680

Log report SDMB680 is generated whenever information not related to the file system or creating links needs to be communicated to the customer. Two such instances are when the fileTransferMode experiences a transition or when a connection to the PSS file server has been reestablished.

Format

The format for log report SDMB680 is as follows:

```
SDMB680 <date> <time> <seq#> INFO SDM BILLING CONFIG
<specific resolution>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<date>	mon:day	Date: month and day
<time>	hrs:mins:secs	Time: hours, minutes, and seconds
<seq#>	4 digits	Sequence number of 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.

SDMB690

Log report SDMB690 indicates an SBAIF alarm has cleared. The fault that generated the SBAIF alarm has also cleared.

Format

The format for log report SDMB690 is as follows:

```
SDMB690 <date> <time> <seq_no> INFO INFO SDM BILLING FILE TRANSFER SCHEDULE
   STREAM: <stream> SBAIF alarm is cleared for stream <stream>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<date>	mmmdd	Date:month and day
<time>	hh:mm:ss	Time: hours, minutes, and seconds
<seq_no>	4 digits	Sequence number of log
<stream>	variable	Name of billing stream affected by SBAIF alarm

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.

SDMB691

Log report SDMB691 identifies the following events related to the scheduled transfer of billing files.

- A fault in the system has led to a problem with the scheduled transfer of billing files.
- A fault in the system has cleared, and the scheduled transfer of billing files is now operating normally.
- A file transfer schedule is manually deactivated or deleted.

Format

Format 1

An example of format 1 follows:

```
SDMB691 <date> <time> <seq_no> INFO SDM BILLING FILE TRANSFER SCHEDULE
   STREAM: <stream> <destination>: Unable to initialize file transfer schedu
   for stream <stream>.
```

Format 2

An example of format 2 follows:

```
SDMB691 <date> <time> <seq_no> INFO SDM BILLING FILE TRANSFER SCHEDULE
   STREAM: <stream> <destination>: File transfer schedule is now working for
   stream <stream>.
```

Format 3

An example of format 3 follows:

```
SDMB691 <date> <time> <seq_no> INFO SDM BILLING FILE TRANSFER SCHEDULE
   STREAM: <stream> <destination>: File transfer schedule deactivated.
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<date>	mmmdd	Date:month and day
<time>	hh:mm:ss	Time: hours, minutes, and seconds
<seq_no>	4 digits	Sequence number of log
<stream>	variable	Name of billing stream affected by SBAIF alarm
<destination>	variable	Destination to which the SBA transfers billing files.

Action

Format 1

Make sure the system is free of faults. When the system is free of faults, the SuperNode Billing Application (SBA) will resume the scheduled transfer of billing files. Refer to the procedure to troubleshoot problems with scheduled billing file transfers in the Fault Management documentation for your release.

Note: If you do not receive an SBAIF alarm or SDMB390 log with this log, you may be able to use the **sendfile** command to manually send billing files to the downstream destination. Use the procedure to send billing files from disk in the Accounting documentation for your release.

Format 2

Format 2 requires no action.

Format 3

Format 3 requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMB820

Log report SDMB820 is generated when a backup hits a threshold.

Format

The format for log report SDMB820 is as follows:

```
SDMB820 <mmmdd hh:mm:ss ssdd> INFO SDM BILLING BACKUP
   STREAM= <stream>: <48_character_text_string>
   VOLUMES= <volume>
```

Example

```
SDMB820 May06 11:20:51 2876 INFO SDM BILLING BACKUP
   STREAM= SBA0: WARNING, 50% or less of Backup space is free
   VOLUMES= SD00AMA13 SD00AMA15 SD01AMA11 SD01AMA12 SD01AMA13
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
stream	stream name or “ALL"	Identifies the affected billing stream
48_character_text_string	Variable	Identifies the billing problem
volumes	Variable	Identifies disk volume(s) configured for the stream

Action

You must resolve the reason for backup or provide more space on backup volumes.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SDMO375

Log report SDMO375 indicates that OMDD discovered a problem while performing an outbound file transfer and could not ensure that the OM report was transferred downstream.

Format

The format for log report SDMO375 is as follows:

```
SDMO375 MAJOR TBL <mm dd hh:mmm:ss> <sdm/cbm name> syslog:
SDM OM FILE TRANSFER ODM FTP:<reason for ftp failure>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
<mm dd hh: mmm:ss>	date and time	Indicates the date and time when the log was generated.
<sdmname>	sdm/cbm name	The hostname of the SDM/CBM where the log was generated.
<reason for ftp failure>	text string	The reason for the ftp failure.

Action

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.

SPM625

The SPM625 log report is generated when crossover message channels are not configured for SPMs.

Format

The log report format for SPM625 is as follows:

```
MSH3XAPT     SPM625 mmmdd hh:mm:ss ssdd INFO SPM XOVER
   NonConformity Report
   This office has 2 SPMs that do not have crossover
   message channels configured.

   Crossover message channel configuration is
   recommended for all DS-512 connected SPMs.
   Please refer to Crossover Messaging IM 65-7644 or
   contact the next level of support.

   The following nodes are not in message channel
   crossover mode:
   SPM 8    SPM 9
```

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.

SPM710

The SPM710 log report is generated when the audit updates the ISDNPROT table.

Format

The log report format for SPM710 is as follows:

```
SPM710 mmmdd hh:mm:ss ssdd NONE INFO ISDNPROT Table
update for SPM <spmno>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
spmno	1 through 64	Identifies the node number of the SPM.

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.

CMT300

Log report CMT300 indicates a data mismatch between the server where the Succession Element and Sub-network Manager (SESM) software is installed and the Communication Server 2000.

Format

The format for log report CMT300 when a data mismatch has occurred is as follows:

```
CMT300 JUL17 22:20:05 0805 TBL CMT Fault
        Location: audit
        Notification ID: 1000
        State: Raise
        Category: Processing Error
        Cause: Corrupt data
        Time: Jul 17 22:20:05 2003
        Component ID: SESM-AuditSystem;Audit=CS2K DAta Inegrity Audit
        Specific Problem: Data mismatches detected
        Description: The SESM audit; CS2K Data Integrity Audit, has 10
        unresolved problems. To view and correct the problems, open the
        audit problem report from the Audit System found under the SESM
        Maintenance menu item.
```

Selected field descriptions

This log report has no selected fields.

Action

View the report generated from the CS2K Data Integrity Audit. Refer to procedure "Performing an audit" in the ATM/IP Solution-level Fault Management document, NN10408-900, if required.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

CMT301

Log report CMT301 indicates that the CS 2000 GWC Manager cannot download data to a Gateway Controller (GWC) on recovery, or that a problem related to a gateway profile certificate file has occurred. Log report CMT 301 is associated with a minor alarm.

Note: For information on how to create, add, and remove a certificate file, refer to the OSSGate User Guide, NE10004-512.

Format

The format for log report CMT301 is shown in the following example:

```
CMT301 JUL17 22:20:05 0805 TBL CMT Fault
        Location: gwcem
        Notification ID: 681
        State: Raise
        Category: Processing Error
        Cause: Corrupt data
        Time: Jul 17 22:20:05 2003
        Component ID: SESM-=GWCEMalarm; GWCEM=Recovery: GWC=GWC-1 UNIT-1
        Specific Problem: GWC Recovery failed. Check PTM MI2 logs
        Description: Problem detected in GWC Recovery Subsystem
```

Selected field descriptions

This log report has no selected fields.

Action

Check the MI2 logs on the server where the CS 2000 Management Tools reside. Refer to procedure "Viewing debug logs" in the ATM/IP Solution-level Fault Management document, NN10408-900, if required.

If the alarm is caused by a gateway profile certificate problem, use the following guidelines to clear the alarm:

Note: Refer to the OSSGate User Guide, NE10004-512, for detailed information on how to create, add, and remove a gateway profile certificate file.

- If a certificate file has corrupt syntax or is invalid, create a new (correct) certificate and delete the invalid one.
- If a certificate has a duplicate name, remove the duplicate certificate file.

  Note: Certificate names are case insensitive and must be unique.

- If a third-party certificate file still associated with some gateways has been removed, replace the certificate file. You can also clear the alarm by removing all the gateways associated with the deleted certificate.
- If some certificate fields have been changed and the changes are invalid, correct the appropriate fields with the valid values.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

CMT302

Log report CMT302 indicates that the SNMP NE Poller on the CS 2000 Management Tools server cannot communicate with a network device such as GWC and UAS.

Format

The format for log report CMT302 when the SNMP NE Poller cannot communicate with a network device is as follows:

```
CMT302 MAJOR TBL CMT Fault
        Location: SNMP_NE_Poller
        Notification ID: 18
        State: Raise
        Category: Communications
        Cause: Communications subsystem failure
        Time: Mar 30 14:30:12 2005
        Component ID: SESM=SNMP Device Poller;Device=GWC-10-UNIT-0;
Device ID=0x00000063000000alac11f14a
        Specific Problem: SNMP Timeout
        Description: CMT Unable to communicate with managed device
```

Selected field descriptions

This log report has no selected fields.

Action

Determine cause of the SNMP timeout to the device.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

CMT303

Log report CMT303 indicates that SESM has failed to get available Call Agent IP address from Core. This is probably caused by a communication problem between SESM and Core or the Call Agent IP address was not properly filled in Core.

Format

The format for log report CMT303 is as follows:

```
CMT303 MMMDD hh:mm:ss <sequence number> TBL CMT Fault
        Location: CS2K Config Manager
        Notification ID: <Notification ID>
        State: Raise
        Category: Environment
        Cause: Configuration or customization error
        Time: Mmm DD hh:mm:ss YYYY
        Component ID: SESM=Cs2kCfgMgr;Cs2kCfgMgr=NoAvailableCallServerIP
        Specific Problem: Communication problem between SESM and Core.
Or Call Agent IP address was not properly filled in Core table <CMIPADDR>
        Description: Cannot get available Call Agent IP address from Core.
```

The format when the log is cleared:

```
<OFFICE> CMT399 MMMDD hh:mm:ss <sequence number> INFO CMT Fault
        Location: CS2K Config Manager
        Notification ID: <Notification ID>
        State: Clear
        Time: Mmm DD hh:mm:ss YYYY
        Component ID: SESM=Cs2kCfgMgr;Cs2kCfgMgr=NoAvailableCallServerIP
        Description: Cannot get available Call Agent IP address from Core.
```

Selected field descriptions

This log report has no selected fields.

Action

Ensure that there is connectivity between SESM and Core (use ping, for example).

Refer to the SDM/CBM document to check if Call Agent IP is properly filled in Core.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory, /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

CMT304/CMT399

Log report CMT304 indicates that the request from the Gateway Controller (GWC) Manager to the Certificate Manager to retrieve IKE certificates has failed. This is due to a communications failure or that the Certificate Manager and GWC Manager is not ready for certificate retrieval.

Format

The format for log report CMT304 when the request from the GWC Manager to the Certificate Manager fails to retrieve IKE certificates is as follows:

```
<OFFICE> ***  CMT304 MMMDD hh:mm:ss <sequence number> TBL  CMT Fault
        Location: gwcem
        NotificationID: <Notification ID>
        State: Raise
        Category: ProcessingError
        Cause: Corrupt data
        Time: Mmm DD hh:mm:ss YYYY
        Component Id: SESM=GWCEMalarm;GWCEM=GWCGetCertAarm;GWC=<GWC
node/unit>
        Specific Problem: GWCEM can not get the certificates from IEMS.
        Description: Failed to get certificates from IEMS.
```

Log report CMT399 indicates that the fault condition has cleared. The format for log report CMT399 is as follows:

```
<OFFICE>      CMT399 MMMDD hh:mm:ss <sequence number> INFO CMT Fault
        Location: gwcem
        NotificationID: <Notification ID>
        State: Clear
        Time: Mmm DD hh:mm:ss YYYY
        Component Id: SESM=GWCEMalarm;GWCEM=GWCGetCertAarm;GWC=<GWC
node/unit>
        Description: Clearing Get Certificate Alarm Type FAIL GET CERT
```

Selected field descriptions

This log report has the following selected fields.

Log report CMT304/CMT399 field descriptions

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.
Notification ID	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.
GWC node/unit	character string	Identifies the GWC node and unit affected by the event. Example: GWC-1-UNIT-0.

Action

Perform the following actions for a CMT304 log report. No action is required for a CMT399 log report.

- Ensure that there is connectivity between the Certificate Manager and GWC Manager (using **ping**, for example)
- Execute either the procedure Installing an initial WebPKProxy certificate or Installing a WEBPKPROXY certificate to clear PKM306 alarm
- Execute WEBPKPROXY registration
- Re-attempt to retrieve IKE certificates for the affected GWC that is highlighted in the ComponentID using procedure Download IKE certificates on the GWC Manager

If the problem persists, attempt the following:

CAUTION
CS2000 Management Tools access will temporarily go down when proceeding with this action.
Ensure your next level of support are readily available.

- At a command prompt, enter

  ```
  servstop SESMService
  servstart SESMService
  ```

- Re-attempt to download certificates for the affected GWC that is highlighted in the ComponentID using procedure Download IKE certificates on the GWC Manager. If the problem still persists, then contact your next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

CMT398

Log report CMT398 is a default alarm log if the SESM receives a TRAP that does not contain the OID nortelINMInotifyAlarmNeTechnologySpecificInfo (.1.3.6.1.4.1.562.29.1.6.4.1.11) or if the ReportName and ReportNumber are not specified in the value of nortelINMInotifyAlarmNeTechnologySpecificInfo.

Format

The format for log report CMT398 varies according to the reason it was raised.

Action

Restore communication with the CS 2000 GWC Manager. Determine if the CS2000 GWC Manager is down and/or disconnected. Determine if the GWC has been setup to use the wrong IP address for the CS2000 GWC Manager at the CS2000 SAM21 Manager.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

CMT399

Log report CMT399 indicates that log report CMT304 from the CS 2000 Management Tools server has cleared.

Format

The format for log report CMT399 is as follows:

```
<OFFICE>      CMT399 MMMDD hh:mm:ss <sequence number> INFO CMT Fault
        Location: gwcem
        NotificationID: <Notification ID>
        State: Clear
        Time: Mmm DD hh:mm:ss YYYY
        Component Id: SESM=GWCEMalarm;GWCEM=GWCGetCertAarm;GWC=<GWC
node/unit>
        Description: Clearing Get Certificate Alarm Type FAIL GET CERT
```

Selected field descriptions

This log report has the following selected fields.

Log report CMT399 field descriptions

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.
Notification ID	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.
GWC node/unit	character string	Identifies the GWC node and unit affected by the event. Example: GWC-1-UNIT-0.

Action

This log report requires no action.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

CMT500

Log report CMT500 indicates that the Succession Element and Sub-network Manager (SESM) alarm system is initializing.

Format

The format for log report CMT500 is as follows:

```
<host> CMT500  JUN30  11:01:55  0580  INFO CMT INFO
   CS2K Management Tools Alarm Manager Initialization.
```

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

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

CMT501

Log report CMT501 indicates that the Succession Element Sub-network Manager (SESM) server application has been shut down.

Format

The format for log report CMT501 is as follows:

```
<host> CMT501  JUN30  11:01:55  0580  INFO CMT INFO
   CS2K Management Tools Alarm Manager Shutting Down.
```

Selected field descriptions

This log report has no selected fields.

Action

Verify whether the SESM server application was intentionally shut down and that it is being restarted.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

CMT502

Log report CMT502 indicates that the CS 2000 Management Tools alarm system cannot generate alarm event notifications.

Format

The format for log report CMT502 is as follows:

```
<host>  CMT502  JUN30 11:01:55  0580  INFO CMT INFO
   CS2K Management Tools Alarm Manager failed to raise alarm
   notification due to CORBA failure. Please check CORBA
   status on CS2K Management Tools server.
```

Selected field descriptions

This log report has no selected fields.

Action

Determine the status of the CORBA communications on the CS 2000 Management Tools server and the network connectivity of the server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log is intended for users of the SESM CORBA alarm notifications to inform them that events cannot be generated.

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

DB600

Log report DB600 indicates a database connection error.

Format

The format for log report DB600 when a database connection error occurs is as follows:

```
DB600 JUL17 22:20:05 0805 INFO DB Connection Error
        Location: SPFS=wnc0s0jd
        Information: I/O error, the database did not respond
        Time: Jul 17 22:20:05 2003
        Component ID: Database, GWCEM User
        Specific Problem: I/O error was detected when attempting to get a
                          database connection.
        Description: Transient error detected. The database may be stopped
                     for administrative actions. Investigate when this log
                       occurs repeatedly.
```

Selected field descriptions

This log report has no selected fields.

Action

If the log is generated multiple times for the same component ID within 15 to 30 minutes, investigate to determine if specific authorized administrative actions are the cause. If administrative actions are not the cause, verify the database is functioning normally.

Associated OM registers

This log report has no associated OM registers.

Additional information

A few occurrences of this log can be attributed to the database being stopped for administrative purposes. However, continuous occurrence of this log within a period of 15 to 30 minutes can be attributed to the database not functioning normally and needs to be investigated.

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

DB601

Log report DB601 indicates the database connection is closed.

Format

The format for log report DB601 when the database connection is closed is as follows:

```
DB601 JUL17 22:20:05 0805 INFO DB Connection Error
        Location: SPFS=wnc0s0jd
        Information: Database connection closed, stale connnections will
                     refresh.
        Time: Jul 17 22:20:05 2003
        Component ID: Database, GWCEM User
        Specific Problem: A closed or stale database connection was
                          detected, all stale connections will be refreshed.
       Description: Transient error detected. Investigate when a threshold
                     is exceeded in a short time.
```

Selected field descriptions

This log report has no selected fields.

Action

If the log is generated multiple times for the same component ID within 15 to 30 minutes, investigate to determine if specific authorized administrative actions are the cause. If administrative actions are not the cause, verify the database is functioning normally.

Associated OM registers

This log report has no associated OM registers.

Additional information

A few occurrences of this log can be attributed to the database being stopped for administrative purposes. However, continuous occurrence of this log within a period of 15 to 30 minutes can be attributed to the database not functioning normally, and needs to be investigated.

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

DB602

Log report DB602 indicates an invalid password.

Format

The format for log report DB602 when an invalid password is encountered is as follows:

```
DB602 JUL17 22:20:05 0805 INFO DB Connection Error
        Location: SPFS=wnc0s0jd
        Information: User password has changed
        Time: Jul 17 22:20:05 2003
        Component ID: Database, GWCEM User
        Specific Problem: Invalid password was detected on a database
                          connection, the new password is now in use for
                          this database user.
       Description: Transient error detected. When a threshold is exceeded
                    in a short time, investigate to ensure security
                     violations or unauthorized access are not the cause.
```

Selected field descriptions

This log report has no selected fields.

Action

If the log is generated multiple times within 15 to 30 minutes, investigate to determine if authorized administrative actions to change the database password are the cause. If administrative actions are not the cause, verify for security violations or unauthorized system access.

Associated OM registers

This log report has no associated OM registers.

Additional information

A single occurrence of this log can be attributed to the database password being changed for a database user. However, multiple occurrences of this log within a period of 15 to 30 minutes can be attributed to security violations or unauthorized system access.

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

DB603

Log report DB603 indicates that the threshold for the maximum database sessions has been exceeded.

Format

The format for log report DB603 when the threshold for the maximum database sessions has been exceeded is as follows:

```
DB603 JUL17 22:20:05 0805 INFO DB Connection Error
        Location: SPFS=wnc0s0jd
        Information: Maximum database sessions limit reached
        Time: Jul 17 22:20:05 2003
        Component ID: Database, GWCEM User
        Specific Problem: Maximum database sessions active was detected on
                          an attempt to create a database connection.
       Description: Transient error detected. When a threshold is exceeded
                    in a short time, reconfiguration of the database's
                     limits may be required.
```

Selected field descriptions

This log report has no selected fields.

Action

If the log is generated multiple times within 15 to 30 minutes, contact your database or system administrator.

Associated OM registers

This log report has no associated OM registers.

Additional information

Database resources may need reconfiguration or the value of the Sessions initialization parameter may need to be increased.

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

DB604

Log report DB604 indicates that the threshold for the maximum database processes has been exceeded.

Format

The format for log report DB604 when the threshold for the maximum database processes has been exceeded is as follows:

```
DB604 JUL17 22:20:05 0805 INFO DB Connection Error
        Location: SPFS=wnc0s0jd
        Information: Maximum database processes limit reached
        Time: Jul 17 22:20:05 2003
        Component ID: Database, GWCEM User
        Specific Problem: Maximum database processes was detected on
                          an attempt to create a database connection.
       Description: Transient error detected. When a threshold is exceeded
                    in a short time, reconfiguration of the database's
                     processes limit may be required.
```

Selected field descriptions

This log report has no selected fields.

Action

If the log is generated multiple times within 15 to 30 minutes, contact your database or system administrator.

Associated OM registers

This log report has no associated OM registers.

Additional information

Database resources may need reconfiguration or the value of the Processes initialization parameter may need to be increased.

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

NPM360

Log report NPM360 indicates an alarm has been raised.

Format

The format for log report NPM360 is as follows:

```
*** NPM360 JAN25 17:37:2 0100 INFO Alarm Raise

Alarm <alarm name> has been raised.

Alarm Description: <alarm description>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Alarm	character string	Indicates the name of the alarm (see table NPM system alarms below).
Alarm Description	text string	Provides a brief description of the alarm (see table NPM system alarms below).

The following table lists the NPM system alarms and provides a brief description of each.

NPM system alarms

Alarm name	Description	Severity
ACT_NOT_APP	An activatable patch is not applied to all applicable devices.	No alarm
ACT_NOT_ACT	An activatable patch is applied to all applicable devices, but is not activated in all devices.	No alarm
DEBUG_APP	Some debug patches are applied.	Minor

NPM system alarms

Alarm name	Description	Severity
DNR_NOT_APP	Some Do Not Remove (DNR)-type patches are not applied.	Critical
EMG_NOT_APP	Some Emergency (EMG)-type patches are not applied.	Critical
GEN_NOT_APP	Some General (GEN)-type patches have not been applied.	No alarm
LTD_NOT_APP	Some Limited (LTD)-type patches not are applied.	No alarm
OBS_NOT_REMOVED	Some Obsolete (OBS)-type patches have not been removed.	Major
OBE_NOT_REMOVED	Some Obsolete Emergency (OBE)-type patches have not been removed.	Critical
REMOVED_PATCHES	Some patches, which are not category OBS, OBE, or DBG, have been removed.	No alarm
PATCH_ONHOLD	Some patches are on hold.	Minor
DEVICE_ONHOLD	Some devices are on hold.	Minor
DEVICE_AUDITFAIL	Some devices have either not executed or failed audits since registration.	Major
DISABLED_APPLIED	An OAM processor patch has been applied, but not enabled.	Major
ENABLED_REMOVED	An OAM processor patch has been removed, but not disabled.	Major

Action

The Alarm Description provides the reason for the failure and is self-explanatory in terms of what action to take, if any, to resolve.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

NPM370

Log report NPM370 indicates when an alarm has been cleared.

Format

The format for log report NPM370 is as follows:

```
NPM370 JAN25 18:34:44 0300 INFO Alarm Cleared

Alarm <alarm name> has been cleared.

Alarm Description: <alarm description>
```

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

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

NPM400

Log report NPM400 indicates the results of an attempted apply, remove, and audit command.

Format

The format for log report NPM400 is as follows:

```
NPM400 APR29 16:57:24 0400 SUMM Action Summary
Patch ID, Device ID, Command, Pass/Fail, Time Complete
-------------------------------------------------
NONE, gwc9-Unit-0-47.142.108.62, AUDIT, Pass, 4:57:24 PM
NONE, gwc9-Unit-1-47.142.108.63, AUDIT, Fail, 4:57:24 PM
```

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

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

NPM600

Log report NPM600 indicates when the NPM server has been started, either through a reboot or manual restart.

Format

The format for log report NPM600 is as follows:

```
NPM600 Jan 4, 2001 10:34:28 AM INFO General Information
The NPM Server has been started.
```

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

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

NPM601

Log report NPM601 relates to patch files.

Format

The format for log report NPM601 is as follows:

```
NPM601 OCT23 13:51:16 78900 TBL File Failure
There was an i/o exception using patchfile
File: ftp://47.142.84.207/data/npm/Au/heu00u62.ptchmg9p
```

Selected field descriptions

This log report has no selected fields.

Action

The following table lists probable causes and suggested actions.

Probable cause	Required action
The contents of the patchfile were incorrect.	Contact the source of the patch for further investigation.
The specified patchfile was not readable.	Verify that the patchfile is in the specified location. Make sure the directories leading to the file are readable and executable by the NPM server. Also verify that the patch file is readable by the NPM server.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

NPM603

Log report NPM603 indicates problems between the database and the device during a device audit.

Format

The format for log report NPM603 is as follows:

```
NPM603 Jan 4, 2001 10:34:28 AM TBL Device Audit Failure
The audit of the following device was not successful
device: <device ID>
```

Selected field descriptions

This log report has no selected fields.

Action

Verify the device and OAM system are running normally

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

NPM605

Log report NPM605 indicates a patch application or removal failed.

Format

The format for log report NPM605 is as follows:

```
NPM605 OCT23 3:13:39 5700 TBL General Trouble
Apply failed
Patch: <PATCH>
Device: <DEVICE>
DeviceMessage: <error message from device>
```

Selected field descriptions

This log report has no selected fields.

Action

Contact the source of the patch for further investigation.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

NPM610

Log report NPM610 provides information related to the execution of a task.

Format

The format for log report NPM610 is as follows:

```
NPM610 NOV11 11:43:16 4900 INFO Task Information
Command: APPLY Task Name: MYTASK1 TaskId: 26
Requestor's Name: npm Execution: Non-Interactive
Execution of the Apply Task has been terminated because no
operations have passed the pre-apply step.
```

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

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

NPM620

Log report NPM620 provides information about restarts initiated and completed through the NPM GUI or CLUI.

Format

The format for log report NPM620 is as follows:

```
NPM620 SEP6 21:3:34 5100 INFO NPM Initiated Restart
A restart has been initiated by the NPM on device: PSE_snc0s0j
```

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

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

NPM660

Log report NPM660 indicates problems when a plan fails to execute.

Format

The format for log report NPM660 is as follows:

```
NPM660 OCT23 0:43:43 97100 TBL Automated Process Failure
Plan SYSTEMPLAN executed but had failures.
```

Selected field descriptions

This log report has no selected fields.

Action

Look for related logs on the target devices.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

NPM680

Log report NPM680 is generated when a plan is automatically executed.

Format

The format for log report NPM680 is as follows:

```
NPM680 OCT23 15:22:39 44700 INFO Automated Process Information
Plan AUDPSEPLAN was executed 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

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

GWC300

Log report GWC300 indicates an “Active unit disabled.” Unit Out of Service: Service is not available or Invalid GWC Profile Data. The alarm severity is Critical.

Format

The format for log report GWC300 is as follows:

```
COMPACT2 *** GWC300 JUN30 11:01:55 0580 TBL GWC Fault
      Location: GWC-0-UNIT-0
      NotificationID: 1
      State: Raise
      Category: Quality of Service
      Cause: Underlying resource unavailable
      Time: Jun 30 11:09:16 2003
      Component Id: GWC-0-UNIT-0
      Specific Problem: Unit Out of Service: Service is not available
      Description: Active unit disabled.
```

Selected field descriptions

This log report has no selected fields.

Action

See the following table:

Specific problem Probable cause	Action
Specific problem: Indicates that a unit is out of service: Service is not available. Probable cause: the lack of availability of the underlying resource.	This log reports that the unit is not in service (Operational state of "disabled"). If the Administrative state is “unlocked” and the Usage state is “busy” this indicates the unit is trying to recover itself to an in service state. Note that when both units are out of service, the active unit must recover before the standby unit will. Check the following: 1- Whether the unit is manually locked out of service (Administrative state of “locked”). 2- Alarms that may indicate a problem on the unit preventing it from returning to service. 3- Other state indicators which may indicate problems, such as - Isolation state of “isolated” - If it is the standby unit, Availability state of “degraded” - Availability state of “offLine” 4- Logs which may also indicate a failure of a step in the process of recovering the unit.
Specific problem: Indicates that a unit has invalid GWC Profile Data: Service is not available. Probable cause: A configuration or customization error	Check the profile data for the unit and do one of the following: - Change to another profile. - Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility. Then, RTS the unit.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC301

Log report GWC301 indicates a "Standby unit disabled." Unit Out of Service: Service is not available or Invalid GWC Profile Data. The alarm severity is Minor or Major.

Format

The format for log report GWC301 is as follows:

```
COMPACT2 * GWC301 JUN30 11:02:44 0588 TBL GWC Fault
       Location: GWC-0-UNIT-1
       NotificationID: 1
       State: Raise
       Category: Quality of Service
       Cause: Underlying resource unavailable
       Time: Jun 30 10:54:34 2003
       Component Id: GWC-0-UNIT-1
       Specific Problem: Unit Out of Service: Service is not available
       Description: Standby unit disabled.
```

Selected field descriptions

This log report has no selected fields.

Action

See the following table:

Specific problem Probable cause	Action
Specific problem: Indicates that a unit is out of service: Service is not available. Probable cause: the lack of availability of the underlying resource.	This log reports that the unit is not in service (Operational state of "disabled"). If the Administrative state is “unlocked” and the Usage state is “busy” this indicates the unit is trying to recover itself to an in service state. Note that when both units are out of service, the active unit must recover before the standby unit will. If the Operational state “disabled” and Administrative state is “unlocked”, the unit is system busy (SysB) - the alarm is major. If the Operational state “disabled” and Administrative state is “locked”, the unit is manually busy (ManB) - the alarm is minor. Check the following: 1- Alarms that may indicate a problem on the unit preventing it from returning to service. 2- Other state indicators which may indicate problems, such as - Isolation state of “isolated” - Availability state of “offLine” 3- Logs which may also indicate a failure of a step in the process of recovering the unit.
Specific problem: Indicates that a unit has invalid GWC Profile Data: Service is not available. Probable cause: A configuration or customization error	Check the profile data for the unit and do one of the following: - Change to another profile. - Reconfigure the GWC unit software or CS 2000 GWC Manager software to remove the incompatibility. Then, RTS the unit.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC302

Log report GWC302 indicates a Major for active unit; Minor for inactive unit. "Core communication lost." No response received to Core heartbeat messages.

Format

The format for log report GWC302 is as follows:

```
COMPACT06BT * GWC302 JUL1 15:02:21 0055 TBL GWC Fault
        Location: GWC-2-UNIT-0
        NotificationID: 3
        State: Raise
        Category: Communications
        Cause: LAN error
        Time: Jul 01 15:02:27 2003
        Component Id: GWC=GWC-2-UNIT-0;Version=PGC91AQ;Unit=unit_0;
            Software=NODE MTC
        Specific Problem: No response received to Core heartbeat messages.
        Description: Core communication lost.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log clears automatically after a Core or network outage clears. Otherwise, verify that the node number and Core Side IP address is correct for the GWC to communicate with the Core.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC303

Log report GWC303 indicates a "Mate unit communication lost." No response received to mate heartbeat messages. The alarm severity is Minor.

Format

The format for log report GWC303 is as follows:

```
COMPACT2 * GWC303 JUN30 11:02:47 0589 TBL GWC Fault
      Location: GWC-0-UNIT-0
      NotificationID: 4
      State: Raise
      Category: Communications
      Cause: LAN error
      Time: Jun 30 11:10:08 2003
      Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
          Software=NODE MTC
      Specific Problem: No response received to mate heartbeat messages.
      Description: Mate unit communication lost.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by restoring communication from the CS 2000 GWC Manager to the GWC unit. Do this by unlocking the GWC at the CS 2000 SAM21 Manager. Also, verify that the Ethernet cable is connected, and that the GWC is setup to use the correct node number.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC304

Log report GWC304 indicates that communication with a gateway is down. The alarm severity is Major.

Note: 'Gateway' is defined as large gateway or audio gateway (for example, PVG, H.323 gateway with 64 or more endpoints, MG 9000, UAS).

Format

The format for log report GWC304 is as follows:

```
COMPACT2 ** GWC304 JUL2 01:25:58 0619 TBL GWC Fault
       Location: GWC-1-UNIT-1
       NotificationID: 78
       State: Raise
       Category: Communications
       Cause: Underlying resource unavailable
       Time: Jul 02 01:21:20 2003
       Component Id: GWC=GWC-1-UNIT-1;Version=PGT09BL;
             Unit=unit_1;Software=SSC
       Specific Problem: TESTPVG
       Description: Communication with a gateway is down.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by restoring communication to the managed gateway. Do this by verifying the availability of the gateway, and comparing the configuration data at the Gateway and the CS 2000 GWC Manager (IP address, protocol/version, etc).

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC305

Log report GWC305 indicates that a test alarm is generated from pmdebug interface to log in to the notilog table. May be any level.

Format

The format for log report GWC305 is as follows:

```
COMPACT2 *** GWC305 JUL10 09:56:30 0671 TBL GWC Fault
      Location: GWC-0-UNIT-0
      NotificationID: 12
      State: Raise
      Category: Communications
      Cause: Unspecified reason
      Time: Jul 10 10:07:23 2003
      Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
          Software=DEBUG
      Specific Problem: Alarms test from debug interface
      Description: This is a test alarm generated from pmdebug interface.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by using the pmdebug command (not a customer interface) or with a GWC reload.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC306

Log report GWC306 indicates a DQoS/COPS connection failure. The alarm severity is major.

Format

The format for log report GWC306 is as follows:

```
COMPACT2 ** GWC306 JUL10 09:56:31 0672 TBL GWC Fault
       Location: GWC-0-UNIT-0
       NotificationID: 13
       State: Raise
       Category: Communications
       Cause: Communications subsystem failure
       Time: Jul 10 10:07:24 2003
       Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
            Software=DQOS MTC
       Specific Problem: DQoS connection CMTS065 has failed - attempting
            rec overy.
       Description: DQoS/COPS connection failure.
```

Selected field descriptions

This log report has no selected fields.

Action

The DQoS connection loss alarm is cleared by DCCNXMGR (using DCALARM) when the connection is reestablished or the connection is deleted from provisioning.

Associated OM registers

This log report has no associated OM registers.

Additional information

When a dynamic quality of service (DQoS) connection is down between the CS 2000 and a CMTS, the CS 2000 will allow new calls hosted by that CMTS to proceed without DQoS. The behavior of the multimedia terminal adapter (MTA) and CMTS determines whether new calls are attempted using best-effort service or whether they are torn down:

- Some MTA vendors allow calls to proceed as data calls (best-effort) and do not send a data-over-cable service interface specification (DOCSIS) authorization block to the CMTS. In this case, the CMTS

cannot recognize the call as a voice call and so it proceeds without managed quality of service.

- Other MTA vendors send the DOCSIS authorization block to the CMTS with no authorization key or gate-id. When this happens, the CMTS decides whether or not to allow calls to proceed.

When the DQoS connection is up, but the CS 2000 does not receive a DQoS gate-id from the CMTS, the CS 2000 will tear down a call.

GWC307

Log report GWC307 indicates an "Element Manager communication failure." EM indicates provisioned data mismatched in this unit, or EM is not responding, provisioned data loaded from local Flash. The alarm severity is Major.

Format

The format for log report GWC307 is as follows:

```
COMPACT06BT ** GWC307 JUL1 10:45:47 0028 TBL GWC Fault
        Location: GWC-3-UNIT-1
        NotificationID: 10
        State: Raise
        Category: Communications
        Cause: Communications subsystem failure
        Time: Jul 01 10:45:51 2003
        Component Id: GWC=GWC-3-UNIT-1;Version=PGC91AQ;Unit=unit_1;
            Software=NODE MTC
       Specific Problem: EM indicates provisioned data mismatched in this
            unit
        Description: Element Manager communication failure.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared with a Busy/RTS of GWC unit.

Restore communication with the CS 2000 GWC Manager. Determine if the CS 2000 GWC Manager is down and or disconnected. Determine if the GWC has been setup to use the wrong IP address for the CS 2000 GWC Manager at the CS 2000 SAM21 Manager.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC308

Log report GWC308 indicates a "Flash memory error." Erase of Flash sector failed. The alarm severity is Minor

Format

The format for log report GWC308 is as follows:

```
COMPACT2 * GWC308 JUL10 09:56:37 0675 TBL GWC Fault
       Location: GWC-0-UNIT-0
       NotificationID: 16
       State: Raise
       Category: Equipment
       Cause: Equipment Malfunction Time: Jul 10 10:07:23 2003
       Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
            Software=FLAS H
       Specific Problem: Erase of Flash sector failed
       Description: Flash memory error.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by replacing the hardware.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC309

Log report GWC309 indicates that the number of the security associations (SA) that the system can support has been exceeded. The associated alarm severity is Minor.

Format

The format for log report GWC309 is as follows:

```
GWC309 AUG10 14:15:09 0674 TBL GWC Fault
    Location: GWC-12-UNIT-0
    Component ID: GWC=GWC-12-UNIT-0;Version=GN070BV;Unit=unit_0;
                  Software=Signalling security
    Alarm Level: Minor
    Alarm Description: Security SAs are nearing capacity
    Category: Processing Error
    Alarm Time: 14:05:10 10-Aug-2004 EDT
    Probable Causes: Resource at or nearing capacity
    Specific Problem: SA nearing capacity
    System Uptime: 1 hours, 0 minutes, 45 seconds
```

Selected field descriptions

This log report has no selected fields.

Action

This log is associated with a minor information alarm. Report this alarm with details to your next level of support. Note that the alarm clears automatically as SA usage decreases.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC311

Log report GWC311 indicates a Warning. "Provisioned GWC Profile not yet activated." The GWC Profile loaded into Flash will activate on the next reload.

Format

The format for log report GWC311 is as follows:

```
COMPACT06BT GWC311 JUL1 10:39:56 0022 TBL GWC Fault
        Location: GWC-3-UNIT-0
        NotificationID: 12
        State: Raise
        Category: Quality of Service
        Cause: Configuration or customization error
        Time: Jul 01 10:40:03 2003
        Component Id: GWC=GWC-3-UNIT-0;Version=PGC91AQ;Unit=unit_0;
             Software=CONFIG
        Specific Problem: GWC Profile loaded into Flash will activate on
             next reload.
        Description: Provisioned GWC Profile not yet activated.
```

Selected field descriptions

This log report has no selected fields.

Action

The alarm condition associated with this log can be cleared by reloading the GWC.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC312

Log report GWC312 indicates a QCA connection failure, either a major alarm (partial outage) or a critical alarm (total outage).

Format

The format for log report GWC312 is as follows:

```
COMPACT2 *** GWC312 JUN30 11:02:37 0586 TBL GWC Fault
       Location: GWC-0-UNIT-0
       NotificationID: 3
       State: Raise
       Category: Communications
       Cause: Communications subsystem failure
       Time: Jun 30 11:09:58 2003
       Component Id: GWC=GWC-0-UNIT-0;Version=PGT09BL;Unit=unit_0;
            Software=QCAMTC
      Specific Problem: QCA connection <qca_47.142.130.70 Port # 20000> has
            failed - attempting recovery.
      Description: QCA connection failure
```

Selected field descriptions

This log report has no selected fields.

Action

No reports are lost since they are collected on a backup server.

- Ensure that the QCA contains the correct properties (port, IP address, etc). Check that the QCA is properly provisioned using the CS 2000 Management Tools.
- Use the ping command to see if you can reach the QCA server. If you cannot reach the server, there may be a problem in the network.
- Verify that there is no memory exhaustion on the QCA server.
- To bring up the links, restart the QCA application on the server.
- Try connecting to a QCA on another CS 2000 Management Tools server.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC313

Log report GWC313 indicates that "RMGC is overloaded." The corresponding alarm severity is Major.

Note: RMGC stands for Redirecting Media Gateway Controller.

The specific problem is that RMGC cannot process all incoming requests. The probable cause is that the resource at or nearing capacity.

Format

The format for log report GWC313 is as follows:

```
COMPACT2 *** GWC313 JUN30 11:02:37 0586 TBL GWC Fault
       Location: GWC-0-UNIT-0
       NotificationID: 3
       State: Raise
       Category: Communications
       Cause: Communications subsystem failure
       Time: Jun 30 11:09:58 2003
       Component Id: GWC=GWC-0-UNIT-0;
       Version=PGT09BL;Unit=unit_0;Software=RMGC
       Specific Problem: RMGC can't process all the incoming requests.
       Description: RMGC overloaded
```

Selected field descriptions

This log report has no selected fields.

Action

The RMGC is temporarily overloaded. The alarm corresponding to this log will clear itself once the RMGC is able to process requests again. Gateways keep sending requests until they get a response. So, once the overload clears, gateways should be able to register without any further intervention.

If the alarm corresponding to this log is seen regularly or does not clear, then this is an indication that there is insufficient RMGC processing capacity in the office. Consider commissioning another RMGC.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC314

Log report GWC314 indicates a Major alarm (partial outage). The Centrex IP Client Manager (CICM) location identification reporting application fails to establish a TCP/IP connection to the location recipient, or the established connection is broken.

Format

The format for log report GWC314 is as follows:

```
CS2K1 *** GWC314 JUN30 11:02:37 0586 TBL GWC Fault
     Location: GWC-213-UNIT-0
     NotificationID: 3
     State: Raise
     Category: Processing Error
     Cause: Communications subsystem failure
     Time: Jun 30 11:09:58 2003
     Component Id: GWC=GWC-213-UNIT-0;Version=GI070BCD;Unit=unit_0;
          Software=LocIdRep
     Specific Problem: Location Id Reporting connection <47.30.178.20>
          has failed - attempting recover
     Description: Location Id Reporting connection failure
```

Selected field descriptions

This log report has no selected fields.

Action

Clear the alarm condition using one of the following approaches:

- Re-establish the connection to the location recipient.
- Disable the location ID reporting application.
- Busy/RTS the GWC unit.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC315

Log report GWC315 indicates the loss of external host interface signals. The alarm severity is as follows:

- Critical
  - more than 50% of provisioned small GWs or media proxies in a disabled state (Format 1)
  - more than 50% of peer connections failed during the 5-minute polling period (Format 2)
- Major
  - 20-49% of provisioned small GWs or media proxies in a disabled state (Format 1)
  - 20-49% of peer connections failed during the 5-minute polling period (Format 2)
  - USP SS7 paths disabled (both links down; Format 3)
  - both USP SS7 links inactive (Format 4)
- Minor
  - some (less than 20%) provisioned small GWs or media proxies in a disabled state (Format 1)
  - some (less than 20%) peer connections failed during the 5-minute polling period (Format 2)
  - USP SS7 paths disabled (one link down; Format 3)
  - one USP SS7 link inactive (Format 4)
- Warning
  - GWs failed DNS lookup during the 5-minute polling period (Format 5)

Format

The formats for log report GWC315 are as follows:

Format 1

```
Network Element: GWC-8-UNIT-1
IP:  (data not available)
Component Id: GWC=GWC-8-UNIT-1;Version=GN090BT;Unit=unit_1;
     Software=OM Collection
Category: Communications
Alarm Time: Wed Aug 17 09:00:00 EDT 2005
Alarm Level: Critical
Probable Cause: Loss of signal
Specific Problem: Small GWs in Disabled State
Description: External communication interface
System Uptime: 1 day, 2 hours, 25 minutes, 0 seconds


Network Element: GWC-22-UNIT-0
IP:  (data not available)
Component Id: GWC=GWC-22-UNIT-0;Version=GN090BV;Unit=unit_0;
     Software=OM Collection
Category: Communications
Alarm Time: Tue Aug 16 06:35:01 EDT 2005
Alarm Level: Major
Probable Cause: Loss of signal
Specific Problem: Media Proxies in Disabled State
Description: External communication interface
System Uptime: 0 hours, 3 minutes, 31 seconds
```

Format 2

```
Network Element: GWC-50
IP:  (could be mate)
Component Id: GWC=GWC-50-UNIT-0;Version=GN090BO;Unit=unit_0;
     Software=OM Collection
Category: Communications
Alarm Time: Mon Jul 25 17:50:00 EDT 2005
Alarm Level: Minor
Probable Cause: Loss of signal
Specific Problem: Peer connections failed during interval
Description: External communication interface
System Uptime: 4 hours, 35 minutes, 36 seconds
```

Format 3

```
Network Element: GWC-11-UNIT-0
IP:  (data not available)
Component Id: GWC=GWC-11-UNIT-0;Version=GN090BV;Unit=unit_0;
     Software=OM Collection
Category: Communications
Alarm Time: Thu Aug 18 09:40:00 EDT 2005
Alarm Level: Minor
Probable Cause: Loss of signal
Specific Problem: USP SS7 paths disabled
Description: External communication interface
System Uptime: 2 days, 3 hours, 9 minutes, 9 seconds
```

Format 4

```
Network Element: GWC-11-UNIT-0
IP:  (data not available)
Component Id: GWC=GWC-11-UNIT-0;Version=GN090BV;Unit=unit_0;
     Software=OM Collection
Category: Communications
Alarm Time: Thu Aug 18 09:40:00 EDT 2005
Alarm Level: Minor
Probable Cause: Loss of signal
Specific Problem: USP SS7 paths inactive
Description: External communication interface
System Uptime: 2 days, 3 hours, 9 minutes, 9 seconds
```

Format 5

```
Network Element: GWC-8-UNIT-1
IP:  (data not available)
Component Id: GWC=GWC-8-UNIT-1;Version=GN090BT;Unit=unit_1;
     Software=OM Collection
Category: Quality of Service
Alarm Time: Wed Aug 17 09:00:01 EDT 2005
Alarm Level: Warning
Probable Cause: Configuration or customization error
Specific Problem: DNS failed GW discovery
Description: External communication interface
System Uptime: 1 DAY, 2 hours, 25 minutes, 1 seconds
```

Selected field descriptions

This log report has no selected fields.

Action

Clear the alarm condition using one of the following approaches:

- Use the small GW OMs to check how many small line GWs are out of service, and use the logs to identify which GWs need attention.
- Use the peer messaging OMs to check the number of calls failed over a longer period, and check the Ethernet link between the GWC and the remote host or peer GWCs.
- Check the USP connections.
- Check the USP configuration to the GWC.

Associated OM registers

The OM name is the same as the log description, for example, External communication interface. This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC318

Log report GWC318 indicates that the Gateway Controller (GWC) initiated an autonomous switch of activity (SWACT) in an attempt to restore communication with its associated media gateways. The alarm severity is critical.

Format

An example of the format for log report GWC318 is as follows:

```
znc0s0jh *** GWC318 NOV16 11:02:37 0126 TBL GWC Fault
        Location: GWC-9-UNIT-0
        NotificationID: 5
        State: Raise
        Category: communications
        Cause: underlyingResourceUnavailable
        Time: Nov 16 11:02:58 2005
        Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0
                      Software=AUTOSWACT
        Specific Problem: GWC-9-UNIT-0: No communication with associated
                          media gateway(s)
        Description: Autonomous SWACT initiated
```

Selected field descriptions

This log report has no selected fields.

Action

Check the related network component managers to identify failures within the network.

The alarm clears automatically when a manual SWACT back to the original active unit is performed.

You can also manually clear this alarm once the problem on the original active unit is solved. Follow procedure "Clear the GWC318 critical alarm manually" in the *Gateway Controller Fault Management*, NN10202-911.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC319

Log report GWC319 indicates that the Gateway Controller (GWC) lost communication with all associated media gateways. The alarm severity is critical.

Format

An example of the format for log report GWC318 is as follows:

```
znc0s0jh *** GWC319 NOV16 15:17:23 0126 TBL GWC Fault
        Location: GWC-9-UNIT-0
        NotificationID: 4
        State: Raise
        Category: communications
        Cause: underlyingResourceUnavailable
        Time: Nov 16 15:17:23 2005
        Component Id: GWC=GWC-9-UNIT-0;Version=GN91AWJK;Unit=unit_0
                      Software=SSC
        Specific Problem: GWC-9-UNIT-0: No communication with associated
                          media gateway(s)
        Description: GWC communication loss with all associated media
                     gateway(s).
```

Selected field descriptions

This log report has no selected fields.

Action

Check the related network component managers to identify failures within the network.

The alarm clears when the GWC detects communication with at least one associated gateway. It also clears when the GWC automatically or manually switches activity but it is raised again on the newly active unit if communication is still lost with all associated gateways.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC320

Log report GWC320 indicates an IKE/IPSec processing problem. The log entry identifies the specific problem. The alarm severity and action depends on the specific problem. For the description of associated GWC320 alarms, see procedure "View and troubleshoot GWC service alarms" in the *Gateway Controller Fault Management*, NN10202-911.

In addition, each specific alarm (except “private key mismatch”) has an associated security log, which provides additional details about the problem. For the description of all IPSec and IKE security logs, see procedure "IPSec and IKE security logs" in the *Gateway Controller Fault Management*, NN10202-911.

Format

The format for log report GWC320 is as follows:

```
Mmm DD hh:mm:ss <OFFICE> GWC320 <severity> TBL  GWC Fault
        Location: GWC-###-UNIT-#
        NotificationID: <integer>
        State: <Raise, Clear>
        Category: processingError
        Cause: <probable_cause>
        Time: Mmm DD hh:mm:ss YYYY
        Component Id: GWC=GWC-###-UNIT-#;Version=<load>;Unit=unit_#;
        Software=Signaling security
        Specific Problem: <specific problem>
        Description: IKE/IPSec
```

Selected field descriptions

The following table explains the selected fields in the log report.

Field	Value	Description
sequence number	0000-9999	Four-digit sequence number identifying a specific log entry.
location	alpha-numeric character string	Identifies the GWC node and unit that initiated the alarm. Example: GWC-8-UNIT-0
notificationID	integer	A unique value assigned each time an alarm is raised.

Field	Value	Description
state	Raise or Clear	Indicates whether the alarm is raised or cleared.
cause	text description	Identifies one of the following probable causes for the alarm: • key expired • underlyingResourceUnavailable • unexpected information
componentID	text description	Identifies the GWC node, its load and the unit that initiated the alarm.
specific problem	text description	Identifies the specific problem associated with the alarm.
description	text description	Indicates an IKE/IPSec-related problem.

Action

The following table describes specific problems and required actions associated with this log report.

Specific problem	Action
`One or more certificates in set number <x> are expiring. An outage may occur if an IKE connectin policy is using these certificates. At the GWCEM, please verify the expiry dates for certificates in set number <x> -- <IP>` *where*: <x> - is the set number of the [IKE certificates] panel <IP> - is the IP address of the GWC node	This log report indicates that an IKE certificate is expiring soon and the GWC Manager has not obtained a new certificate from the Certificate Manager. This condition may cause service disruptions. For information on how to clear the alarm associated with this log report, see the **<*ATM/IP Solution-level ???*, NN?? - to be determined>**
`One or more certificates in set number <x> are expired. An outage will occur if an IKE connectin policy is using these certificates. At the GWCEM, please verify the expiry dates for certificates in set number <x> -- <IP>` *where*: <x> - is the set number of the [IKE certificates] panel <IP> - is the IP address of the GWC node	This log report indicates that an IKE certificate is expired and the GWC Manager has not obtained a new certificate from the Certificate Manager. Service disruption will occur when the certificate expires. For information on how to clear the alarm associated with this log report, see the **<*ATM/IP Solution-level ???*, NN?? - to be determined>**
`Invalid Subject Alternative Name in GWC certificate (set number <x>) -- IP` *where*: <x> - is the set number of the [IKE certificates] Panel <IP> - is the IP address of the GWC node	This log report indicates that the Subject Alternative Name in the GWC certificate does not match the provisioned IP address for the GWC certificate. This may indicate a data or communication problem between the GWC and the GWC Manager. Contact your next level of support.

Specific problem	Action
Phase 1 SA failure -- <remote_gateway_IP_ address>	This log reports indicate that a Phase 1 negotiation failed. This log report is the result of an outage. Refer to the appropriate security log associated with the alarm to obtain more detailed information. See procedure "IPSec and IKE security logs" in the *Gateway Controller Fault Management*, NN10202-911 for the description of IPSec/IKE security logs and required actions.
Phase 2 SA failure -- <remote_gateway_IP_ address>	This log reports indicate that a Phase 2 negotiation failed. This log report is the result of an outage Refer to the appropriate security log associated with the alarm to obtain more detailed information. See procedure "IPSec and IKE security logs" in the *Gateway Controller Fault Management*, NN10202-911 for the description of IPSec/IKE security logs and required actions.
GWC certificate in set number <x> doesn't match private key -- <GWC_IP_address>	This log report may indicate an outage. Contact your next level of support immediately. There are no security logs associated with this specific problem.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC321

Log report GWC321 indicates that the auto-negotiation capability is disabled on the Ethernet Routing Switch 8600. An associated major alarm is raised whenever the system detects that auto-negotiation is disabled on the Ethernet Routing Switch 8600.

Format

The format for log report GWC321 is as follows:

```
<OFFICE>  **  GWC321 MMMDD hh:mm:ss 7413 TBL  GWC Fault
        Location: GWC-###-UNIT-#
        NotificationID: <integer>
        State: Raise
        Category: Communications
        Cause: Configuration or customization error
        Time: Mmm DD hh:mm:ss YYYY
        Component Id: GWC=GWC-###-UNIT-#; Version=<load>;Unit=unit_#;
        Software=IP
        Specific Problem: Auto-negotiation disabled on ethernet link
        Description: Ethernet/IP Errors
```

Selected field descriptions

The following table explains the selected fields in the log report.

Field	Value	Description
Location	Alpha-numeric character string	The field indicates the GWC node and unit that initiated the alarm. Example: GWC-8-UNIT-0
NotificationID	Integer	A unique value assigned each time an alarm is raised for that GWC.
State	Text description	This field indicates the alarm is raised.
Category	Text description	Indicates the X.733-based category of the alarm. In this case, Communications.
Cause	Text description	Indicates the cause of the alarm. In this case, Configuration or customization error.

Field	Value	Description
Time	Alpha-numeric character string	Indicates the date and time of the alarm raise. Example: Jan 26 15:14:25 2006
ComponentID	Text description	This field identifies the GWC node, its load and the unit that initiated the alarm. Example: GWC=GWC-8-UNIT-0;Version=GN091BH;Unit=unit_0;Software=IP
Specific Problem	Text description	This field identifies the specific cause for the alarm. Example: Auto-negotiation disabled on ethernet link.
Description	Text description	This field describes the specific cause for raising the alarm. Example: Ethernet/IP Errors.

Action

Enable the auto-negotiation capability on the Ethernet Routing Switch 8600. If required, refer to Ethernet Routing Switch 8600 configuration documentation.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log is cleared by log report GWC399. If required, see GWC399 on page 281 for more information.

GWC322

Log report GWC322 indicates that the simple network management protocol (SNMP) message rate exceeded the recommended maximum. A minor alarm is raised on crossing the Panic Levels and a warning alarm is raised on crossing the Warning Levels.

Format

The format for log report GWC322 is as follows:

```
<OFFICE>  **  GWC322 MMMDD hh:mm:ss 1234 TBL  GWC Fault
        Location: GWC-###-UNIT-#
        NotificationID: <integer>
        State: Raise
        Category: Communications
        Cause: Threshold crossed
        Time: Mmm DD hh:mm:ss YYYY
        Component Id: GWC=GWC-###-UNIT-#;Version=<load>;Unit=unit_#;
        Software=SNMPMessaging
        Specific Problem: <specific problem>
        Description: A subsystem is overloaded
```

Selected field descriptions

The following table explains the selected fields in the log report.

Field	Value	Description
Location	Alpha-numeric character string	Indicates the GWC node and unit that initiated the alarm. Example: GWC-8-UNIT-0
NotificationID	Integer	A unique value assigned each time an alarm is raised.
State	Raise	Indicates that the alarm is raised.
Category	Text description	Indicates the X.733-based category of the alarm. In this case, Communications.
Cause	Text description	Indicates the cause of the alarm. In this case, Threshold crossed.

Field	Value	Description
Time	Alpha-numeric character string	Indicates the date and time of the alarm raise. Example: Jan 26 15:14:25 2006
ComponentID	Text description	Identifies the GWC node, its load and the unit that initiated the alarm. Example: GWC=GWC-8-UNIT-0;Version=GN091BH;Unit=unit_0;Software=SNMPMessaging
Specific Problem	Text description	Identifies the specific cause for the alarm. Examples: SNMP message rate exceeded recommended maximums . or SNMP message rate is close to recommended maximums.
Description	Text description	Describes the specific cause for raising the alarm. Example: A subsystem is overloaded.

Action

Make sure that the SNMP traffic is reduced.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log is cleared by log report GWC399. If required, see GWC399 on page 281 for more information.

GWC399

Log report GWC399 clears all other GWC logs.

Note: In the case of H.323 GWCs, this log report is generated only for H.323 gateways that contain 64 endpoints or greater.

Format

The format for log report GWC399 is as follows:

```
MSH10_IO6BR      GWC399 MAY26 13:38:30 0529 INFO GWC Fault
        Location: GWC-2-UNIT-1
        NotificationID: 6
        State: Clear
        Time: May 26 13:38:40 2003
```

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.

GWC400

Log report GWC400 is an information-only log and there is no alarm associated with it. Log GWC400 provides IPSec-associated metrics, that is, the log reports how many times an event occurs within a 15-minutes interval. This log is generated every 15 minutes.

Format

The format for log report GWC400 is as follows:

```
GWC400 mmd/dd hh:mm:ss <sequence number> INFO SUMM Security Metrics Summary
Location: GWC-<node number>-UNIT-<unit_number>
AP_REQ: <numeric value>
WAKEUP: <numeric value>
SA_SUCCESS: <numeric value>
SA_FAIL: <numeric value>
SUSPICIOUS_FAIL: <numeric value>
```

Selected field descriptions

The following table explains selected fields in the log report.

Field	Value	Description
sequence number	0000-9999	Four digit sequence number identifying a specific log entry.
node number	numeric	Identifies the GWC node, for example, GWC-6.
unit number	0 or 1	Identifies the GWC unit, 0 or 1.
AP_REQ: <numeric value>	numeric	Identifies how many times the Kerberos application on the GWC received an AP_REQ message.
WAKEUP: <numeric value>	numeric	Identifies how many times the Kerberos application on the GWC sent a wake-up request.
SA_SUCCESS: <numeric value>	numeric	Identifies how many SAs have been successfully established on the GWC.

Field	Value	Description
SA_FAIL: <numeric value>	numeric	Identifies how many times an attempt to establish SAs on the GWC has failed.
SUSPICIOUS_FAIL: <numeric value>	numeric	Identifies how many times an attempt to establish SAs has failed under suspicious circumstances, such as, encryption failure. Contact your next level of support when this event is listed.

Action

This log report requires no action. You can use it for maintenance and diagnostic purposes.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC501

Log report GWC501 indicates a connection fault between the Gateway Controller (GWC) and a gateway configured with NCS or MGCP signaling protocol. The fault requires investigation.

Format

The format for log report GWC501 is as follows:

```
<OFFICE>     GWC501 MMMDD hh:mm:ss <sequence number> PBSY SSC LOG MESSAGE
        Location: <GWC node/unit>
        Component Id: GATEWAY=<MG_name> GWIP:<MG_IP>
        Reason: <fault_reason>
```

Selected field descriptions

The following table explains the selected fields in the log report.

Field	Value	Description
sequence number	0000-9999	Four-digit sequence number identifying a specific log entry.
GWC node/unit	alpha-numeric character string	Identifies the GWC node and unit affected by the failure. Example: GWC-8-UNIT-0
MG_name	alpha-numeric character string	Name of the media gateway (MG) associated with the GWC card and affected by the connection fault. Example: SLOA118-0-3
MG_IP	numeric	IP address of the media gateway Example: 123.1.2.3
fault_reason	text description	Provides more information about the connection fault. Example: GW failed to respond to HeartBeat/Audit.

Action

Verify the availability of the gateway and compare the configuration data at the gateway and the CS 2000 GWC Manager (IP address, protocol, protocol version, and so on).

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC502

Log report GWC502 indicates that service is restored to the referenced gateway.

Note: This log report refers only to gateways configured with NCS or MGCP signaling protocol.

Format

The format for log report GWC502 is as follows:

```
<OFFICE>     GWC502 MMMDD hh:mm:ss <sequence number> RTS SSC LOG MESSAGE
        Location: <GWC node/unit>
        Component Id: GATEWAY=<MG_name> GWIP:<MG_IP>
        Reason: <reason>: <MG_name>
```

Selected field descriptions

The following table explains the selected fields in the log report..

Field	Value	Description
sequence number	0000-9999	Four-digit sequence number identifying a specific log entry.
GWC node/unit	alpha-numeric character string	Identifies the GWC node and unit where the gateway connection was restored. Example: GWC-8-UNIT-0
MG_name	alpha-numeric character string	Name of the media gateway (MG) associated with the GWC card that has the connection restored. Example: SLOA118-0-3
MG_IP	numeric	IP address of the media gateway. Example: 123.1.2.3
reason	text description	Provides more information, including the name of the gateway to which the connection was restored. Example: Connection to remote gateway restored: SLOA23.

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.

GWC503

Log report GWC503 indicates that the gateway dropped the connection to the associated GWC.

Note: This log report refers only to gateways configured with NCS or MGCP signaling protocol.

Format

The format for log report GWC503 is as follows:

```
<OFFICE>     GWC503 MMMDD hh:mm:ss <sequence number> OFFL SSC LOG MESSAGE
    Location: <GWC node/unit>
    Component Id: GATEWAY=<MG_name> GWIP:<MG_IP>
    Reason: <reason>: <MG_name>
```

Selected field descriptions

The following table explains the selected fields in the log report.

Field	Value	Description
sequence number	0000-9999	Four-digit sequence number identifying a specific log entry.
GWC node/unit	alpha-numeric character string	Identifies the GWC node and unit to which the gateway dropped the connection. Example: GWC-8-UNIT-0
MG_name	alpha-numeric character string	Name of the media gateway (MG) that dropped the connection with the associated GWC. Example: SLOA118-0-3
MG_IP	numeric	IP address of the media gateway. Example: 123.1.2.3
reason	text description	Provides more information about the connection drop, including the name of the gateway that initiated it. Example: Connection drop initiated by remote gateway: SLOA23.

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.

GWC506

Log report GWC506 indicates that an H.323 GWC unit has lost the connection to an H.323 gateway. The log entry identifies the specific problem and describes the reason for the failure.

This log report recommends a set of actions that depend on the specific problem and reason for the problem.

Note: This log report is generated only for H.323 gateways that contain less than 64 endpoints.

Format

The format for log report GWC506 is as follows:

```
RTPG     GWC506 MAY21 14:54:47 <sequence number> PBSY Gateway State Change
         Category: Communication
         Component Id: GWC=<GWC node/unit>;LINK=<gateway name>
         Specific Problem: H323 Connection lost to gateway <gateway name>
         Description: <reason for problem>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
sequence number	0000-9999	Four digit sequence number identifying a specific log entry.
GWC node / unit	Alpha-numeric text label	Identifies the GWC node and unit affected by the failure. Example: GWC-11-UNIT-0
gateway name	Alpha-numeric text label	Identifies the gateway connected to the GWC card affected by the failure condition. Example: BCM_RTPG1
reason for problem	Text description	Describes the specific reason for the failure.

Action

The following table describes the actions the user may take when a GWC experiences a loss of connection to an H.323 gateway.

Actions associated with a loss of connection to an H.323 gateway

Description	Action
Gateway Unregistration by CS2K Successful	No action required. The craftsperson has busied the D-channel for the H.323 gateway, or the CS 2000 has busied the D-channel for H.323 gateway due a maintenance action such as GWC cold SWACT, CS 2000 restart reload, etc.
Time to Live Expired	The H.323 gateway failed to refresh the 30 second keepalive timer in the CS 2000 GWC. Verify communication between the gateway and the GWC. If necessary, check the H.323 gateway itself since the CS 2000 GWC unregistered the H.323 gateway because the Time To Live value has expired.
Gateway Initiated Unregistration Successful	The H.323 gateway initiated the unregistration from the CS 2000 for some reason. Action on the H.323 gateway side may be warranted if the Unregistration was unplanned.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

GWC507

Log report GWC507 indicates that the connection between a GWC and an H.323 gateway has been restored.

Note: This log report is generated only for H.323 gateways that contain less than 64 endpoints.

Format

The format for log report GWC507 is as follows:

```
RTPG     GWC507 AUG02 14:15:28 <sequence number> RTS Gateway State Change
         Category: Communication
         Component Id: GWC=<GWC node/unit>;LINK=<gateway name>
         Specific Problem: H323 Connection restored to gateway <gateway name>
         Description: Gateway Registration Successful
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
sequence number	0000-9999	Four digit sequence number identifying a specific log entry.
GWC node / unit	Alpha-numeric text label	Identifies the GWC node and unit affected by the failure. Example: GWC-11-UNIT-0
gateway name	Alpha-numeric text label	Identifies the gateway connected to the GWC card affected by the failure condition. Example: BCM_RTPG1

Action

No action is required.

You may verify that the D-channel has gone in service (INSV) at the MAPCI;MTC:TRKS; TTP; PRADCH; POST GD <trkname >. If any trunk members are provisioned and you wish to be able to make calls, then check the trunk members to see that they are also idle (IDL).

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

GWC600

Log report GWC600 is an information log for an H.323 failure. The log entry identifies the specific problem and describes the reason for the failure.

This log report recommends a set of actions that depend on the specific problem and reason for the problem.

Format

The format for log report GWC600 is as follows:

```
<OFFICE>      GWC600 MMMDD hh:mm:ss <sequence number INFO GWC Protocol Event
        Location: <GWC node/unit>
        Component Id: GWC=<GWC node/unit>;LINK=<gateway name>
        Category: Communication
        Specific Problem: <specific problem>
        Description: <reason for problem>
```

Example:

```
COM4        GWC600 FEB14 23:55:51 0415 INFO GWC Protocol Event
        Location: GWC-44-UNIT-0
        Component Id: GWC=GWC-44-UNIT-0;LINK=HURR02
        Category: Communication
        Specific Problem: H323 Call Rejected
        Description: Codec / Payload Mismatch With CS2K
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	Alphanumeric	11-character identifier indicating which office the log comes from.
sequence number	0000 to 9999	Four-digit sequence number identifying a specific log entry.
GWC node/unit	Alphanumeric text label	Identifies the GWC node and unit affected by the failure. Example: GWC-11-UNIT-0

Field	Value	Description
gateway name	Alphanumeric text label	Identifies the gateway connected to the GWC card affected by the failure condition. Example: BCM_RTPG1
specific problem	Text description	Identifies the H.323 failure condition (see the table below for a list of possible values and corresponding user actions required).
reason for problem	Text description	Describes the specific reason for the failure.

Action

The following table describes the actions the user takes when an H.323 failure condition occurs.

Note:
GRQ = Gatekeeper request
RRQ = Registration request
ARQ = Admission request
URQ = Unregistration request
DRQ = Disengage request
RAS = Registration, admission and status

Actions associated with an H.323 failure (Sheet 1 of 4)

Specific problem	Description	Action
H323 GRQ rejected	Gateway Name Not Provisioned ***Note:*** A log with same description is generated for RRQ received with invalid GW name.	Ensure that the H.323 gateway name provisioned on the CS 2000 GWC Manager matches exactly with the gateway name provisioned using the H323 GW provisioning tool.
H323 GRQ rejected	Gateway IP Address Invalid ***Note:*** A log with same description is generated for RRQ received with an invalid source gateway IP address. In this case, the source IP address is the IP address in the ethernet frame. So, for gateways behind the NAT, the source IP address will be the NAT IP address. The RAS IP address is not part of the H.323 payload. If the H.323 gateway is not behind a NAT, the source IP will be the IP address of the H.323 gateway.	If the H.323 gateway is behind the NAT: • Ensure that the H.323 gateway IP address provisioned on the CS 2000 GWC Manager matches exactly the IP address of the NAT box. If the H.323 Gateway is not behind a NAT box: • Ensure that the H.323 gateway IP address provisioned on the CS 2000 GWC Manager matches exactly the IP address of the H323 gateway.

Actions associated with an H.323 failure (Sheet 2 of 4)

Specific problem	Description	Action
H323 GRQ rejected	Gateway Port Invalid ***Note:*** A log with same description is generated for an RRQ received with an invalid source gateway port. In this case, the source port is the source port address in the ethernet frame. So, for gateways behind a NAT, the source port is the port entry of the static bind at the enterprise NAT for the H323 gateway. It is not the RAS port which is part of the H323 payload. If the H323 Gateway is not behind a NAT, the source port will be the RAS port of the H323 gateway.	If the H.323 gateway is behind the NAT: • Ensure that the H.323 gateway port provisioned on the CS 2000 GWC Manager matches exactly the port entry of the static bind at the enterprise NAT for the H323 gateway. If the H.323 Gateway is not behind a NAT box: • Ensure that the H.323 gateway IP address provisioned on the CS 2000 GWC Manager matches exactly the IP address of the H323 gateway.
H323 GRQ rejected	Missing Mandatory RAS Address	No action needed. This log report is for information only.
H323 RRQ rejected	Incorrect Endpoint Identifier Syntax	No action needed. This log report is for information only.
H323 keepAlive RRQ rejected	Incorrect Endpoint Identifier Syntax	No action needed. This log report is for information only.
H323 RRQ rejected	Invalid Endpoint Identifier	No action needed. This log report is for information only.
H323 ARQ rejected	Invalid Endpoint Identifier	No action needed. This log report is for information only.
H323 RRQ rejected	D-Channel Not Provisioned	Ensure that the trunk datafill is provisioned correctly on the CS 2000 Core and CS 2000 GWC Manager.

Actions associated with an H.323 failure (Sheet 3 of 4)

Specific problem	Description	Action
H323 RRQ rejected	D-Channel Out Of Service	Ensure that the D-channel associated with the H.323 gateway is in LO state at mapci, mtc, ttp, trks, pradch level on the CS 2000 Core before the H.323 gateway registers. This log can be cleared with a BSY/RTS of the D-channel associated with the H.323 gateway on the CS 2000 Core. ***Note:*** Trunk logs are also generated which are similar to PRI trunk logs. For example, H.323 gateway "BCM_RTPG" appears on the Core as trunk name "RTPG_BCM_LOCAL" Refer to section Additional information on page 299 for examples of Core logs.
H323 RRQ rejected	Table LTDATA Needs H323 Option	Check the datafill in Table LTDATA on the CS 2000 Core. The option PRI_IP_PROT H323 should be present for the D-channel associated with the H.323 gateway.
H323 RRQ rejected	Max Gateways Registered	No action needed. This log report is for information only. The CS 2000 GWC has reached the maximum limit for the number of H.323 gateways it can have registered simultaneously.
H323 ARQ rejected	B-Channel Resource Unavailable	Ensure that B-channels associated with the gateway are idle (IDL) at mapci, mtc, ttp, trks level on the CS 2000 Core. This log can be cleared with a BSY/RTS of the B-channels associated with the H.323 gateway on the CS 2000 Core. If all the B-channels associated with the H.323 gateway are call processing busy (CPB) at mapci, mtc, ttp, trks level on the CS 2000 Core, then no action is needed. There is no B-channel available for the call. This log report is for information.

Actions associated with an H.323 failure (Sheet 4 of 4)

Specific problem	Description	Action
H323 RRQ rejected	No GWC Unit Active Running ***Note:*** A log with the same description will be generated if any RAS message (GRQ, RRQ, ARQ, URQ, DRQ) is received when the GWC unit is not active running. This log can be cleared with a BSY/RTS of GWC unit.	Ensure that the CS 2000 GWC is in active running state. This log can be cleared with a BSY/RTS of GWC unit.
H323 DRQ rejected	Request to Drop Non Existent Call	No action needed. This log report is for information only. This reports a disengage request for a call which is not active or non-existent.
H323 URQ rejected	Endpoint Not Registered	A RAS request is received from a H.323 gateway which is not registered on the CS 2000 GWC. Verify that the H.323 gateway is provisioned on the CS 2000 GWC.
H323 Call rejected	Codec Mismatch With CS2K	Ensure that at least one of the codecs provisioned on the H323 gateway matches the codec for the CS 2000 provisioned at the CS 2000 GWC Manager.
H323 Call rejected	Codec / Payload Mismatch With CS2K	Ensure that at least one of the codecs provisioned on the H323 gateway matches the codec for the CS 2000 provisioned at the CS 2000 GWC Manager. Ensure that the payload (packetization) time on the H323 gateway matches the payload (packetization) for the CS 2000 provisioned at the CS 2000 GWC Manager.
H323 Call rejected	H245 Tunneling Not Enabled On Gateway	Ensure that H.245 tunneling is enabled on the H.323 gateway.

Associated OM registers

This log report has no associated OM registers.

Additional information

This section provides examples of Core logs relevant to

- Specific problem: H323 RRQ rejected
- Description: D-Channel Out Of Service.

Examples of Core logs when the D-channel is manually busied (BSY):

```
RTPG * ISDN105 JUN16 21:45:44 2311 FLT PRA Sync Loss
   ISP = 0 GWC 11 PORT 0 CHNL 0

RTPG *** ISDN112 JUN16 21:45:44 2412 INFO PRA D-CHANNEL
  CRITICAL ALARM RTPG_BCM_LOCAL DCH=GWC 11 120 1 : OOS

RTPG *** TRK103 JUN16 21:45:49 2917 FLT GROUP_ALARM
   RTPG_BCM_LOCAL 100% BUSY
```

Examples of Core logs when the D-channel is returned to service (RTS) and the gateway registers with GWC:

```
RTPG ISDN118 JUN16 21:46:52 6654 INFO PRA Sync Established
   ISP = 0 GWC 11 Port 0 Chnl 0

RTPG TRK104 JUN16 21:46:56 7462 INFO GROUP OK
   RTPG_BCM_LOCAL
```

GWC601

Log report GWC601 is an information-only log that indicates the change of the Gateway Controller (GWC) Manager IP address.

This log report is available on both Managers:

- the one that is currently associated with the GWC
- the one that served the GWC before the configuration changed

Format

The format for log report GWC601 is as follows:

```
<OFFICE>      GWC601 MMMDD hh:mm:ss <sequence number> INFO Configuration Change
         Location: <GWC node/unit>
         Component Id: GWC=<GWC node/unit>;Software=SystemConfig
         Changed value: Element Manager address
         Previous: <previous_EM_IP> New: <current_EM_IP>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	alphanumeric	11-character identifier indicating the office that generated the log report.
sequence number	0000 to 9999	Four-digit sequence number which can be used for lost log detection.
GWC node/unit	alphanumeric character string	Identifies the GWC node and unit for which the configuration change occurred.
previous_EM_IP	numeric	IP address of the Manager that served the GWC before the configuration changed.
current_EM_IP	numeric	IP address of the Manager that is currently serving the GWC after the configuration change.

Action

No action required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log event is extremely rare. If it occurs, treat it as a sign of possible security problem.

GWC603

Log report GWC603 is an information-only log and there is no alarm associated with it. Log GWC603 indicates that a netfail event occurred on the gateway and it was reported to the Gateway Controller (GWC).

Format

The format for log report GWC603 is as follows:

```
<OFFICE>     GWC603 MMMDD hh:mm:ss <sequence_number> INFO NETFAIL EVENT
        Location: GWC-<node>-UNIT-<unit>
        Component Id: GATEWAY=<MG_name> GWIP:<MG_IP> ENDPOINT ID: <Epid>
        TID: <Tid> Reason: <Exception Reason>
```

Selected field descriptions

The following table explains the selected fields in the log report.

Field	Value	Description
sequence_number	0000-9999	Four-digit sequence number identifying a specific log entry.
GWC node-unit	alpha-numeric character string	GWC node and unit affected by the failure. Example: GWC-11-UNIT-0
MG_name	alpha-numeric character string	Name of the media gateway associated with the GWC card affected by the failure condition.
MG_IP	numeric	IP address of the media gateway. Example: 123.1.2.3
Epid	alphanumeric character string	Identifier of the endpoint that caused the exception. Example: tp/0/0028
Tid	numeric	Internal Terminal ID maintained by the GWC. Example: 4125
Exception Reason	alpha-numeric character string	The cause of the netfail event. Example: 599 Connection Lost

Action

No action required. This log report provides additional information when TRK113 or LINE104 log is generated on the Core as a result of netfail event received from H.248 gateways.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report required no additional information.

GWC604

Log report GWC604 is an information-only log and there is no alarm associated with it. This report indicates an internal Gateway Controller (GWC) exception. Use this log report for debugging process.

Format

The format for log report GWC604 is as follows:

```
<OFFICE>    GWC604 MMMDD hh:mm:ss <sequence_number> INFO GWC EXCEPTION EVENT
        Location: GWC-<node>-UNIT-<unit>
        Component Id: GATEWAY=<MG_name> GWIP:<MG_IP> ENDPOINT ID: <Epid>
        TID: <Tid> Reason: <Exception Reason>
```

Selected field descriptions

The following table explains the selected fields in the log report.

Field	Value	Description
sequence_number	0000-9999	Four-digit sequence number identifying a specific log entry.
GWC node-unit	alpha-numeric character string	GWC node and unit affected by the failure. Example: GWC-11-UNIT-0
MG_name	alpha-numeric character string	Name of the media gateway associated with the GWC card affected by the failure condition.
MG_IP	numeric	IP address of the media gateway. Example: 123.1.2.3
Epid	alphanumeric character string	Identifier of the endpoint that caused the exception. Example: tp/0/0028
Tid	numeric	Internal Terminal ID maintained by the GWC. Example: 4125
Exception Reason	alpha-numeric character string	The reason for raising the exception. Example: Insufficient Bandwidth

Action

No action required. Usually (but not always) this log report is generated in conjunction with log report TRK113 or LINE104 on the Core. Use both log reports for debugging process.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report required no additional information.

GWC605

Log report GWC605 indicates that the M3UA Application Server Process (ASP) path audit has detected all the ASP paths in the down state for ten minutes. When this happens, the system initiates an autonomous SWACT request.

Format

The format for log report GWC605 is as follows:

```
<OFFICE>        GWC605 MMMDD hh:mm:ss <sequence number> INFO M3UA EVENT
        Location: <GWC node/unit>
        Component Id: GWC=<GWC node/unit>;Software=M3UA_ASP_AUDIT
        Event: Autonomous Swact Request
        Reason: M3UA ASP paths down
```

Example:

```
COM4        GWC605 JAN04 16:29:54 9129 INFO M3UA EVENT
        Location: GWC-34-UNIT-0
        Component Id: GWC=GWC-34-UNIT-0;Software=M3UA_ASP_AUDIT
        Event: Autonomous Swact Request
        Reason: M3UA ASP paths down
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	Alphanumeric	11-character identifier indicating which office the log comes from.
sequence number	0000 to 9999	Four-digit sequence number which can be used for lost log detection.
GWC node/unit	Alphanumeric text label	Identifies the GWC node and unit affected by the event.
Event	Text description	Indicates that the event Autonomous Swact Request is initiated.
Reason	Text description	Indicates the reason for the log: the M3UA ASP paths are down for ten minutes.

Action

GWC605 log reports that a warm SWACT request is initiated if the M3UA ASP paths are down for ten minutes. The warm SWACT attempts to recover the M3UA links and bring back the trunks into service. No specific action is required, as the event takes place automatically.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC606

Log report GWC606 is an information log for a Media Proxy (MP) idle or long call detection event. Idle and long call durations are measured in terms of audit periods, which the user can define in the Media Proxy element manager.

The log contains a correlation ID passed down from the Core. This correlation ID is used for correlation with an associated billing record for that call. In (I)SN09FF this is the only mechanism available to link generated logs with particular billing records.

Format

The format for log report GWC606 is as follows:

```
<OFFICE>        GWC606 MMMDD hh:mm:ss <sequence number> INFO Media Proxy
        Location: <GWC node/unit>
        Component Id: MEDIA PROXY=<MP_name>
        Reason: <Long/Idle> Call Detected, CorrelationID=<Correlation Id>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	Alphanumeric	11-character identifier indicating which office the log comes from.
sequence number	0000 to 9999	Four-digit sequence number which can be used for lost log detection.
GWC node/unit	Alphanumeric text label	Identifies the GWC node and unit affected by the event.
MP_name	Alphanumeric character string	The name of the Media Proxy for which the long or idle call has been detected.
Long/Idle	Alphabetic; Long or Idle	Identifies the type of call (long call or idle call) detected.
Correlation Id	Numeric	30-digit number used for correlation with an associated billing record for that call.

Action

The user should review the contents of the log report and take action as shown in the following table.

Actions associated with a long/idle call event

Specific problem	Description	Action
Long Call Detected	Call longer than long call duration defined in Media Proxy element manager.	Use the correlation ID in the log to identify the associated billing record for that call.
Idle Call Detected	Call longer than idle call duration defined in Media Proxy element manager.	Use the correlation ID in the log to identify the associated billing record for that call.

Note: In order to associate the correlation ID with a particular billing record, the Quality of Service feature must be configured and activated.

Associated OM registers

This log report has no associated OM registers.

Additional information

This section provides examples of log report GWC606.

NTSTD example

```
CS2K5      GWC606 FEB16 02:52:09 3592 INFO Media Proxy
        Location: GWC-3-UNIT-0
        Component Id: MEDIA PROXY=SAM16P4
        Reason: Long Call Detected, CorrelationID=1110002231110001572472410060000

CS2K5      GWC606 FEB16 02:52:09 3593 INFO Media Proxy
        Location: GWC-3-UNIT-0
        Component Id: MEDIA PROXY=SAM16P4
        Reason: Idle Call Detected, CorrelationID=1110002231110001572472410060000
```

SNMP example

```
enterprise=1.3.6.1.4.1.562.29.6.1.0.306
uptime=26274273
agent_ip=47.129.118.161
version=Ver2
1.3.6.1.4.1.562.29.6.1.3.1.1=.0.0
1.3.6.1.4.1.562.29.6.1.3.1.2="IEMS=0x00000063000000a10a68011a-GWC-3-UNIT-0;MEDIA PROXY=SAM16P4"
1.3.6.1.4.1.562.29.6.1.3.1.3="Hex String=07 D6 02 10 02 34 09 00 2D 05 00"
1.3.6.1.4.1.562.29.6.1.3.1.4=GWC606
1.3.6.1.4.1.562.29.6.1.3.1.5="  52 GWC 606 3591 INFO Media Proxy          <010><013>Long Call Detected,
CorrelationID=1110002231110001572472410060000"

enterprise=1.3.6.1.4.1.562.29.6.1.0.306
uptime=26274273
agent_ip=47.129.118.161
version=Ver2
1.3.6.1.4.1.562.29.6.1.3.1.1=.0.0
1.3.6.1.4.1.562.29.6.1.3.1.2="IEMS=0x00000063000000a10a68011a-GWC-3-UNIT-0;MEDIA PROXY=SAM16P4"
1.3.6.1.4.1.562.29.6.1.3.1.3="Hex String=07 D6 02 10 02 34 09 00 2D 05 00"
1.3.6.1.4.1.562.29.6.1.3.1.4=GWC606
1.3.6.1.4.1.562.29.6.1.3.1.5="  52 GWC 606 3592 INFO Media Proxy          <010><013>Idle Call Detected,
CorrelationID=1110002231110001572472410060000"
```

SCC2 example

```
52 GWC 606 3591 INFO Media Proxy
      Location: GWC-3-UNIT-0
      Component Id: MEDIA PROXY=SAM16P4
      Reason: Long Call Detected, CorrelationID=1110002231110001572472410060000

52 GWC 606 3592 INFO Media Proxy
      Location: GWC-3-UNIT-0
      Component Id: MEDIA PROXY=SAM16P4
      Reason: Idle Call Detected, CorrelationID=1110002231110001572472410060000
```

Syslog example

```
Feb 16 16:10:59 zcary0tn IEMS: _V2_~I=~H=zcary0tn~A=IEMS~S=3986~~  GWC606 NONE INFO  Media Proxy^M
Location: GWC-3-UNIT-0^M        Component Id: MEDIA PROXY=SAM16P4^M        Reason: Long Call Detected,
CorrelationID=1110002231110001572472410060000

Feb 16 16:10:59 zcary0tn IEMS: _V2_~I=~H=zcary0tn~A=IEMS~S=3987~~  GWC606 NONE INFO  Media Proxy^M
Location: GWC-3-UNIT-0^M        Component Id: MEDIA PROXY=SAM16P4^M        Reason: Idle Call Detected,
CorrelationID=1110002231110001572472410060000
```

GWC609

Log report GWC609 is an information log that is generated when the Gateway Controller (GWC) detects communication issues with an in-service trunk or large capacity line gateway. This occurs for the first missed heartbeat reply and when communication lost is declared for a gateway. In the later case, an accompanying GWC304 trouble log is also generated.

The GWC609 log contains the output of a traceroute command performed from the GWC to the IP address of the gateway. For traceroute to function end-to-end, ICMP protocol must be allowed to pass through all routers and firewalls between the GWC and the gateway.

The personnel that support the network path between the GWC and gateway may use this log to determine if action is required to restore or maintain communication from the GWC to gateway.

Format

The format for log report GWC609 is as follows:

```
<OFFICE>        GWC609 MMMDD hh:mm:ss <sequence number> INFO Traceroute
        Location: <GWC node/unit>
        Component Id: GWC Card=<GWC node/unit>;GATEWAY=<Gateway>
        Description: Traceroute to <Gateway IP>  <Status>.
        <Result>.
        Hop Data (rtt in ms):
        1  47.142.64.1      0
        2  47.142.204.205   2
        3  47.143.206.21    5
        4  47.143.205.1     10
        5      *
        6      *
        7      *
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
OFFICE	Alphanumeric	11-character identifier indicating which office the log comes from.
sequence number	0000 to 9999	Four-digit sequence number which can be used for lost log detection.
GWC node/unit	Alphanumeric text label	Identifies the GWC node and unit where the traceroute originated from. Example: GWC-3-UNIT-1
Gateway	Alphanumeric text label	Identifies the name of the gateway for which the traceroute is being executed for. This gateway name will match the gateway name seen in the GWC Manager.
Gateway IP	IPv4 IP address	Identifies the IP address for the Gateway which the traceroute is being executed for. Example: 47.135.21.3
Status	Executed or Aborted	Identifies the summary status of the traceroute.
Result	Alphanumeric text label	Explanation for the result of the traceroute. Aborted explanations: "Running longer than 5 seconds" or "Max of 20 hops exceeded." Executed explanations: "Could not reach destination." or "Destination reached. Last GW signaling msg received <x> secs ago." For the case where the traceroute successfully reached the destination, the log also includes how many seconds have elapsed from when the traceroute completed and the GWC last received a message from the gateway on its signaling (e.g., H.248) path. The log also includes the hop data with the round-trip time in milliseconds. A time out for a hop is indicated by an asterisk.

Action

No action is required. The traceroute hop data can be used to help identify network issues that may be causing communication problems between the GWC and gateway.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

GWC702

Log GWC702 is generated when the dynamic data download for trunk subgroup data, table TRKSGRP in the CS 2000 Core, fails for a specific tuple. The log indicates the tuple that failed to download to a GWC, and the GWC that failed to receive the data.

Format

The format for log report GWC702 is as follows:

```
MSH306BT  GWC702 DEC24 13:17:53 9000 INFO GWC Trunk Subgroup DDM Dynamic
                                                                    Update
      DDM Dynamic Update Failed for Group: DPT113EGATM
      Subgroup: 0  GWC: 11
```

Selected field descriptions

The following table describes the fields in the log report:

Field	Values	Description
INFO	GWC Trunk Subgroup DDM Dynamic Update	
Group	alphanumeric	The tuple that failed to download to a GWC.
Subgroup	numeric	The tuple that failed to download to a GWC.
GWC	numeric	The GWC that failed to receive the data.

Action

No immediate action is required.

If calls for that trunk group are failing, the trunk data required for routing may be missing in the GWC. There are two possible actions:

- Attempt to change the TRKSGRP tuple in the CS 2000 Core, to force another dynamic data download.
- Cold SWACT the affected GWC, to force the data to load again.

If neither of the above actions corrects the failed calls, contact Nortel support.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log is very rare.

PM180

Log report PM180 appears when the system encounters a software exception. A software exception occurs when software is not used correctly. Operating company personnel use log report PM180 to identify and correct software errors. A software exception that relates to hardware can also generate log report PM180.

The PM subsystem generates this report when a software condition occurs. This software condition affects normal operation of the DMS or the peripherals of the DMS. Formats 3 and 4 supply information on a PM EXCEPTION REPORT. Format 5 identifies software exceptions in the remote line concentrating module with extended distance capability (RLCM-EDC) and the universal edge 9000 (UE9000).

Format

The format for log report PM180 is as follows:

```
PM180 mmmdd hh:mm:ss ssdd TBL PM EXCEPTION REPORT
   pmid UNIT n: acttxt
   TASKID : taskid, TIME: hhhhhhhh, COMID: comid
   TEXT: swerrtxt hh hh hh hh hh hh hh
   CONTEXT TERMINAL: TID=(nodenum,termnum), EXTBYTE=n,
   AGENT=CKT trkid
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
TBL PM EXCEPTION REPORT	Constant	Indicates a PM exception report.
pmid	Symbolic text	Identifies the affected PM
UNIT	Integer (0 or 1)	Identifies the PM unit that generates the report
acttxt	Act	Indicates that the PM unit is active (Act). Not provided for digital line module (DLM).
	Inact	Indicates that the PM unit is inactive (Inact). Not provided for DLM.
TASKID	Symbolic text	Provides identification for suspect task

Field	Value	Description
TIME	Hex (0000-FFFF)	Indicates time that exception occurred
COMID	Hex (0000-FFFF), Character string	Provides communication port identification. Not provided for DLM.
swerrtxt	Character string	Provides the reason for the exception.
hhhh	Hex (0000-FFFF)	The 14 hexadecimal characters display contents of process status word for DLMs. The hexadecimal characters display more than 14 characters in the hhhh format to display the following: • contents of process status word • different registers • other information used in troubleshooting
CONTEXT TERMINAL	Constant	Indicates the information that follows applies to the terminal involved in the transaction that produced the exception condition. Not provided for DLM.
TID	Integers	Provides the node number and terminal number for terminal identification. Not provided for DLM.
EXTBYTE5000	0 or 1	Identifies the extension byte of the call involved in the exception condition. Electronic business sets use the extension byte to distinguish directory number (DN) keys. For 500 series and 2500 series sets and for trunks, the field does not apply and is set to zero. Not provided for DLM.
AGENT	Symbolic text	Provides identification for context terminal equipment. Not provided for DLM.
TEXT	CMR CARD TROUBLE	Indicates the system detected a problem on the CLASS modem resource (CMR) card. The system attempts to reset the card. Report that this log occurred.
	Character string or blank	Provides additional information for operating company personnel to isolate problems
hhhh	Hex (0000-FFFF)	Provides a dump of information for operating company personnel to use
Text string	Alphabetic	Provides the reason of the exception

Field	Value	Description
Software Exception	Character string	Provides the reason for the log
Processor ID	MP, CP, or PP	Indicates that the processor in the RLCM-EDC or the UE9000 that generates the report is one of the following: • master processor • control side (C-side) • peripheral processor (P-side)
Task ID	Symbolic text	Identifies the ID of the RLCM-EDC or the UE9000 task that generated the log
Time	00 00-2359	Indicates the RLCM-EDC or the UE9000 time of exception
Data	Hex (0000-FFFF)	Identifies the type of hardware exception
site	0000-ZZZZ	Identifies the site to the ILDR
frame	0 through 99	Identifies the line concentrating module (LCM) frame number
drawer	0 through19	Identifies the ILDR drawer number in the LCM
swerrdata	Character string	Provides the exception data from the software error text (swerrtxt)

Action

Attempt to interpret swerrdata character string to determine the cause of the exception. If you are not able to interpret swerrdata, contact the next level of support.

If the system indicates a hardware problem, perform diagnostic and maintenance procedures on the suspect equipment.

If the character string indicates a software error, retain the log report for trend analysis. There is no action required.

For formats 3 and 4, save all reports generated during the 5 min before the subsystem generated log report PM180 report. Contact the next level of support.

For format 5, save all reports generated during the 6 h before the subsystem generated log report PM180. 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.

PM181

Log report PM181 is generated when a specified step occurs in a PM function. This log also reports the occurrence of a PM exception.

This log report contains the following information:

- The section Examples on page 320 provides examples of events and fault conditions associated with log report PM181.
- The section Format on page 330 presents the different formats for log report PM181.
- The section Selected field descriptions on page 337 contains a table describing the selected fields applicable to the different log formats.
- The section Action on page 343 provides actions associated with the different fault conditions and log formats.
- The section Additional information on page 352 provides information, explanations and actions associated with different fault conditions and messages.

Examples

This section provides numbered examples of events and fault conditions associated with the different formats of log report PM181. To see each format referenced, refer to section Format on page 330.

Format 1 - The following conditions use format 1:

- Examples 1 and 2 use Format 1. The PM generates these examples when a request for diagnostics arrives from the host. The subsystem also generates these examples during a return to service (RTS) procedure with diagnostics permitted. Format 1 specifies the unit (0 or 1) for a routine exercise (REX) test failure, if the failure is unit specific.
- Example 3 uses Format 1. The PM subsystem generates this example in the following condition. The call processing node status table is not the same as the current status of the line appearance on a digital trunk (LDT). The LDT node status table records the current status.
- Example 4 uses Format 1. The PM subsystem generates this example when one or more frame transport buses (F-bus) tap in a link interface module (LIM). The error occurs because the frame transport buses have changed to the in-service trouble (ISTb) state within the previous 3 s.

- Example 5 uses Format 1. The PM subsystem generates this example when an XMS-based peripheral module (XPM) facility audit detects a state change in an echo canceller module.
- Example 22 uses Format 1. The PM subsystem generates this example under the following conditions:
  - a line concentrating module (LCM) REX test or LCM continuity and voltage (LCMCOV) REX test passes
  - the LCM REX test or LCMCOV REX test has not occurred on a specified node for a fixed number of days

  In NA004 and up, feature AF5898 (LCM REX Controller Enhancement) migrates the LCM REX test from the LCM node audit process of the system REX (SREX) controller. Feature AF5898 also places the continuity and voltage (COV) part of the LCM REX test in a separate LCMCOV test.
- Example 24 uses Format 1. The PM subsystem generates this example when a return to service command fails on an external node entered in table EXNDINV.
- Example 25 uses Format 1. This example generates when a TEST command fails on an external node entered in table EXNDINV.
- Example 26 uses Format 1. The PM subsystem generates this example when a service processor with UNIX (SPX) is system busy. The log lists the possible causes for the system being busy, which can include faults in the following components:
  - the single-shelf link peripheral processor (SSLPP)
  - Ethernet interface unit (EIU)
  - local area network (LAN) connections
  - the LAN-BAY cards
  - the SPX cards

Format 2 - The following conditions use Format 2:

- Example 6 uses Format 2. The PM subsystem generates this example for PMs when a PM exception occurs.
- Examples 7, 8, and 9 use Format 2. These examples provide the status of the intelligent peripheral equipment (IPE) load.
- Example 21 uses Format 2. The subsystem generates this example when a BSY PM command causes removal of an LCM node from

an in-service (InSv) state. The LCM node changes to an out-of-service (OOS) state.

- Example 28 uses Format 2. The PM subsystem generates this example when a digital subscriber loop (xDSL) line card is added to the LNINV table. The drawer for the table does not support the high speed data traffic of the 1 Meg Modem Service. The line installed functions as a standard voice line only.
- Example 29 uses Format 2. The PM subsystem generates this example when an xDSL line card is added to the LNINV table. The drawer for the table supports the high speed data traffic of the 1 Meg Modem Service. The line drawer contains more xDSL line cards than the xDSL engineering rules allow. The installed xDSL line card functions as an xDSL line. The whole line drawer is at risk of failure because the drawer is operating beyond its thermal and electrical limits. Operating company personnel receive warning of the xDSL engineering rules breach at the time of the addition. These personnel can perform the following actions to correct the condition:
  - use the QXNET EXPANDALL command to locate another LCM that supports xDSL and has room for expansion
    upgrade another LCM line drawer with a data-enhanced bus interface card (DBIC) and relocate this xDSL line card to that drawer
  - use the QXNET VERIFY <site> <frame> <unit> <drawer> command to verify the xDSL line card assignments
- Example 30 uses Format 2. The PM subsystem generates this example when an xDSL line card is added to the LNINV table. The drawer contains more xDSL line cards in a vertical row than the xDSL engineering rules allow. The installed xDSL line card functions as an xDSL line. The whole line drawer is at risk of failure because the drawer is operating beyond the thermal and electrical limits. Operating company personnel receive warning of the xDSL engineering rules breach at the time of the addition. These personnel can perform the following actions to correct the condition:
  - use the QXNET EXPAND<site> <frame> <unit> <drawer> command to locate another row in the same drawer for the xDSL line card
  - use the QXNET EXPANDALL command to locate another LCM that supports xDSL

Format 3 - The following conditions use Format 3:

- Example 10 uses Format 3. This example indicates the detection of a fault on an LIM during any InSv or OOS test. Refer to the MS200 and MS300 series of logs for the possible faults.
- Example 11 uses Format 3. The PM subsystem generates this example when the central control (CC) receives a report from an XPM. This report indicates the detection of a parity fault. The parity fault can be hard, soft or not continuous. If the XPM detects a hard parity fault, the system displays the card that has faults on the card list. Format 3 changes to include the user name and the message `Performed Override of SWACT Controller`. This change occurs when a user overrides the rejection by the switch of activity (SWACT) controller to perform a SWACT. The user assumes all responsibility for XPM SWACT operation when the user overrides the decision of the SWACT controller.
- Example 12 uses Format 3. The PM subsystem generates this example when an XPM diagnostic detects a fault in the echo canceller control card.
- Example 23 uses Format 3. The PM subsystem generates this example when the system detects an F-Bus composite clock fault on the LIM. The log also lists possible cause and possible action. Possible cause indicates all possible causes to the composite clock fault report. Possible action indicates the actions to take to resolve the composite clock fault and the CCS7 outage protection.
- Example 43 uses Format 3. The PM subsystem generates this example when an XPM unit reports a fault report message that is not requested. The XPM unit report this message to the computing module (CM). The log report contains the current degradation level in the XPM unit and a card list of any cards that have faults. The following list is a correct list of status messages that can appear in this occurrence of PM181 log:
  - No degradation of service in unit
  - Minor or potential service degradation in unit
  - Partial service degradation in unit
  - Severe service degradation in unit
- Example 45 uses Format 3. This format is generated when an XPM unit reports an unsolicited fault report message to the computing module (CM). Beginning in XPM09, the log report also identifies the

type of fault and the states in which the faults have been detected. Following is a list of the fault types:

— Fault inferred by maintenance

— Fault detected by diagnostics

— Operational fault

Format 4 - The following conditions use Format 4:

- Examples 13 and 14 use Format 4. The PM subsystem generates these examples when the host sends a request for diagnostics. These examples also occur during a return to service (RTS) with diagnostics permitted.
- Example 15 uses Format 4. This example indicates if the broadcast patching function was successful and if the units passed or failed.
- Example 16 uses Format 4. The PM subsystem generates this example as a result of a PM diagnostic failure or as notification of test completion. The system also generates this log with the new system busy reason of XPM in emergency stand-alone (ESA). This generation occurs when a remote cluster controller (RCC) can return to service after the RCC enters a CC warm or cold restart.
- Example 17 uses Format 4. This example produces a message that indicates unified processor (UP) activity because of signaling processor (SIGP) clock failure or power failure.
- Example 18 uses Format 4. The PM subsystem generates this example when the enhanced ISDN-line concentrating module (LCME) does not load multipoint embedded operations channel (EOC) data from the CC. The LCME returns a failure code to the CC. The system also generates this log when the LCME does not load data from the CC that monitors performance.
- Example 19 uses Format 4. The message field indicates that the firmware name for LOADABLE EEPROM is different from the firmware name for EXECUTABLE EEPROM. During the initialization, an attempt to upgrade the EEPROM with the wrong firmware name can result in failure. This error is the reason for the mismatch.
- Example 20 uses Format 4. The PM subsystem generates this example when a user uses the SWACT Force MAP command to attempt an XPM SWACT. This attempt overrides the rejection of the SWACT controller to perform a SWACT. Format 4 changes with the text string `failed: XPM SWACT Back` to inform the user that a SWACT back occurred. Format 4 also changes to indicate if the aborted SWACT was an override of the SWACT controller. When the system generates this log with this text string, the active unit is

not indicated. The user assumes all responsibility for the XPM SWACT when the user overrides the decision of the SWACT controller.

The system suppresses PM181 log reports in Format 4 that indicate `Static Data Updated/Cleared for the following XPMs that run REX:`

- line trunk controller (LTC), LTC+, ISDN LTC (LTCI)
- line group controller (LGC), LGC+, ISDN LGC (LCDI)
- digital trunk controller (DTC), DTC7, DTC+, ISDN DTC (DTCI)
- remote cluster controller (RCC), RCC+, RCC2
- subscriber carrier module-100S (SMS), SM-100 rural (SMR), SM-100 urban (SMU), and SMS remote (SMSR)
- remote cluster controller (RCC), RCC+, RCC2
- subscriber carrier module-100S (SMS), SM-100 rural (SMR), SM-100 urban (SMU), and SMS remote (SMSR)

Several of the following formats apply to ISDN line drawer for remotes (ILDR). The ILDR is first available for remote switching center-SONET (RSC-S) and remote switching center (RSC) configurations in the NA007/XPM08 timeframe. The ILDR is first available for the following configurations in the NA008/XPM81 timeframe:

- remote line concentrating module (RLCM)
- outside plant module (OPM)
- outside plant access cabinet (OPAC)

Format 5 - The following condition uses Format 5:

- Example 31 uses Format 5. The PM subsystem generates this example when an ISDN line drawer for remotes (ILDR) state changes from InSv to SysB.

Format 6 - The following condition uses Format 6:

- Example 32 uses Format 6. The PM subsystem generates this example when an ILDR changes from InSv to ISTb.

Format 7 - The following condition uses Format 7:

- Example 33 uses Format 7. The PM subsystem generates this example when an ISTb reason is set or deleted (ILDR).

Format 8 - The following condition uses Format 8:

- Example 34 uses Format 8. The PM subsystem generates this example when a switch bank is complete. The system generates this log if the switch bank is successful or not successful.

Format 9 - The following condition uses Format 9:

- Example 35 uses Format 9. The PM subsystem generates this example when an ILDR test fails.

Format 10 - The following condition uses Format 10:

- Example 36 uses Format 10. The PM subsystem generates this example when a file is loaded to the ISDN drawer controller (IDC). The PM subsystem also generates this example when the load attempt fails.

Format 11 - The following conditions use Format 11:

- Examples 37 and 38 use Format 11. The PM subsystem generates these examples when a minimum of one LIS or FBus taps change state. The log indicates the LIS number and the tap number when these numbers apply. This format applies only to an LIM with triple FBus configuration. Tap number range is 0-11.

Format 12 - The following condition uses Format 12:

- Example 39 uses Format 12. The PM subsystem generates this example when the system detects a tap fault. This format applies

only to an LIM with triple FBus configuration. Tap number range is 0-11.

Format 13 - The following condition uses Format 13:

- Example 40 uses Format 13. The PM subsystem generates this example when the system detects a bus fault. This format applies only to an LIM with triple FBus configuration.

Format 14 - The following conditions use Format 14:

- Example 41 uses Format 14. The PM subsystem generates this example when an ILDR enters the congestion state.
- Example 42 uses Format 14. The PM subsystem generates this example when an ILDR exits the congestion state.

Format 15 - The following condition uses Format 15:

- Example 44 uses Format 15 when a load containing MtcArb is present in only one unit. Beginning with CSP09, MtcArb will always be functional by the fact of its being part of the load. The operating company personnel will not be able to disable MtcArb. Therefore, log PM181 will not indicate if MtcArb is functional or disabled.

Format 16 - The following condition uses Format 16:

- Example 46 displays the EEPROM loading process log report in Format 16. One of the F/W loading processes is the erase step. After the erase step finishes, the system displays the log.

Format 17 - The following condition uses Format 17:

- Example 47 displays the recovery failure log report in Format 17. The SXO5 processor card could contain a flash memory (SX06) in one of it's internal slots. When the XPM image dump fails, the system displays the log.

Format 18 - The following condition uses Format 18:

- Example 48 uses Format 18. If the configuration data table (CDT) Audit finds a static data mismatch between the CM and the XPM configuration data, the system sets the XPM to ISTb. In the event of a configuration data manager (CDM) checksum mismatch, the PM subsystem generates a log. The log displays the table and the table ID of the CDT table that failed.

Format 19 - The following condition uses Format 19:

- Example 49 uses Format 19. An RTS of a unit that does not have the hardware associated with the extended messaging feature will fail. A log will be generated.

Format 20 - The following condition uses Format 20:

- Example 50 uses Format 20. If the CC and LCM do not indicate the same current generator for the LCM units, the system generates this example. During a one night process (ONP), the system initializes the CC to the default ring generator of the LCM. If there is a mismatch between the CC and LCM, on NORESTARTSWACT the system updates the CC to match the LCM. This log does not require action.

Format 21 - The following condition uses Format 21:

- Example 51 uses Format 21. The system generates this example in section VCPY (module XPMMASUI) when the configuration data management (CDM) dynamic tuple update fails.

Format 22 - The following condition uses Format 22:

- Example 52 uses Format 22. The system generates this example when the static data download fails.

Format 23 - The following condition uses Format 23:

- Example 53 uses Format 23. The system generates this example when the state of the entry `xpm_supports_dynamic_sd` is false.

Format 24 - The following condition uses Format 24:

- Example 54 uses Format 24. The system generates this example when a reload is finished.

Format 25 - The following condition uses Format 25:

- Example 55 uses Format 25. The system generates this example when the active unit, which is handling call processing, changes. The other unit is in standby mode and is ready to take over activities if there is a problem with the active unit. You can use the CS 2000

GWC Manager to manually change the active unit by performing a warm or cold swact.

Format 25 is also used to report the cause of a GWC autonomous SWACT. If enabled, an autonomous SWACT occurs when the GWC loses communication with all associated media gateways.

Format 26 - The following condition uses Format 26:

- Example 56 uses Format 26. The system generates this example when the Core detects irregular heartbeat messages coming from the GWC. This is likely due to a router problem.

Format 27 - The following condition uses Format 27:

- Example 57 uses Format 27. When a GWC is attempting to return to service and encounters a problem with the return to service sequence, any of the following logs may be seen to indicate a problem. Each log lines up sequentially with an Core side step that must be completed to successfully return a GWC to service. A failure at any one of these steps can cause the GWC to fail to return to service.

Format 28 - The following condition uses Format 28:

- Example 58 uses Format 28. The GWC uses a heartbeat mechanism to detect communication loss between the GWC and the Core. The heartbeat is sent periodically from the GWC to the Core, and is then acknowledged from the Core back to the GWC. This log is printed if a heart beat is not received from the GWC.

Format 29 - The following condition uses Format 29:

- Example 59 uses Format 29. If the heartbeat is not sent consistently then the Core will determine that communication between the Core and GWC has been lost and will create this log. If both units of the GWC suffer a loss of communication, then the Core will also change the Core status of the GWC to SYSB. This will cause all call processing on the Core side to be cleared.

Format 30 - The following condition uses Format 30:

- Example 60 uses Format 30. The GWC uses a heartbeat mechanism to keep the Core informed of its current state. If the Core determines that the recorded state of the GWC node or GWC unit is not the same state as shown in the heartbeat message, then a state mismatch is detected.

Format 31 - The following condition uses Format 31:

- Example 61 uses Format 31. If a state mismatch has been consistently detected, then the Core will take action to resolve the mismatch by synchronizing the GWC and Core states as well as any related call processing. This may involve sending the GWC a message which will cause the GWC to go out of service and then return to service, necessitating a call processing outage.

Format 32 - The following condition uses Format 32:

- Example 62 uses Format 32. There are a few logs that are specific to GWC recovery. These logs are primarily intended to make customers aware of GWCs that are datafilled, but these logs are not associated with the recovery of real hardware. Since this can negatively affect system recovery, the logs are produced so that customers can confirm that datafilled GWCs represent actual working hardware.

Format 33 - The following condition uses Format 33:

- Example 63 uses Format 33. The system generates this example when a GWC unit is in an overload condition. The system continues to output the log every 10 seconds while the GWC unit remains in overload.

Format

This section contains the different formats for log report PM181.

The fields and entries associated with maintenance arbitrator are optional (apply only to XPMs). When a load containing MtcArb is present in both XPM units, the MtcArb state is indicated for each unit as either functional or disabled. In XPM81, when a load containing MtcArb is present in only one of the units, the MtcArb state is indicated for that unit only. The state of the of the second unit is not indicated. Beginning in TL09, MtcArb is always functional and the MtcArb state is not indicated in the logs.

Note: Selected field descriptions for the following log report PM181 formats appear in section Selected field descriptions on page 337

The formats for log report PM181 are as follows:

Format 1

```
PM181 mmmdd hh:mm:ss ssdd INFO
spmid
opttxt
Unit0: MTCARB is <state>, Unit1: MTCARB is <state>
```

Format 2

```
PM181 mmmdd hh:mm:ss ssdd INFO
pmid
Node : statxt
opttxt
```

Format 3

```
PM181 mmmdd hh:mm:ss ssdd INFO
pmid Unit n
Unit0: MTCARB is <state>, Unit1: MTCARB is <state>
TEXT_STRING
Site Flr RPos Bay_id Shf Description Slot EqPec
site nn cn ccc 00 nn type :no :nn pec_id
```

Format 4

```
PM181 mmmdd hh:mm:ss ssdd INFO
pmid Unit n
Node: statxt, Unit0 actxt: statxt1, opttxt0 Unit1 actxt: stat
opttxt
Unit0: MTCARB is <state>, Unit1: MTCARB is <state>
```

Format 5

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
Node: <state>, Unit0: <state>, Unit1: <state>
Drawer <drawer>: <state> from <state>
Reason: <SysB_reason>
```

Format 6

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
Node: <state>, Unit0: <state>, Unit1: <state>
Drawer <drawer>: <state> from <state>
Reason: <SysB_reason>
```

Format 7

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
Node: <state>, Unit0: <state>, Unit1: <state>
Drawer <drawer>: <state>
Reason: <ISTb_reason>
(<Set/Delete>) <ISTb_reason>
```

Format 8

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
Node: <state>, Unit0: <state>, Unit1: <state>
Drawer <drawer>: ILD <C/W> switch bank <S/F> (<S/M> action).
Reason: <Switch_Bank_Failure_reason>
```

Note: In Format 8, the log report displays the “Reason” only when the switch bank fails.

Format 9

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
Node: <state>, Unit0: <state>, Unit1: <state>
Drawer <drawer>: Test <C/F>
Reason: <Test_Failure_reason>
```

Format 10

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
Node: <state>, Unit0: <state>, Unit1: <state>
ILD <drawer>
IDC bank <bank_no> load <load_result> from <srctxt> Load file:
<load_file>
Failure reason: <reasontxt>
ILD <drawer>
IDC bank <bank_no> load <load_result> from <srctxt> Load file:
<load_file>
Failure reason: <reasontxt>
```

Note 1: Format 10 applies to loading all ILDRs in the LCM. When loading a given ILDR, the log report shows only the results for that IDC.

Note 2: In format 10, the log report displays the “Failure reason” only if the loading fails.

Format 11

```
<node><Alarm_ind>PM181 mmmdd hh:mm:ss seqnbr INFO
LIM <LIM_number>
LIS <LIS_number>
FBus <FBus_number>
<Tap_header> <Tap_number>
From: <from_s>
To: <to_s> : <Tap_header> <Tap_number>
```

Note: Format 11 applies only to an LIM in the triple FBus configuration.

Format 12

```
<node><Alarm_ind>PM181 mmmdd hh:mm:ss seqnbr INFO
LIM <LIM_number>
LIS <LIS_number>
FBus <FBus_number>
<Tap_header> <Tap_number>

Service affecting faults. CODE: <Fault_code>
```

Note: Format 12 applies only to an LIM in the triple FBus configuration.

Format 13

```
<node><Alarm_ind>PM181 mmmdd hh:mm:ss seqnbr INFO
LIM <LIM_number>
LIS <LIS_number>
FBus <FBus_number>
<Tap_header> <Tap_number>

Fault found against LIS <LIS_number> (Shelf Pos <shelf_positic
```

Note: Format 13 applies only to an LIM in the triple FBus configuration.

Format 14

```
PM181 mmmdd hh:mm:ss ssdd INFO
LCM <site> <frame> <unit>
<text>
```

Format 15

```
PM181 mmmdd hh:mm:ss ssdd INFO
pmid
opttxt
Unit n: MTCARB is <state>
```

Format 16

```
PM181 mmmdd hh:mm:ss log no INFO PM no Unit no
Node: <state>, Unit n : <state>, Unit n : <state>
<string1>
```

Format 17

```
PM181 mmmdd hh:mm:ss ssdd INFO
Node: <state>, Unit n : <state>, Unit n : <state>
<string 1>
<string 2>
```

Format 18

```
PM181 mmmdd hh:mm:ss ssdd INFO pmid
Node: statxt, Unit0 actxt: statxt1, Unit1 actxt: statxt1
<ISTb_reason>: <TBL> <(tab_id)>
```

Format 19

```
PM181 mmmdd hh:mm:ss ssdd INFO pmid Unit <n>:actxt
Node: statxt, Unit0 actxt: statxt1, Unit1 actxt: statxt1
<Switch Bank Failure Reason>: Reason: <SysB_reason>
```

Format 20

```
PM181 mmmdd hh:mm:ss ssdd INFO LCM <site> <frame> <unit> Unit
Node: <state>, Unit0 : <state>, Unit1 : <state>
RGI Mismatch
```

Format 21

```
PM181 mmmdd hh:mm:ss ssdd INFO pmid Unit<n>:actxt
Node: <statxt>, Unit0 actxt: statxt1, Unit1 actxt: statxt1
Dynamic Tuple update failed tabID: <table ID) (Reason:
<Dynamic_Download_Failure_Reason>)
```

Format 22

```
PM181 <mmmdd> hh:mm:ss ssdd INFO <PM no.>
Node: <state> UNIT : <state> UNIT : <state>
<string l>
```

Format 23

```
PM181 <mmmdd> hh:mm:ss ssdd INFO pmid
Node: statxt, Unit0 actxt: statxt Unit1 actxt: statxt
<Reason>
```

Format 24

```
PM181 <mmmdd> hh:mm:ss ssd INFO pmid
PMTYPE loaded with LOADFILE, Elaspsed time: mm: ss
```

Format 25

```
<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC#> <Unit #>
   GWC activity gained.

<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC#> <Unit #>
   GWC activity dropped.
```

Note: Format 25 is outputted as a no alarm info log.

Format 26

```
<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC#> <Unit #>
   Unexpected heartbeat flooding (<Flood Count>)
```

Note: Format 26 is outputted as a no alarm info log.

Format 27

```
<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC #><Unit#>
   <Return to service step being performed> failed
   <Reason for failure>
```

Format 28

```
<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC #><Unit#>
    Detecting communication loss between core and GWC
```

Format 29

```
<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC #><Unit#>
   Communication loss between core and GWC has been confirmed
```

Format 30

```
<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC #><Unit#>
    A GWC state discrepancy has been detected
    CM recorded state: <State> <Activity>
    GWC reporting state: <State> <Activity>
```

Format 31

```
<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC #><Unit#>
    The GWC state discrepancy is being resolved
    CM recorded state: <State> <Activity>
    GWC reporting state: <State> <Activity>
```

Format 32

```
<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC #><Unit#>
    GWC node timed out on recovery.
    Ensure datafilled GWC is communicating with the core.
```

Format 33

```
<Clli> PM181 <Date> <Time> <Sequence #> INFO <GWC #> <Unit #>
: <Activity>
    Unit is in an overload condition.
```

Selected field descriptions

The following table explains selected fields in the different log report formats:

Field	Value	Description
actxt	Act	Identifies the activity state of the PM unit as active (Act).
	Inact	Identifies the activity state of the PM unit as inactive (Inact).
alarm		Optional field. Indicates the type of alarm that accompanied the change of state.
	***	Indicates a critical alarm.
	**	Indicates a major alarm.
	*	Indicates a minor alarm.
	(blank)	Indicates no alarm.
bank_no	0 or 1	Indicates the bank number loaded.
C/F	completed or failed	Indicates the test result. The “Reason” line is populated only in the case of a failed result.
C/W	cold or warm	Indicates a cold or warm switch bank.
Dynamic_Download_Failure_reason	tblnacktimeout Wrong Message, UNIT OOS, or unknown	Indicates why dynamic tuple download failed.
drawer	0 through 19	Indicates the drawer number.
ISTb_reason	Incoming message overloaded One DMSX channel is unavailable Load name mismatch CDT Chksm mismatch Noncritical in-service test failed One or both Bd-channels are out of service Load in progress Invalid load file or Overload	Indicates the reason for the ISTb state.
load_result	succeeded or failed	Indicates if the load succeeded or failed. The log format changes according to this field.

Field	Value	Description
<link_mtc_action>	RTS Request ManB Request SysB Request Mtce Open Request Close Request Test Request or Abort Request	Indicates the maintenance action request made to link maintenance.
link_mtc_result	Failed to close link Fault found on link Failed to open link Failed to mtce open link or Failed to test link	Indicates the result of the maintenance action request sent to link maintenance.
<m>	6 to 21	Indicates the MS card.
opttxt	Character string	Optional field. Provides additional information to help software troubleshooting technicians isolate problems.
opttxt0	Character string (8x46) (swacting) (XPM in ESA)	Optional field. Provides additional information to help software troubleshooting technicians isolate trouble. Indicates that the NT8X46 card on unit 0 failed pulse code modulation (PCM) or signaling tests. Indicates that unit 0 is switching activity in response to a SWACT Force MAP command. This action overrides the rejection by the SWACT controller to switch activity. Indicates that unit 0 became SysB because of an XPM in ESA mode.

Field	Value	Description
opttxt1	Character string (8x46) (swacting) (XPM in ESA)	Optional field. Provides additional information to help software troubleshooting technicians isolate trouble. Indicates that the NT8X46 card on unit 1 failed PCM or signaling tests. Indicates that unit 1 is switching activity in response to a SWACT Force MAP command. This switch overrides the rejection by the SWACT controller to switch activity. Indicates that unit 1 is switching activity in response to a SWACT Force MAP command. This switch overrides the rejection by the SWACT controller to switch activity.
pmid	alphanumeric	Indicates the PM affected. **Note:** A change of state in the F-bus taps in an LIM can generate PM181. In this condition, the pmid field appears in the form: LIM nn FBus n TAP. The subfield “FBus n Tap” indicates the specific F-bus tap responsible.
reasontxt	Illegal S-record File incorrect Fail to erase bank Bad checksum Task aborted while loading Invalid load address Failed to write the record Sequence number error Fail to send query message Fail to load mate bank Fail to get route or Fail to establish connection	Indicates the reason for the failure.
S/F	succeeded or failed	Indicates the switch bank result. The “Reason” line is populated only in the case of a failed result.
S/M	system or manual	Indicates the action originator.
Set/Delete	set or deleted	Indicates if the reason for the ISTb is a new reason (Set) or if a reason was cleared (Deleted).

Field	Value	Description
Switch_Bank_Failure_reason	No reply from ILD Active bank not changed Invalid load Bsy failed or RTS failed	Indicates the reason for the switch bank failure.
SysB_reason	Incoming message overload Critical in-service test failed No response from ILD Active bank mismatch Call process activity mismatch LCM activity mismatch Unsolicited message limit exceeded S/W error message limit exceeded WAI received Cold switch bank in progress CC restart has occurred C-side node RTSILDR Bus interface card (BIC) loop failure Fault message received from ILD or Extended Messaging Hardware Mismatch	Indicates the reason for the SysB state.
state	functional or disabled	Indicates the state of MtcArb in the XPM unit at the time the log is formatted for display. This state can differ from the state of the log at the time the system generated the log. The possibility of this difference increases as the time between log generation and log formatting increases.

Field	Value	Description
statxt	InSv, ISTb, Cbsy, SysB, and ManB username: <userid> Performed Override of SWACT Controller username: <userid> Performed a BSY PM FROM: <state> (sq) TO: <statxt> (sq) TAP: <tap_number_set> Diag Failed: <TTTTTT> <CCCCCCn> <reason text> Loading of mp-eoc data failed Loading of Performance Monitoring Data Failed	Defines the current state of the PM node. Examples are: C-side busy (Cbsy), system busy (SysB), manual busy (ManB).
statxt1	ManB, InSv, ISTb, Cbsy, OffL, UnEq, SysB	Defines the current state of the PM unit. Off-line (OffL) is an example.
TBL	character string	Indicates the name of the table.
TEXT_STRING	Character string	Indicates the type of fault detected in the XPM. Beginning in XPM09, this field also indicates the states in which the faults were detected and how the faults were detected. This value is followed by a card list if the log indicates a hard fault. See the Parity audit faults table in the “Additional information” section of this log report. See the *Peripheral Modules Maintenance Guide* (Circuit location display) for details about the card list format.

Field	Value	Description
Test_Failure_reason	Flash memory bank Sanity timeout Active bank: Checksum Inactive bank: Checksum Timing MatrixB53 Application-specific integrated circuit (ASIC) 100VU-loop power supply or No reply from ILD	Indicates the reason for the switch bank failure.
tab_id	alphanumeric	Indicates the table identification number.
Unit n	0 or 1	Identifies the PM unit that generates the report. If the PM that generates the report is an ESA, there is no unit specified. When MtcArb is loaded in only one PM unit, this value identifies that unit.
Unit 0: MTCARB is	constant	Indicates that the current state of the maintenance arbitrator in XPM unit 0 follows. This field is optional and applies only to digital trunk controllers (DTC), line trunk controllers (LTC) and line group controllers (LGC). If the XPM maintenance arbitrator is not loaded in the unit, the field is blank. Beginning in TL09, this field is not present.
Unit 1: MTCARB is	constant	Indicates the current state of the maintenance arbitrator in XPM unit 1 follows. This field is optional and applies only to DTCs, LTCs, and LGCs. If the XPM maintenance arbitrator is not loaded in the unit, the field is blank. Beginning in TL09, this field is not present.

Action

This section describes additional action you can take to resolve problems indicated in the log report.

Take action as the report specifies. If you cannot resolve the problem, save all reports generated during the 5 min before the system generated PM181. Contact the next level of maintenance.

The following table suggests actions to take in response to the different failure conditions associated with log report PM181:

Actions for log report PM181 (Sheet 1 of 10)

Problem	Additional information	Action
Loading the IPE fails.	See log format 2, examples 7, 8, and 9.	Maintenance may be required. Contact the next level of maintenance.
PM nodes fail the patching function.	See log format 4, example 15.	Modify the nodeset (or create a new nodeset) that includes the failed units. Try to remove or apply the patch again
Failure involving an SPX.	See log format 1, example 26.	Perform fault diagnostics on the SPX. Access the SPX through the console port at the DMS ServiceBuilder LAN-BAY.
Failure involving an integrated digital terminal (IDT).	The IDT becomes ManB.	Take the correct maintenance steps. If the problem persists, contact the next level of support. A time-out can occur while the CC maintenance task waits for the busy request reply from the subscriber carrier module-100 access (SMA). If a time-out occurs, check the status of the SMA, the IDT, and the P-side message DS-1 links at the MAP display. If the SMA responds that the busy request failed, refer to log reports for additional information.

Actions for log report PM181 (Sheet 2 of 10)

Problem	Additional information	Action
Parity audit fault.	See log format 3, example 11.	Refer to the Parity audit faults table at the end of this log. The table contains information on the correct action to take.
XPM diagnostic detects a fault in the echo canceller control card.	See log format 3, example 12.	Replace the card.
XPM facility audit detects a state change in an echo canceller module.	See log format 1, example 5.	Replace the echo canceller module that has faults. Check the buses that connect the ring generator to the units.
A line card that has faults overloads the ring generator.	Log report PM179 is the current report for ring generator overload.	Determine the line card that causes the fault. Remove the cards and test the drawer that faults to check for the card that has faults. The test passes when more than one line card that has faults is installed. With all line cards unseated, test the drawer to clear the fault. Next, reseat the cards one at a time. The LCM sends a message that is not requested. This message reports the ring generator overload when you reseat the card that has faults. Remove the known card that has faults and replace the card.
ASU attempts SYSB recovery (autoloading of an ASU).	An error occurs if a mismatch between the processor card and the loadsize causes the loading to fail. The load continues to fail autoload until the load is compatible with the process size.	No action indicated.
Ring generator overload (that a line card that has faults does not cause).	None.	Replace the ring generator that has faults.

Actions for log report PM181 (Sheet 3 of 10)

Problem	Additional information	Action
The opttxt field indicates that the firmware name of the loadable EEPROM is different from that of the executable EEPROM.	See log format 4, example 19. In this condition, the action fails because the system cannot upgrade the EEPROM with the wrong firmware name.	Load the firmware to the EEPROM. If the log appears again, replace the card.
The opttxt field indicates that the unit is in ROMlevel.	None.	Perform the command PMRESET. If this command does not work, load the unit again and perform an RTS. After you perform the RTS, load the firmware to the EEPROM again.
The opttxt field indicates the programming was not successful.	The programming failed because of time-out open route.	Perform the LOADPM command again.
The opttxt field indicates that the query was not successful.	None.	Perform the LOADPM command again. If the system generates same log message is after you reissue the LOADPM command, replace the card.
The number of erases that erased more than one time is close to 3000, and the time of the load process increases.	None.	Replace the EEPROM in the unit with a newer one because the EEPROM is old.
The opttxt field indicates that the programming was not successful because of a file name that was not correct.	In this condition, the loadfile in the inventory table is not correct.	Change the file name in the inventory table.
The opttxt field indicates that the programming was not successful because of flags that were not correct.	In this condition, the loadfile in the inventory table is not correct.	Return the unit to service to upgrade the erased EEPROM. Change the firmware file that includes correct flags. Replace the loadfile.

Actions for log report PM181 (Sheet 4 of 10)

Problem	Additional information	Action
The opttxt field indicates that the programming was not successful because burning action failed.	None.	In this condition, issue the LOADPM command again. If the system generates the same log message after you reissue the LOADPM command, replace the EEPROM. If the system generates the same log message after the reissue, replace the card.
The opttxt field indicates that the programming was not successful because of address overlap.	The loadfile in the inventory table is not correct.	Change the file name in the inventory table.
The opttxt field indicates that the programming was not successful because of an S-record that was not legal.	The loadfile in the inventory table is not correct.	Change the file name in the inventory table.
The opttxt field indicates that the programming was not successful because of address range error.	The loadfile in the inventory table is not correct.	Change the file name in the inventory table.
The opttxt field indicates that the checksum of the EEPROM failed.	None.	Perform the LOADPM command again. If the system generates the same log, change the file name in the inventory table.
The opttxt field indicates that the switching action between the two EEPROMs failed.	None.	Perform the LOADPM command. If the system generates the same log again, replace the card.

Actions for log report PM181 (Sheet 5 of 10)

Problem	Additional information	Action
The opttxt field indicates that the ROM diagnostics failed.	None.	Perform the LOADPM command. If the system generates the same log, replace the card.
The opttxt field indicates that the running on the EEPROM that executes was not successful.	None.	Check for additional log messages and load the unit again with the previous firmware. Load the firmware to the EEPROM. If the log appears again, replace the card.
The opttxt field indicates one of the following: • `LCM REX test has not been performed on this node for nn days.` • `LCMCOV REX test has not been performed on this node for nn days.`	None.	The operating-company technician can determine why the test was not performed on the specified LCM. The TST REX OFF or TST COVREX OFF commands can cause the system to disable REX testing on the LCM. These commands are at the LCM level of the MAP display. The technician should make the correct entry changes to enable REX testing for the LCM.
The opttxt field indicates `LCM REX TEST PASSED or LCMCOV REX TEST PASSED.`	None.	No action required.
An NT8X46 card fails a PCM or signaling test.	A card that has faults affects voice and data calls until you replace the card.	Follow resolution recommendations in the PCM/Signaling test failures table. Refer to *Meridian SL-100 Digital Line Module Reference Manual* for additional information on the NT8X46 card.

Actions for log report PM181 (Sheet 6 of 10)

Problem	Additional information	Action
The system generates this log as a result of an override of the decision of the SWACT controller.	See log format 3, example 11. The system generates this log to inform the user that a SWACT back occurred. This log also informs the user if the SWACT back was an override of the decision of the SWACT controller. The system also generates this log to identify the user with the responsibility for the SWACT.	This condition does not require immediate action.
The state of the ILDR changes to ISTb, SysB, or switch bank failure.	See the following: • log format 5, example 31 • log format 6, example 32 • log format 8, example 34	Proceed according to the failure reason. If none of these changes are the reason, there is no action required.
The ILDR load operation fails.	None.	Check the reason for the failure and proceed as required. Notes: • If you correctly load the ILDR file, there is no action required • If the ILDR load operation fails, check the reason for the failure and proceed as required. • There is no action required if ILDR enters or exits the congestion state.

Actions for log report PM181 (Sheet 7 of 10)

Problem	Additional information	Action
The XPM maintenance arbitrator (MtcArb) diagnostic detects a card that has faults in the XPM unit.	None.	Replace the card.
RTS fails because of an Extended Messaging Hardware Mismatch	None.	Install the appropriate circuit packs to support extended messaging.
The CDT Audit detects a CDT Chksm Mismatch.	The log identifies the mismatched CDM table. The system sets the peripheral to ISTb. See log format 16, example 48.	To clear the ISTb, busy (BSY) and return the peripheral to service (RTS). This action sends a static data download to the PM and corrects the static data mismatch in the CDM table.
The system indicates `Could not configure NETPROT for unit 1 occurs`, reload static data.	None.	Use the LOADPM command to reload static data in the unit identified in the log (for example, LOADPM UNIT 1 CC DATA).
If the flag `xpm_supports_dynamic_sd` is false.	The 1 minute audit sets the boolean to 'True' and generates a log indicating the same.	No action required.
Log format 26, example 56.	None.	Contact Nortel Networks customer support.

Actions for log report PM181 (Sheet 8 of 10)

Problem	Additional information	Action
Log format 27, example 57.	There are many possible failure reasons that may be printed and, as a result, not all of them can be listed here. The failure reason will give some specific information to indicate the cause of the failure. The most common failure reason is "`NO reply from PM`" as shown in the example log. If this failure reason is given, then the communication path between the Core and the GWC is probably faulty. Most commonly, recently datafilled GWCs may encounter this problem due to one of the following: • the SRVRADDR IP address is incorrect in table SRVRINV on the Core • the CS IP number or node number is incorrect on the GWC.	If the reason is "`NO reply from PM`" then verify that the GWC is datafilled correctly and that the ethernet links and Passport 8600 are connected and working properly.
Log format 28, example 58.	A number of reasons can cause the heartbeat to be missed: • A packet could have been intermittently lost. • There could be a problem with the GWC such that it is not sending a heartbeat message. • The communication link between the GWC and Core could be broken.	If the log is printed only once then there was likely just an intermittent packet loss in the network and no action is required If the log is printed periodically then there is likely a problem with the network path between the GWC and the Core and packets are being dropped periodically. In this case the network should be examined to reduce packet loss.

Actions for log report PM181 (Sheet 9 of 10)

Problem	Additional information	Action
Log format 29, example 59.	The GWC may have stopped sending heartbeat messages without notifying the Core that it is going out of service. This may occur if the GWC is re-booted without first being taken out of service, or if an autonomous restart occurs due to sever failures on the GWC.	If the GWC is in service at the time these logs are printed, then there is likely a network fault and the network should be examined to locate the broken communication path.
Log format 30, example 60.	A state mismatch could occur if a state transition message sent from the GWC to the Core is lost. This log report is not common and should rarely be seen.	A transient log seen once is of no concern. If these logs are seen periodically then there may be an internal software problem. There may be a problem with the network if communication loss logs are also seen.
Log format 31, example 61.	A state mismatch has occurred consistently. The Core will resolve the mismatch automatically.	The circumstances surrounding the mismatch should be investigated by the design group. Please contact Nortel Networks customer support if this log is seen.
Log format 32, example 62.	The active GWC unit failed to respond within 30 seconds of receiving notification of an Core restart. Therefore, the Core recovery of the GWC node has timed out.	Check the GWC to ensure it is functioning correctly. If the datafilled GWC does not represent actual GWC hardware, then the tuple should be deleted from table SERVRINV.

Actions for log report PM181 (Sheet 10 of 10)

Problem	Additional information	Action
Log format 33, example 63.	None.	No action is required; this log is for information only.
Log format 25, reason: "no GW communication"	The GWC performed an autonomous SWACT due to loss of communication with all associated media gateways.	This log indicates a problem in the network. Use the related network component managers to identify the root cause.

Associated OM registers

This log report has associated OM register XPMOVLD.

Note: The OM register applies only when log PM181 reports GWC overload.

Additional information

Host-requested diagnostics

The following table provides failure reasons for host-requested diagnostics.

Host-requested diagnostics - failure reasons (Sheet 1 of 2)

Failure reason	Explanation
CMR NT6X78AA OOS CMR Diagnostic Fail	Indicates the class modem resource card is out-of-service. This failure implies that the calling number delivery feature does not work for terminating lines on that peripheral.
Test Failed: CTRDIAG	Indicates the detection of an operational fault on the CX10. Call progress tone receiver (CTR) configured in the specified test access controller XPM (TAC) is not available for call progress tone reception.
Test Failed: CPADIAG	Indicates the detection of an operational fault on the CX09. Class protocol analyzer (CPA) configured in the specified TAC is not available for class message reception.
Diagnostic TestAll passed.	Indicates diagnostics ran and did not find faults.

Host-requested diagnostics - failure reasons (Sheet 2 of 2)

Failure reason	Explanation
Diagnostic TestAll failed.	Indicates the diagnostic failed but was not able to generate a card list.
Diagnostic TestAll failed, CardList: nXnn, nXnn	Indicates the diagnostic failed the cards listed in the card list. Table ROM test failures provide the text strings that reflect the failure of ROM tests run on the NT6X51AB board. Refer to the end of the log for the Table ROM test failures.
Diagnostic TestAll failed, Invalid Static Data.	Indicates the diagnostic failed because the requested diagnostics require static data in the peripheral module.
Diagnostic TestAll failed, a resource was unavailable	Indicates the request to run a diagnostic. The diagnostic system in the PM was not able to allocate all the resources that the diagnostic required.
Diagnostic TestAll was not run.	Indicates that for some reason, the diagnostic system in the PM was not able to run the requested diagnostic.
Diagnostic TestAll failed, PP has an invalid load.	Indicates the diagnostic system did not run the diagnostic because this system has a temporary overload.
Diagnostic TestAll not run, Diagnostic system is in overload	Indicates the diagnostic system did not run the diagnostic because this system has a temporary overload.
Software error in Diagnostic TestAll	Indicates the diagnostic system encountered a software error. The error occurred when the system tried to run the requested diagnostics.
Diagnostic Test All not present in PP load.	Indicates the requested diagnostic is not present in that given peripheral module.
Diagnostic TestAll - unknown return code.	Indicates the diagnostic system returned a reply to the host that the host cannot process.

The following table provides maintenance action explanations for host-requested diagnostics.

Host-requested diagnostics - maintenance actions

Maintenance action	Explanation
(Blank)	There is no action required.
Reload this unit	
BSY and RTS this unit.	
Diagnose this unit.	The audits in the PM discovered a fault. Use the TST command from the MAP display to isolate the fault in this unit.
Try diagnostics again later.	
Watch for and report PM180 logs.	The diagnostics can have triggered some PM180 logs. Record these PM180 logs on any problem report.
Replace cards on card list.	The card list presents cards in order of the most probable cause of the failure. Replace each card in order, testing with each replacement until a replacement clears the fault.
Report this log to your field support division.	A C-side peripheral module is the most probable cause of the failure. The most possible state for this module is a system busy state. Perform the BSY and RTS commands on the peripheral module identified in the text section of the log.
BSY and RTS C-Side PP LCM REMn n n	
Diagnose C-Side PP LCM REMn n n	A fault isolation in the PM determined the fault lies in the C-side peripheral. Perform the POST and TST commands on the peripheral identified in the log text.
Diagnose C-Side links:	Post the C-side peripheral of this unit and diagnose the P-side links of that peripheral module.
Reload Static Data:	Use the LOADPM command to reload static data in the unit identified in the log (for example, LOADPM UNIT 1 CC DATA).

DMPC faults

The format of the text string (opttxt) for digital port maintenance card (DMPC) faults is as follows:

Diag Failed: DPMC Fault - <fault reason>

The following table lists DPMC faults and actions.

DPMC faults and actions

DPMC fault reason	Action
Card Not Present	Insert a DPMC card completely in the DLM shelf in slot 13 or change customer data in table DLMINV. Change this data to indicate that the DLM is not equipped with a DPMC.
Card Not Accessible	The card was in use during the test. Start InSv tests on one of the units of the DLM to test the DPMC again.
Control Logic Defective	Replace the DPMC.
Relay Drivers Defective	Replace the DPMC.
Facility Sensors Defective	Replace the DPMC.
DSIC 30V Measurement Circuit Defective	Replace the DPMC.
Loop Voltage Sensor Defective	Replace the DPMC.
30V Source Defective	Replace the DPMC.
Defective DSIC Emulation Circuit	Replace the DPMC.
Prime DSIC 10V Measurement Circuit Defective	Replace the DPMC.
Mate DSIC 10V Measurement Circuit Defective	Replace the DPMC.

RLCM/RDLM-ESA messages

The following table provides RLCM/RDLM-ESA log messages and actions.

RLCM/RDLM-ESA messages and actions

RLCM/RDLM-ESA message	Explanation	Action
PM in ESA, communication restored, ready to be returned to service	The RLCM/RDLM runs in ESA and the office parameter RLCM_XPMESAEXIT is set to 0. This condition means that the system will issue a warning log for every audit cycle.	Manually return the RLCM/RDLM to service when problems with the links of the RLCM/RDLMs links are resolved.
ESAExit failed, Reason: no reply from PM	Indicates that the RLCM/RDLM did not perform a successful exit from the ESA	For information only.
LCM unit inhibiting ESA. Return to service or reload this PM.	The CC found an LCM unit that requests ESA while the LCM is InSv. The possible cause is a defective exit or an ESA REX test.	Busy and return the unit to service to clear the problem. If this action does not work, reload the unit from the mate and return the unit to service.
DLM unit inhibiting ESA. Return to service or reload this	The CC found a DLM unit that requests ESA while the DLM is InSv. The possible cause is a defective exit or an ESA REX test.	Busy and return the unit to service to clear the problem. If this action does not work, reload the unit from the mate and return the unit to service.
DLM unit inhibiting ESA. Return to service or reload this PM.	The CC found a DLM unit that requests ESA while the DLM is InSv. The possible cause is a defective exit or an ESA REX Test.	Busy and return the unit to service to clear the problem. If this action does not work, reload the unit from the mate and return the unit to service.

EIU failure messages

The following table lists EIU failure messages and actions.

EIU failure messages and actions (Sheet 1 of 4)

EIU failure message	Additional information	Action
ISTb condition	Indicates the EIU detects the following errors on the LAN: • rx framing errors • rx overflow errors • rx CRC errors • tx deferred errors • loss of carrier errors • late collision errors • retries exceeded errors	Perform external diagnostics. Retain all reports generated 5 min before and 5 min after this report and contact the next level of maintenance.
ISTb condition - lack of buftype	Indicates one of the following buffers caused the EIU to overload: • rx sw buffers • tx hw buffers	Retain all reports generated 5 min before and 5 min after this report and contact the next level of support.
In-service Test Failure Card: <cardtxt> < failure id>	Indicated a test failure occurred. Subfield cardtxt identifies the card. Subfield failure id indicates one of the following messages:	Follow the procedures as indicated for each failure id.
	EIC CARD LOCATE TEST	Verify that the product engineering code (PEC) of the card in the slot is a valid Ethernet interface card (EIC) PEC. Run the test again.
	EIP CARD LOCATE TEST	Verify that the Ethernet interface paddle board (EIP) card is in the correct shelf and slot. Run the test again.

EIU failure messages and actions (Sheet 2 of 4)

EIU failure message	Additional information	Action
	EIP CARD ID PROM TEST	Verify that the PEC of the paddle board in the EIP shelf and slot is a valid EIP PEC. Run the test again.
	EIC CARD TEST	Replace the EIC for the specified EIU and run the test again.
	EIP CARD TEST	Replace the EIP card for the specified EIU and run the test again.
	EIC AND EIP CARD TEST	Replace the EIC for the specified EIU and run the test again. If the second test fails for the same reason, replace the EIP card and run the test again.
	EIP AND EIC CARD TEST	Replace the EIP card for the specified EIU and run the test again. If the second test fails for the same reason, replace the EIC and run the test again.
Operation Affecting Fault: faultxt	Indicates the fault encountered affects the operation. One of the following messages generates:	Refer to the fault messages for any possible action to take.

EIU failure messages and actions (Sheet 3 of 4)

EIU failure message	Additional information	Action
	Local EIU mtce software error: rsntxt. Field rsntxt consists of one of the following messages: • Inconsistent local mtce state • Unexpected msg from EICM • Bad parms for EICM command • EICM in illegal state for command	The system automatically places the EIU in a system busy state. Save this report and all other reports generated in the past 5 min. Contact the next level of support.
	EIC mtce software error	The system automatically places the EIU in a system busy state. Save this report and all other reports generated in the past 5 min. Contact the next level of maintenance.
	• Excessive spurious interrupts • EIC card failure	The system automatically places the EIU in a system busy state. Save this report and all other reports generated in the past 5 min. Contact the next level of support.
	EIU fault: <rsntxt> - Subfield “rsntxt” consists of one of the following messages:	Refer to the correct reason for any possible action to take.
	Enable failed - EIC card not found	Verify that the EIC card is in the correct shelf and slot. Attempt to return the EIU to service.
	Enable failed - EIC PEC mismatch	Verify that the PEC of the card in the EIC shelf and slot is a valid EIC PEC. Return the EIU to service.

EIU failure messages and actions (Sheet 4 of 4)

EIU failure message	Additional information	Action
	Enable failed - EIP card not found	Verify that the EIP card is in the correct shelf and slot. Return the EIU to service.
	Enable failed - EIP PEC mismatch	Verify that the PEC of the card in the EIP shelf and slot is a valid EIP PEC. Return the EIU to service.
	Enable failed - EIC card failure	Replace the EIC card for the specified EIU. Return the EIU to service.
	Enable failed - EIP card failure	Replace the EIP card for the specified EIU. Return the EIU to service.
	Enable failed - EIC and EIP cards failed (EIC most probable)	Replace the EIC card for the specified EIU. Try to return the EIU to service. If the second attempt fails for the same reason, replace the EIP card. Return the EIU to service.
	Enable failed - EIP and EIC cards failed (EIP most probable)	Replace the EIP card for the specified EIU and return the EIU to service. If the second attempt fails for the same reason, replace the EIC card. Return the EIU to service.

NT8X46 PCM/signaling test failure

The following table lists NT8X46 PCM/signaling test failure messages and actions.

NT8X46 PCM/signaling test failure messages and actions

NT8X46 PCM/signaling test failure message	Action
For the following messages: • Unit 0 failed PCM testing. • Unit 0 failed signaling tests. • Unit 0 failed PCM and signaling tests.	If unit 1 is already in a SysB state, unit 0 becomes ISTb. Replace the NT8X46 card in unit 0 as soon as possible. If unit 1 is in an InSv state, unit 0 becomes SysB. Run an InSv test on unit 1. If unit 1 passes and all data packet controllers (DPC) remain InSv, replace the NT8X46 card for unit 0. If any DPCs become SysB during the unit 1 InSv testing, the unit 0 NT8X46 card can be safe. Replace the NT8X47 cards associated with the DPCs that are SysB. Return those cards to service and return to service unit 0. If unit 0 stays in service, the NT8X47 cards are defective and unit 0 NT8X46 card works. If unit 0 becomes SysB again, and the NT8X46 reports the same failure, replace the unit 0 NT8X46 card.
For the following messages: • Unit 1 failed PCM testing. • Unit 1 failed signaling tests. • Unit 1 failed PCM and signaling tests.	If unit 0 is already in a SysB state, the state of unit 1 becomes ISTb. Replace the NT8X46 card in unit 1 as soon as possible. If unit 0 is in an InSv state, the state of unit 1 becomes SysB. Run an InSv test on unit 0. If unit 0 passes and all DPCs remain in service, replace the NT8X46 card for unit 1. If any DPCs become SysB during the unit 0 in service testing, the unit 1 NT8X46 card can be working. Replace the NT8X47 cards associated with the DPCs that are SysB. Return those cards to service and return unit 1 to service. If unit 1 stays in service, the NT8X47 cards are defective. The unit 1 NT8X46 card works. If unit 1 becomes SysB again, and the NT8X46 reports the same failure, replace the unit 1 NT8X46 card.

ESA failure

The following table lists emergency stand-alone (ESA) failure messages and actions.

ESA failure messages and actions (Sheet 1 of 2)

ESA failure message	Additional information	Action
Preparation Failure: LCMREMn nn n Unit n failed to enter ESA	One of the C-side LCM units failed to enter ESA when the software requested this action.	Check the state of the LCM unit. If SysB, attempt to RTS the LCM unit.
Preparation Failure: DLMREMn nn n Unit n failed to enter ESA	One of the C-side DLM units failed to enter ESA when the software requested this action.	Check the state of the DLM unit. If SysB, attempt to return the DLM unit to service.
ESA REX preparation Failure: LCM REMn nn n Unit n failed to enter ESA	Maintenance already started on the LCM when the REX test was requested. This maintenance on the LCM prevents the entry of the LCM unit into the ESA and aborts the REX test.	There is no action required.
ESA REX preparation Failure: DLM REMn nn n Unit n failed to enter ESA	Maintenance already started on the DLM when the REX test was requested. This maintenance on the DLM prevents the entry of the DLM unit into the ESA and aborts the REX test.	There is no action required.
Test Failure: LCM REMn nn n Unit n failed to exit ESA	The ESA software placed a unit of the LCM in ESA. The system used this unit to run the REX test. When the test was complete, the LCM unit failed to return to service. This failure caused the REX test to abort. (A no resources message normally accompanies this occurrence at the MAP display.)	Attempt to RTS the LCM unit.

ESA failure messages and actions (Sheet 2 of 2)

ESA failure message	Additional information	Action
Test Failure: DLM REMn nn n Unit n failed to exit ESA	The ESA software placed a unit of the DLM in ESA. The system used this unit to run the REX test. When the test was complete, the DLM unit failed to return to service. This failure caused the REX test to abort. (A no resources message normally accompanies this occurrence at the MAP display.)	Attempt to RTS the DLM unit.
Preparation Failure: LCMREMn nn n Unit n failed C-side message test	The C-side LCM failed its C-side messaging test.	Post the PM 0 on the C-side of the LCM unit that reports the fault. Test the P-side link from the PM to that LCM unit.
Preparation Failure: DLMREMn nn n Unit n failed C-side message test	The C-side DLM failed its C-side messaging test.	Post the PM on the C-side of the DLM unit that reports the fault. Test the P-side link from the PM to that DLM unit.
ESA Test Preparation Failure: RMM n failed C-side message test	The remote maintenance module (RMM) failed the C-side messaging test. The ESA software module needs the RMM in order to perform a REX test.	Check the state of the RMM to make sure that the RMM is in service and can pass diagnostics.
ESA Test Preparation Failure: ESA failed C-side message test	The ESA software module failed the internal C-side messaging test for ESA.	Post the LCM/DLM that contains the ESA module. Attempt to return to service the system busy link to the ESA.

ROM test failure

The following is a list of ROM test failure messages, all of which require that you replace the NT6X51AB board:

- Config reg rw test
- Stack test
- Rom size test

- Manual bank switch test
- Common bank data test
- Code execution test
- Common bank exec test

RCU and SMU status

The following table lists remote carrier urban (RCU) and SMU status messages and actions.

RCU and SMU status messages and actions (Sheet 1 of 3)

RCU/SMU status message	Explanation	Action
Node Status Mismatch	A difference in status information between the SMU and the CC is present.	Contact your maintenance support group.
AST Line Testing Initiated from <MAP or RCU>	Automatic system testing initiated from the MAP level or from the faceplate of the maintenance card at the RCU. Automatic system testing includes testing and switchover of common equipment cards and line card testing.	There is no action required.
AST Line Testing Completed from <MAP or RCU>	The system initiated automatic system testing from the MAP level or faceplate of the maintenance card at the RCU. Then the system completed automatic system testing.	There is no action required.

RCU and SMU status messages and actions (Sheet 2 of 3)

RCU/SMU status message	Explanation	Action
AST Line Testing Aborted from <MAP or RCU>	One of the following reasons caused the automatic system testing to abort: • a user entered the TST command with the ABORTLNTST parameter at the MAP display • a user pressed the EXEC button at the faceplate of the maintenance card at the RCU • a user set the AUTOTEST field in Table RCUINV to N during a test	There is no action required.
Switchover Initiated	The system initiates 24 h switchover for each RCU.	There is no action required.
Switchover Completed	24 h switchover for each RCU is complete.	There is no action required
Switchover Timeout waiting for Reply	A task waiting for a reply on the completion of the 24 h switchover for a RCU has timed out.	There is no action required.
RCU node status flag cleared	The setting of the RCU node status flag was not correct. This flag setting is now clear.	There is no action required.

RCU and SMU status messages and actions (Sheet 3 of 3)

RCU/SMU status message	Explanation	Action
Status Mismatch: Call Processing; *STATUS*, RCU Node Status; *STATUS*	The call processing node status table does not agree with the current status of the RCU. The call processing node status table is a quick reference for call processing to check the status of a given node. The RCU node status table records the current status.	There is no action required. The system updates the call processing node status table to reflect the status from the RCU node status table.
PCM Loopback test failed on P-side link 5	The PCM loopback test failed on the specified link. A PM183 state change log always follows this log. The PM183 log indicates that the system placed the link in the SysB state.	Post the correct RCU from the PM level of the MAP display, and determine if any alarms are present. Run tests on the RCU or the links to determine the cause of the failure. Link tests can run with the SMU posted at the PM level, or with the links posted at the CARRIER level

TONES sample generation messages

The following table lists TONES sample generation messages and actions.

TONES sample generation messages and actions

TONES sample generation message	Explanation	Action
Maketone Passed	Indicates the tone samples generation facility in the XPM had successful completion.	There is no action required.
Maketone Failed	Indicates the tones samples generation facility in the XPM failed.	After posting the defective PM on the MAP display, ManB the unit. Run OOS tests and proceed depending on return code. If OOS test fails, reload and return the unit to service. If the RTS command is not successful, contact the next level of support.

CMR loading status messages

The following table lists CLASS modem resource (CMR) loading status messages and actions.

CMR loading status messages and actions

CMR status message	Explanation
Loaded CMR	Indicates the system loaded the CMR file.
Loaded CMR via Mate	Indicates the system loaded the CMR file through the mate.
Failed to Load the CMR	Indicates the system failed to load the CMR file.
Failed to load CMR via Mate	Indicates the system was not able to load the CMR file through the mate.
Task Aborted while Loading CMR	Indicates loading process. was aborted.

XPM loading status messages

The following table lists XPM loading status messages and actions.

XPM loading status messages and actions

XPM loading status message	Description
Loaded XPM	Indicates the system loaded the XPM file.
Loaded XPM via Mate	Indicates the system loaded the XPM through the mate.
Failed to Load the XPM	Indicates the system did not load the XPM.
Failed to load XPM via Mate	Indicates the system was not able to load the XPM through the mate.
Task Aborted while Loading XPM	Indicates the loading process was aborted.

The following table lists a summary of loading types.

Summary of loading types (Sheet 1 of 4)

Loading type	Description
Regular loading	Loaded with NDT28AU.
	Loaded CMR with CMR28AB.
	Failed to load with NDT28AU.
	Failed to load while loading with NDT28AU.
	Task aborted while loading with NDT28AU.
	Task aborted while loading CMR with CMR28AU.
Mate loading	Received NDT28AU and broadcasted to the inactive unit of the NDT28AU.
	Failed to receive NDT28AU and failed to broadcast to the inactive unit of the NDT28AU.
	Task aborted during reception of NDT28AU broadcasting to the inactive unit of the NDT28AU.

Summary of loading types (Sheet 2 of 4)

Loading type	Description
Enhanced RCC loading	Loaded with NRC28AU and broadcasted to the inactive unit of the NRC28AU. Loaded CMR with CMR28AU and broadcasted to the inactive unit of the CMR. Failed to load with NRC28AU and failed to broadcast to the inactive unit of the NRC28AU. Failed to load CMR with CMR28AU and failed to broadcast to the inactive unit of the CMR. Loaded with NRC28AU. Loaded CMR with CMR28AU. Failed to load with NRC28AU. Failed to load CMR with CMR28AU. Task aborted while loading with NRC28AU and broadcasting to the mate of NRC28AU. Task aborted while loading CMR with CMR28AU and broadcasting to the CMR mate. Task aborted while loading with NRC28AU. Task aborted while loading CMR with CMR28AU.

Summary of loading types (Sheet 2 of 4)

Loading type	Description
Enhanced RCC loading	Loaded with NRC28AU and broadcasted to the inactive unit of the NRC28AU. Loaded CMR with CMR28AU and broadcasted to the inactive unit of the CMR. Failed to load with NRC28AU and failed to broadcast to the inactive unit of the NRC28AU. Failed to load CMR with CMR28AU and failed to broadcast to the inactive unit of the CMR. Loaded with NRC28AU. Loaded CMR with CMR28AU. Failed to load with NRC28AU. Failed to load CMR with CMR28AU. Task aborted while loading with NRC28AU and broadcasting to the mate of NRC28AU. Task aborted while loading CMR with CMR28AU and broadcasting to the CMR mate. Task aborted while loading with NRC28AU. Task aborted while loading CMR with CMR28AU.

Summary of loading types (Sheet 3 of 4)

Loading type	Description
Broadcast loading	Loaded with NDT28AU and broadcasted to unit 0 of DTC 0, 1, 2, 3, 4. Loaded CMR with CMR28AU and broadcasted to unit 0 of DTC 0, 1, 2, 3, 4. Loaded with NDT28AU and broadcasted to the mate and both units of DTC 0, 1, 2, 3, 4. Loaded CMR with CMR28AU and broadcasted to the mate and both units of DTC 0, 1, 2, 3, 4. Failed to load with NDT28AU and failed to broadcast to unit 0 of DTC 0, 1, 2, 3, 4. Failed to load CMR with CMR28AU and failed to broadcast to unit 0 of DTC 0, 1, 2, 3, 4. Failed to load with NDT28AU. Failed to broadcast to the mate of NDT28AU and both units of DTC 0, 1, 2, 3, 4. Failed to load CMR with CMR28AU. Failed to broadcast to the CMR mate and both units of DTC 0, 1, 2, 3, 4. Task aborted while loading with NDT28AU and broadcasting to unit 0 of DTC 0, 1, 2, 3, 4. Task aborted while loading CMR with CMR28AU and broadcasting to unit 0 of DTC 0, 1, 2, 3, 4. Task aborted while loading with NDT28AU. Task aborted while broadcasting to the mate of NDT28AU and both units of DTC 0, 1, 2, 3, 4. Task aborted while loading CMR with CMR28AU and broadcasting to the CMR mate and both units of DTC 0, 1, 2, 3, 4.

Summary of loading types (Sheet 4 of 4)

Loading type	Description
Broadcast mate loading	Received NDT28AU and broadcasted to the inactive unit of DTC 0, 1, 2, 3, 4. Received CMR28AU and broadcasted to the inactive unit of DTC 0, 1, 2, 3, 4. Failed to receive NDT28AU and failed to broadcast to the inactive unit of DTC 0, 1, 2, 3, 4. Failed to receive CMR28AU and failed to broadcast to the inactive unit of DTC 0, 1, 2, 3, 4. Task aborted while receiving NDT28AU and broadcasting to the inactive unit of DTC 0, 1, 2, 3, 4. Task aborted while receiving CMR28AU and broadcasting to the inactive unit of DTC 0, 1, 2, 3, 4.
Broadcast LCM loading	Received LCM28A and broadcasted to unit 0 of LCM HOST 00 0, REM1 00 1, HOST 10 0. Received LCM28A and broadcasted to both units of LCM HOST 00 0, REM1 00 1, HOST 10 0. Failed to receive NDT28AU and failed to broadcast to unit 0 of LCM HOST 00 0, REM1 00 1, HOST 10 0 Task aborted while receiving NDT28AU and broadcasting to unit 0 of LCM HOST 00 0, REM1 00 1, HOST 10 0.

The following list provides a summary of loading results:

- failed to open link
- no reply from PM
- bad message received from PM
- fail message received from PM
- first get on file failed
- invalid I/P record length
- invalid first char

- invalid character
- load error message received
- failed to get checksum
- failed to open file
- C-side links unavailable
- bad checksum over load
- record count error
- PM reports bad load checksum
- load message error count
- no resources available - try again
- no system resources are available
- load ESA aborted: Nil ESA target
- failed to submit secondary process
- PM excluded from loading group
- timed out waiting to open file
- unexpected who am I (WAI) detected from PM

Operational message faults for DMSX protocols

The following table explain operational message faults for DMSX protocols.

Operational message faults for DMSX protocols (Sheet 1 of 2)

Operational message fault	Explanation
BACKPR	Back pressure time-out - no free receiver buffers.
BADCRC	Occurs when the cyclic redundancy check (CRC) code is not correct.
BADSUM	Occurs when the checksum for a message is not correct.
BCKDWN	Occurs when a slave process waits for a SEND message so that the process can transmit a message. Instead the slave process receives an MIS (may I send) message from the master process.
BUFOVF	Occurs when no buffers are available.

Operational message faults for DMSX protocols (Sheet 2 of 2)

Operational message fault	Explanation
FLSMIS	False MIS that occurs when only one MIS is on the link. A minimum of two MISs are needed on the link for the message to be valid.
MISTO	May I send Time Out.
MSGLEN	Message length error that occurs during reception of a message length that is not correct.
NACK1	Occurs during reception of the first negative acknowledgement (NACK) after a message transmission.
NACK2	Occurs during the reception of a second NACK after a message transmission.
NACKX	Occurs during NACK transmission after reception of a corrupted message.
RBNDMSG	Rebounded message error occurs when a message rebounds.
WACKTO	Wait for acknowledgement time-out error occurs when transmission of a SEND does not result in reception of a start of message (SOM).
WANRTO	Wait for Idle after acknowledging. A positive acknowledgement (PACK) or a NACK can acknowledge a message. A message time-out occurs when this acknowledgement does not result in reception of IDLE.
WANXTO	Wait for Idle after a PACK. A NACK time-out occurs when the reception of a NACK acknowledgement does not result in the reception of a PACK or NACK.
WASTO	Wait to send time-out occurs when the transmission of an MIS does not result in the reception of a filtered SEND.

Operational message faults for HDLC protocols

The following table explain operational message faults for HDLC protocols.

Operational message faults for HDLC protocols

Operational message fault	Explanation
INGLN	Occurs when the first alignment attempt of the protocol fails.
MSURX	The message signal unit (MSU) contains messages that UP tasks generate.
MSUTX	The number of MSUs transmitted on the link divided by 128.
NKRCV	Occurs during reception of NACK.
NTRSH	The number of MSUs retrieved from the transmission queue after reactivation occurred.
REACT	The number of reactivations on the link.
SGERR	Detects loops on the link, and occurs in two conditions: • the system receives on the link a bad backward sequence number (BSN) or bad forward indicator bit (FIB) detected in a signal unit (SU) • the system detects a looped signal
SGRCV	The system detects an error in a received SU.

Loopback status messages

The following is a list of loopback status messages:

- Local loopback enabled
- Local loopback cleared
- Remote loopback enabled
- Remote loopback cleared
- Remote loopback waiting enabled

PSAP test failure messages

The following table lists public-safety answering point (PSAP) messages and actions.

PSAP test failure messages and actions

PSAP test failure message	Explanation	Action
PM not responding	Identifies that the generated LDT fails to receive an expected message from the SMU. This message also can indicate that the CC and SMU do not agree on the status of an LDT node.	Try to determine reason for the failure of the SMU to respond.
LDT node status flag cleared	Indicates that the audit set and cleared the LDT node status flag by accident.	There is no action required.
LDT node status; ManB	Identifies that the generated call processing node status table is not the same as the correct status of the LDT. The LDT node status table records the correct status of the LDT.	There is no action required.
Node status mismatch	Indicates differences in information between the SMU node/link status table and the CC statue table.	There is no action required.

Parity audit fault messages

The following table lists parity audit fault messages and actions.

Parity audit fault messages and actions

Parity audit fault message	Explanation	Action
Parity audit detected hard parity fault	Indicates that the parity audit detected a parity fault that a hardware failure caused. The system generates a list of memory cards that have faults.	Perform the following steps: • Replace the card that has faults displayed in the cardlist. • Reload and RTS the unit that has faults. Refer to table XPM LOADING STATUS for loading information.
Parity audit detected soft parity fault in the program store.	Indicates that the parity audit detected a parity error that a software fault in the program store caused.	Reload and RTS the unit that has faults indicated in the log.
Parity audit detected soft parity fault in the data store.	Indicates that the parity audit detected a parity error that a software fault in the data store caused.	BUSY and RTS the unit that has faults indicated in the log.
Parity audit detected intermittent parity fault.	Indicates that the parity audit detected a parity error. The parity audit did not detect a parity error on the reread of the location at fault.	BUSY and RTS the unit that has faults.

RCC2 messages

A list of RCC2 messages follows:

- Mismatch of the firmware edition between the LOADABLE and EXECUTABLE EEPROM in unit
- Mismatch of the firmware edition between the inventory table and EEPROM # & in the unit
- FAIL TO LOAD EEPROM - UNIT FOUND IN FRM LEVEL
- FAIL TO LOAD EEPROM - TIME OUT OPEN ROUTE
- FAIL TO LOAD EEPROM - UNIT FOUND IN ROM LEVEL
- FAIL TO QUERY FOR EDITION OF EEPROM

- ERASE EEPROM #& COMPLETED SUCCESSFULLY # OF REERASES : &$ # OF REWRITES : &$
- FAIL TO ERASE EEPROM #& # OF REERASES : &$ # OF REWRITES : &$
- FAIL TO LOAD EEPROM # & - FILE INCORRECT
- FAIL TO LOAD EEPROM # & - FLAGS INCORRECT
- FAIL TO LOAD EEPROM # & - FAIL TO PROGRAM
- FAIL TO LOAD EEPROM # & - ADDRESS OVERLAP
- FAIL TO LOAD EEPROM # & - ILLEGAL S-RECORD
- FAIL TO LOAD EEPROM # & - ADDRESS RANGE VIOLATION
- BAD EEPROM # & CHECKSUM MS COUNT OF CC IS : N MSG COUNT OF XPM IS : N
- FAIL TO LOAD EEPROM # & - FAIL TO SWITCH BETWEEN EEPROMS
- FAIL TO LOAD EEPROM # & - ROM DIAGNOSTIC FAILED
- FAIL TO LOAD EEPROM #&-FAIL TO RUN FROM EEPROM # $
- FAIL TO LOAD EEPROM # & - FLAGS UPDATE FAIL
- UPDATE EEPROM #& WITH <file name> COMPLETED SUCCESSFULLY EEPROM # & EDITION WAS CHANGED FROM <edition> to <edition>
- UPDATE EEPROM #& INFO : # OF REWRITES :&$
- UPGRADE EEPROM #& WITH <file name> COMPLETED SUCCESSFULLY EEPROM #& EDITION WAS CHANGED FROM <edition> TO <edition>
- UPGRADE EEPROM # & INFO : # OF REERASES : &$ OF REWRITES : &$
- If the loading process is aborted the text field will read: TASK ABORTED WHILE LOADING EEPROM
- HDLC Cside msg link GAINED sync - link 0
- HDLC Cside msg link LOST sync - link 2

XLIU ISTb messages

When congestion causes an X.25/X.75 link interface unit (XLIU) to go ISTb, the system issues a PM181 log. The system issues PM181 to

provide the reason for the congestion. The following table lists XLIU ISTb messages. These messages use the following acronyms:

- packet (PKT)
- buffer management system (BMS)
- dynamic window (DW)
- HDLC frame processor (HFP)
- HFP buffer management (HBM)
- receiver not ready (RNR)
- layer two (L2)

XLIU ISTb messages

XLIU message	Explanation	Action
PKT drop threshold reached.	ISTb condition	There is no action required.
BMS DW congestion threshold reached.	ISTb condition	There is no action required.
HBM DW congestion threshold reached.	ISTb condition	There is no action required.
BMS RNR@L2 threshold reached.	ISTb condition	There is no action required.

PM185

Log report PM185 gives the trace back of the last trap that caused a peripheral to start again.

Format

The format for log report PM185 is as follows:

```
PM185 date time seqnbr TBL PM TRAP pmtype pmnbr
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
pmtype	alphabetic	The peripheral module type.
pmnbr	0000-9999	The peripheral module number.

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.

PM720

This log report is produced whenever an unsolicited maintenance message is received in the Core from a GWC indicating that a certain number of service ports are to be placed in or out of service. These service ports represent the capability of the subtending UAS to process announcement and conference calls.

Format

The format for log report PM720 is as follows:

```
PM720 mmmdd hh:mm:ss ssdd INFO SERVICE CHANGE pmid
    Mtc Request: <request type>
    Service: <aaaa>  Ports: <nnnn>
    <warning text>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
INFO SERVICE CHANGE	Symbolic text	Information concerning service change request from GWC.
pmid	Symbolic text	Identifies the affected Audio Server node (subtending the GWC).
Mtc Request:	POOL INIT POOL BUSY POOL GRACEFUL BUSY POOL RTS or NODE GRACEFUL BUSY	Identifies the type of service change requested: POOL INIT - indicates that the pool of ports associated with the given service has been initialized. POOL BUSY - indicates that a number of ports associated with the given service are being taken out of service. Active calls involving any of the ports being taken out of service will also be taken down. POOL GRACEFUL BUSY - same as POOL BSY except that outstanding calls are not affected. POOL RTS - indicates that a number of ports associated with the given service are being returned to service. NODE GRACEFUL BUSY - indicates that all ports associated with all services on the node are being taken out of service. However, active calls involving these ports are not affected.
Service:	ANNC, CONF, BCT or ALL	Identifies the service for which the service change is being requested: ANNC - announcements CONF - conferencing BCT - Bearer Channel Tandeming ALL - all services (only applicable to the NODE GRACEFUL BUSY mtc request)
Ports:	Symbolic text	Indicates the number of ports affected for the given service.
<warning text>	Symbolic text	Optional field which applies to POOL INIT requests only. It identifies a mismatch between the data provided by the GWC and the values provisioned in table SERVSINV for the option(s) identified.

Action

Action is required whenever the following warning text is present:

Warning: SERVSINV mismatch detected

Do one of the following:

- Assign one or more of the options ANNC, 3PORT and/or 6PORT in table SERVSINV.
- Change the values of the options ANNC, 3PORT and/or 6PORT in table SERVSINV to correspond with the values which appear in the log report.

Associated OM registers

This log is associated with the following usage registers in OM group AUDSRVS:

- ANNCINSU - indicates the number of ANNC ports which are currently in an in-service state
- CNF3INSU - indicates the number of 3PORT conference circuit ports which are currently in an in-service state
- CNF6INSU - indicates the number of 6PORT conference circuit ports which are currently in an in-service state
- ANNCOOSU - indicates the number of ANNC ports which are currently in an out-of-service state
- CNF3OOSU - indicates the number of 3PORT conference circuit ports which are currently in an out-of-service state
- CNF6OOSU - indicates the number of 6PORT conference circuit ports which are currently in an out-of-service state

Additional information

This log report requires no additional information.

PM777

Log report PM777 is generated when the software detects a hardware defect. This log indicates the source of the defect.

Format

The format for log report PM777 is as follows:

```
PM777 mmmdd hh:mm:ss ssdd INFO SUSPECTED H/W FAULT pmid
   unit no.
   PP TIME: hh:mm:sshs
   ERROR STATE: xxxxxxxxxxxxxxxx
   SUSPECTED CARD(S):
   SITE FLR RPOS BAY ID SHF DESCRIPTION SLOT EQPEC
   host fl# row# bay id sh# frame# slot# cardid
   DATA: xx xx xx xx xx xx xx
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
INFO SUSPECTED H/W FAULT	Symbolic text	Indicates the PM with the suspected hardware defect.
unit no.	Integers	Indicates the unit number.
PP TIME	Integers	Indicates the time of the defect.
ERROR STATE	Symbolic text	Indicates the error state.
SUSPECTED CARD(S)	Numeric	Indicates the suspect cards.
DATA	Alphanumeric	Indicates more information about the defect.

Action

Follow standard maintenance procedures.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

V5200

Log report V5200 generates this information report when the bearer channel connection (BCC) fails on a speech link.

Format

The format for log report V5200 is as follows:

```
V5200 mmmdd hh:mm:ss xxxx <log_type> <link_type> <pm_id>
   <interface_information>
   V5LINK No: <link_number> <chnl_number> V5ID: <ID>
   PORT: <pm_id> <P-side_link_number>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	FLT	Status. V5 link fault.
link_type	BCC	Fault occurred on BCC (speech) link.
pm _id	see subfields	Peripheral module (PM) identifier. Consists of subfields PM type and GPP PM number.
PM_type	GPP	V5 links always terminate on a GPP.
PM_number	0 to 255	Peripheral module number assigned to the GPP.
interface_information	alphanumeric string	Information. BCC failed on a speech link for one of the following reasons: • BCC allocation fails • BCC de-allocation fails • BCC audit fails
link_number	1 to 16	V5 AN C-side link number.
chnl number	0 to 31	channel number. PCM30 channel carrying BCC information on the V5.2 link.
V5ID	see subfields	V5 interface identifier. Equates to field AMCNO in table GPPTRNSL. composed of subfields; SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site designator.

Field	Value	Description
FRAME	0 to 511	Frame number of access node (AN) supplying the V5 interface. Entry can be unique within the site if office parameter, UNIQUE_BY_SITE_NUMBERING, in table OFCENG, is datafilled Y.
UNIT	0 to 9	Access node unit number
PORT	see subfields	GPP port of affected link. Consists of subfield pm_id.
pm _id	see subfields	Peripheral module (PM) identifier. Consists of subfields PM_type and PM_number.
PM_type	GPP	V5 links always terminate on a GPP.
PM_number	0 to 255	Peripheral module number assigned to the GPP.
P-side_link_number	0 to 47	GPP P-side PCM30 link number.

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.

V5201

Log report V5201 generates this information when a V5.2 link bearer channel control (BCC) request for a speech channel is rejected.

Format

The format for log report V5201 is as follows:

```
V5201 mmmdd hh:mm:ss xxxx <log_type> <link_type>
<interface_information>
Reason: <reason>
V5LINK No:<link_number> <chnl_number> <ID>
PORT: <GPP_number> <P-side_link_number>
 LEN: <line_equipment_number> DN: <directory number>
 <user_port_information>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	Status. Protection switching has occurred indicating a link with a C-channel has failed.
link_type	BCC	Fault occurred on BCC (speech) link.
interface_information	alphanumeric string	Information. BCC request rejected.

Field	Value	Description
Reason	alphanumeric string	Reason for failure. BCC request was rejected for one of the following reasons: • Connection already present on time slot to a different port. • Connection already present at PSTN user port to a different time slot. • User port not provisioned. • Invalid V5 time slot identification • Invalid V5 2048 Kbits/s link identification • V5 time slot(s) being used as physical C-channel(s). • Use port unavailable (blocked). • V5 link unavailable (blocked). • De-allocation cannot be completed due to incompatible data content. • De-allocation cannot be completed due to user port time slot(s) data incompatibility. • De-allocation cannot be completed due to port data incompatibility.
LINK_number	1 to 16	Number assigned to V5LINK at the access node (AN). Determined by order of datafill in table GPPTRNSL.
chnl_number	0 to 31	C-channel number. The bearer channel on the PCM30 V5.2 link.
ID	see subfields	V5 interface identifier. Equates to field AMCNO in table GPPTRNSL. composed of subfields; SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site designator.
FRAME	0 to 511	Frame number of access node (AN) supplying the V5 interface. Entry can be unique within the site if office parameter, UNIQUE_BY_SITE_NUMBERING, in table OFCENG, is datafilled Y.
UNIT	0 to 9	Access node unit number
PORT	see subfields	GPP port of affected link. Consists of subfields GPP PM number and P-side link number.
GPP_number	0 to 255	Peripheral module number assigned to the GPP.

Field	Value	Description
line_equipment_number	numeric	Virtual line equipment number from table LNINV assigned to line.
directory_number	numeric (up to 15 digits)	Directory number assigned to line.
user_port_information	alphanumeric string	Information. Failing user port or time slot identification.

Action

Determine the reason the V5 link has been blocked on the access node (AN) side.

Post the GPP P-side links.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

V5202

Log report V5202 generates this information report when a V5.2 link bearer channel control (BCC) audit request is incomplete.

Format

The format for log report V5202 is as follows:

```
V5202 mmmdd hh:mm:ss xxxx <log_type> <link_type>
<interface_information>.
Reason: <reason>
V5LINK No:<link_number> <chnl_number> <ID>
PORT: <GPP_number> <P-side_link_number>
 LEN: <line_equipment_number> DN: <directory_number>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	Status. Incomplete audit request occurred.
link_type	BCC	Fault occurred on BCC (speech) link.
interface_information	alphanumeric string	Information. BCC audit connection incomplete information element.
Reason	alphanumeric string	Reason for failure. BCC audit request was rejected for one of the following reasons: • Incomplete normal • Access network fault • User port not provisioned • Invalid V5 time slot identification • Invalid V5 2048 Kbits/s link identification • V5 time slot(s) being used as physical C-channel(s)
LINK_number	1 to 16	Number assigned to V5LINK at the access node (AN). Determined by order of datafill in table GPPTRNSL.
chnl_number	0 to 31	C-channel number. The bearer channel on the PCM30 V5.2 link.

Field	Value	Description
ID	see subfields	V5 interface identifier. Equates to field AMCNO in table GPPTRNSL. composed of subfields; SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site designator.
FRAME	0 to 511	Frame number of access node (AN) supplying the V5 interface. Entry can be unique within the site if office parameter, UNIQUE_BY_SITE_NUMBERING, in table OFCENG, is datafilled Y.
UNIT	0 to 9	Access node unit number
PORT	see subfields	GPP port of affected link. Consists of subfields GPP_PM_number and P-side_link_number.
GPP_number	0 to 255	Peripheral module number assigned to the GPP.
line_equipment_number	numeric	Virtual line equipment number assigned to line in table LNINV.
directory_number	numeric (up to 15 digits)	Directory number assigned to line.

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.

V5400

Log report V5400 generates this information report when the V5 CC Audit sends a V5 interface query message, and receives no reply message.

Format

The format for log report V5400 is as follows:

```
V5400 mmmdd hh:mm:ss xxxx <log_type> V5AUDIT GPP <gpp_no>
No reply from V5 Interface.
V5id: <ID>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	This field indicates V5 information that follows in field interface information.
gpp_no	0 to 255	Peripheral number assigned to GPP.
ID	see subfields	V5 interface identifier. Made of subfields SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site identifier.
FRAME	0 to 511	Frame number of the access node (AN) that supplies the V5 interface.
UNIT	0 to 9	AN node number.

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.

V5401

Log report V5401 generates this information report when a V5 Interface status mismatch occurs between the computing module (CM) and GPP.

Format

The format for log report V5401 is as follows:

```
V5401 mmmdd hh:mm:ss xxxx <log_type> V5AUDIT GPP <gpp_no>
V5 Interface activity status mismatch.
The interface status will be fixed to <status> on the LE.
V5id: <ID>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	This field indicates V5 information that follows in field interface information.
gpp_no	0 to 255	Peripheral number assigned to GPP.
status	ACTIVE, or DEACTIVE	Status of the V5 interface that will be fixed on the LE.
ID	see subfields	V5 interface identifier. Made of subfields SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site identifier.
FRAME	0 to 511	Frame number of the access node (AN) that supplies the V5 interface.
UNIT	0 to 9	AN node number.

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.

V5402

Log report V5402 generates this information report when a V5 link status mismatch occurs between the computing module (CM) and GPP.

Format

The format for log report V5402 is as follows:

```
V5402 mmmdd hh:mm:ss xxxx <log_type> V5AUDIT GPP <gpp_no>
V5 link status mismatch has been detected.
The link status has been fixed to <status>.
V5LINK No: 1 V5id: V5AN 0 2
PORT: GPP 1 P-Side Link 7
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	This field indicates V5 information that follows in field interface information.
gpp_no	0 to 255	Peripheral number assigned to GPP.
status	InService, or System Busy, or Remote Blocked	Status of the V5 link.
ID	see subfields	V5 interface identifier. Made of subfields SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site identifier.
FRAME	0 to 511	Frame number of the access node (AN) that supplies the V5 interface.
UNIT	0 to 9	AN node number.
P-Side_link_no	0 to 47	GPP P-side PCM30 link number.

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.

V5403

Log report V5403 generates this information report when a C-channel data mismatch occurs between the computing module (CM) and GPP.

Format

The format for log report V5403 is as follows:

```
V5403 mmmdd hh:mm:ss xxxx <log_type> V5AUDIT GPP <gpp_no>
V5 C-channel data mismatch has been detected.
<reason>
V5LINK No: <link_no> C-chnl <C_no> V5id: <ID>
PORT: GPP <gpp_no> P-Side Link <p-side_link_no>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	This field indicates V5 information that follows in field interface information.
gpp_no	0 to 255	Peripheral number assigned to GPP.
reason	C-channel definition C-channel activity mismatch (ACT/STBY)C-channel status mismatch (INSV/OOS)	The reason for the C-channel data mismatch.
link_no	0 to 15	V5 AN C-side link number.
C_no	15, 16, or 31	C-channel number. Note: C-channel links can only be located on PCM30 link channels 15, 16, and 31.
ID	see subfields	V5 interface identifier. Made of subfields SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site identifier.
FRAME	0 to 511	Frame number of the access node (AN) that supplies the V5 interface.
UNIT	0 to 9	AN node number.
P-side_link_no	0 to 47	GPP P-side PCM30 link number.

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.

V5404

Log report V5404 generates this information report when a data link status mismatch occurs between the computing module (CM) and GPP.

Format

The format for log report V5404 is as follows:

```
V5404 mmmdd hh:mm:ss xxxx <log_type> V5AUDIT GPP <gpp_no>
V5 Data link status mismatch has been detected.
Protocol: <text>
Protection group: <group_no>
V5id: <ID>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
log_type	INFO	This field indicates V5 information that follows in field interface information.
gpp_no	0 to 255	Peripheral number assigned to GPP.
text	CONTROL, or PSTN, or ISDN	Name of the V5.2 protocol.
group_no	1 to 2	Number assigned to the protection group.
ID	see subfields	V5 interface identifier. Made of subfields SITE, FRAME, and UNIT.
SITE	alphanumeric	Four character site identifier.
FRAME	0 to 511	Frame number of the access node (AN) that supplies the V5 interface.
UNIT	0 to 9	AN node number.

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.

IPSec and IKE security logs

This section describes how to access and understand IPSec and IKE security log reports associated with GWC nodes. These log reports are stored in the securitylog files in directory /var/log on the CS 2000 Management Tools server.

To access these security log reports, follow procedure View GWC logs in syslog files.

Note: To display IPSec and IKE log reports, search for the text string ISAKMP within the securitylog files.

Format

The format for IKE log reports is as follows:

```
mmm dd hh:mm:ss [<IP address>] class_security.ver01 CMD="ISAKMP_<INFO or
FAIL> <log message>",STAT=<status> MID=<MID>
```

Selected field descriptions

The following table explains selected fields in the log report.

Field	Value	Description
mmm dd hh:mm:ss	alphanumeric	The date and time stamp for the log report. ***Note:*** mmm means three first letters of the month, for example, Aug.
<IP address>	numeric	The IP address of the unit device from which the log originated.
<log type>	class_security.ver01	Common name for security logs.
ISAKMP_INFO or ISAKMP_FAIL	text string	Indicates an information-only or a problem-reporting log.
<log message>	alphanumeric character string	A description of the conditions or reasons generating the log. Refer to section Actions on page 399 for the list of log descriptions and associated actions.

Field	Value	Description
<status>	success or failure	Indicates whether the operation succeeded or failed.
<MID>	MID=MID_Nortel_MGC _autho.<0016 or 0017>	0016 indicates an INFO log. 0017 indicates a FAIL log.

Actions

Required action depends on the log description. The following table lists security log messages and explanations, and the appropriate actions.

IPSec and IKE security logs (Sheet 1 of 5)

Log message	Explanation and Action
Logs associated with the "Phase 1 SA failure" GWC320 major alarm:	
ATTENTION ***Service disruption*** The following log reports and the associated alarms are the result of an outage.	
To clear these fault conditions, complete procedure Clear the GWC320 Phase 1 SA failure alarm.	
`ISAKMP_FAIL IKE phase 1 timeout exhausted (PHASE 1 <INITIATOR or RESPONDER>, init:<IP>, resp:<IP>)`	There is a problem during an IKE Phase 1 negotiation and multiple retransmission attempts fail.
`ISAKMP_FAIL IKE payload not formed correctly, possible preshared key mismatch (PHASE 1 INITIATOR, init:<IP>, resp:<IP>)`	The system cannot authenticate the remote gateway.
`ISAKMP_FAIL IKE payload validation failed, possible preshared key mismatch (PHASE 1 <INITIATOR or RESPONDER>, init:<IP>, resp:<IP>)`	The pre-shared key configured on the GWC does not match the pre-shared key configured on the remote gateway.
`ISAKMP_FAIL payload malformed, possible pre-shared key mismatch (resp:<IP>, init:<IP>)`	The pre-shared key configured on the GWC does not match the pre-shared key configured on the remote gateway.

IPSec and IKE security logs (Sheet 2 of 5)

Log message	Explanation and Action
`ISAKMP_FAIL payload malformed (resp:<IP>, init:<IP>)`	The system cannot authenticate the remote gateway.
`ISAKMP_FAIL No Preferences Match for IKE Phase 1 Negotiation (init:<IP>, resp:<IP>)`	IKE preferences configured on the GWC and on the remote gateway do not match.
`ISAKMP_FAIL invalid signature (init IP:<IP>, resp IP:<IP>)`	The GWC cannot authenticate the remote gateway.
`ISAKMP_FAIL IKE phase 1 signature or certificate check (PHASE 1 <INITIATOR or RESPONDER>, init:<IP>, resp:<IP>)`	There is a problem during an IKE Phase 1 negotiation and the GWC cannot verify or authenticate the certificate presented by the remote gateway.
Logs associated with the "Phase 2 SA failure" GWC320 major alarm:	
ATTENTION ***Service disruption*** The following log reports and the associated alarms are the result of an outage.	
To clear these fault conditions, complete procedure Clear the GWC320 Phase 1 SA failure alarm.	
`ISAKMP_FAIL No Preferences Match for IKE Phase 2 Negotiation (init IP:<IP>, resp IP:<IP>)`	IPSec preferences configured on the GWC and on the remote gateway do not match.
`ISAKMP_FAIL IKE phase 2 timeout exhausted (PHASE 2 <INITIATOR or RESPONDER>, init:<IP>, resp:<IP>)`	There is a problem during an IPSec Phase 2 negotiation and multiple retransmission attempts fail.

IPSec and IKE security logs (Sheet 3 of 5)

Log message	Explanation and Action
Logs associated with the "Certificate expiring" GWC320 minor, major, or critical alarm:	
`Certificate is expiring on Year=<yyyy> Month=<mm> Day=<dd>`	After an IKE Phase 1 negotiation, if any certificate in the chain (excluding the root CA) is expiring within 30 days, this failure log is generated. If the certificates are not replaced immediately, there may be a call processing outage. This log is associated a GWC320 alarm: • critical - certificate expires within 5 days • major - certificate expires within 15 days • minor - certificate expires within 30 days If the certificate is expired, this alarm remains, and if any connection policy and IKE authentication is using this certificate, a "Phase 1" alarm is also raised. To clear the "Certificate expiring" alarm, complete procedure “Recovery of the GWC320 certificate expiry alarm” in the *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.
Logs associated with the "Certificate expired" GWC320 critical alarm:	
`One or more certificates in set number <x> are expired.`	One or more certifcates in a set is expired. An outage will occur if an IKE connection policy is using these certificates. To clear the "Certificate expired" alarm, complete procedure “Recovery of the GWC320 certificate expiry alarm” in the *Nortel CVoIP IPSec Security Service Implementation Overview*, NN10453-100.

IPSec and IKE security logs (Sheet 4 of 5)

Log message	Explanation and Action
Logs indicating problems with the Diffie-Hellman (DH) exchange - no associated alarms:	
ATTENTION ***Service disruption*** The following log reports are the result of an outage.	
`ISAKMP_FAIL IKE Phase 1 key negotiation failed - DH is NULL (ini:<ip>, resp:<ip>)`	The GWC cannot allocate sufficient resources. Contact your next level of support
`ISAKMP_FAIL IKE Phase 1 key negotiation failed - unable to set peer's DH pub key (ini:<ip>, resp:<ip>)`	The GWC cannot allocate sufficient resources. Contact your next level of support
`ISAKMP_FAIL IKE Phase 1 key negotiation failed - unable to gen DH key pair (ini:<ip>, resp:<ip>)`	The GWC cannot allocate sufficient resources. Contact your next level of support
`ISAKMP_FAIL IKE Phase 1 key negotiation failed - unable to compute shared secret (ini:<ip>, resp:<ip>)`	The GWC cannot allocate sufficient resources. Contact your next level of support
`ISAKMP_FAIL DOI no supported (ini:<ip>, resp:<ip>)`	The GWC cannot negotiate a security association with the remote gateway. Contact your next level of support.
Logs indicating problems with the Phase 1 exchange - no associated alarms:	
ATTENTION ***Service disruption*** The following log reports are the result of an outage.	
To clear these fault conditions, complete procedure Clear the GWC320 Phase 1 SA failure alarm.	
`ISAKMP_FAIL invalid signature (ini:<ip>, resp:<ip>)`	The GWC cannot authenticate the remote gateway.

IPSec and IKE security logs (Sheet 5 of 5)

Log message	Explanation and Action
`ISAKMP_FAIL invalid payload (ini:<ip>, resp:<ip>)`	The GWC cannot authenticate the remote gateway.
`ISAKMP_FAIL invalid hash info (ini:<ip>, resp:<ip>)`	The GWC cannot authenticate the remote gateway.
Information-only logs:	
`Certificate provisioning - validity period checked: Certificate <effective or expire> Y/M/D H:M:S: <effective or expiry date and time>`	When a certificate is provisioned on the GWC, the GWC checks the certificate effective and expiry date and generates this log. When certificate provisioning fails, use this log to determine if the certificate is not effective or has expired. There is no associated alarm.
`Phase 1 SA Successfully Established (init IP:<IP>, resp IP:<IP>)`	This log confirms a successful IKE Phase 1 negotiation between the GWC and a remote gateway. If a GWC320 alarm is generated, it clears automatically. No action required.
`Phase 2 SA Successfully Established (init IP:<IP>, resp IP:<IP>`	This log confirms a successful IPSec Phase 2 negotiation between the GWC and a remote gateway. If a GWC320 alarm is generated, it clears automatically. No action required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report has no additional information.

Kerberos logs

This section describes how to access and understand log reports associated with the Kerberos application running on the GWC card. These log reports are stored in the securitylog files in directory /var/log on the CS 2000 Management Tools server.

To access the Kerberos log reports, follow procedure View GWC logs in syslog files.

Note: To display Kerberos log reports, search for the text string KERBEROS (common name for all Kerberos logs).

You can also access the Kerberos log reports through the Integrated Element Management System (IEMS). For more information, refer to the *IEMS Fault Management*, NN10334-911.

Format

The format for Kerberos log reports is as follows:

```
mmm dd hh:mm:ss [<host name>] KERBEROS <log description>, IP=<remote IP
address>
```

Selected field descriptions

The following table explains selected fields in the log report.

Field	Value	Description
mmm dd hh:mm:ss	alphanumeric	The date and time stamp for the log report. ***Note:*** mmm means three first letters of the month, for example, Aug.
<host name>	numeric	The IP address of the GWC.
KERBEROS	text string	Common name for all Kerberos log reports.

Field	Value	Description
<log description>	alphanumeric character string	A description of the conditions or reasons generating the log. The log can be static or variable. Refer to the Action section for the list of log descriptions, causes, and associated actions.
<remote IP address>	numeric	The IP address of the remote gateway.

Action

The following tables list the static and variable Kerberos logs. Use these tables to determine your action.

GWC Kerberos static logs (Sheet 1 of 3)

Kerberos application log description	Cause or condition	Action
WAKE_UP timeout after %d ms, exhausted after %d retries	gateway fails to respond to WAKE_UP request	verify connectivity between the GWC and the gateway
AP_REP timeout after %d ms, exhausted after %d retries	gateway fails to respond to AP_REP (a request for a security association)	verify connectivity between the GWC and the gateway
AP_REP timeout after %d ms, retry attempt is now %d	gateway fails to respond to AP_REP (a request for a security association)	verify connectivity between the GWC and the gateway
failed to get FQDN	gateway is not provisioned at the GWC	verify gateway's authenticity and provision gateway
Cannot exceed maximum of %d KM sessions	a large number of gateways try to recover or restore connectivity at once	information-only log
Received AP_REQ while waiting for SA_RECOVERED	race condition, or gateway did not receive AP_REP request	information-only log

GWC Kerberos static logs (Sheet 2 of 3)

Kerberos application log description	Cause or condition	Action
unsolicited SA_RECOVERED	gateway sends an SA_RECOVERED message. Possible cause is the gateway is responding to an old AP_REP (the session was deleted on the GWC).	information-only log
Received SA_RECOVERED while responder for existing key neg	gateway sends an SA_RECOVERED message whereas the server didn't ask for it.	information-only log
Received SA_RECOVERED out of order	gateway sends an SA_RECOVERED message whereas the server was not waiting for this message type	information-only log
CMS nonce is zero in AP_REQ reply to WAKE_UP	race condition, an AP_REQ was initiated by the GW at the same time that a WAKE_UP was sent from the GWC	information-only log
CMS nonce mismatch in AP_REQ reply to WAKE_UP	race condition, an AP_REQ was sent as a response to a previously initiated WAKE_UP	information-only log
Non-zero CMS nonce in initiator AP_REQ	race condition, an AP_REQ was sent by the GW as a response to a WAKE_UP after the WAKE_UP had already timed out	information-only log
For all the following static logs, contact your next level of support: MUTUAL REQUIRED not set in AP_REQ USE_SESSION_KEY (not supported) set in AP_REQ Sub-key in AP_REQ is not allowed		

GWC Kerberos static logs (Sheet 3 of 3)

Kerberos application log description	Cause or condition	Action
IP mismatch: fqdn=%s, ip=%s Failed HMAC in SA_RECOVERED NULL session key parsing AP_REQ but no KRB ERROR ***Note:*** Some log descriptions use variables such as %d or %s to indicate a numeric value is provided.		

GWC Kerberos variable logs

Kerberos application log description
The following log reports can be displayed with different <reasons>. Refer to table Kerberos log reasons for the list of possible reasons and the associated actions. <reason> while making KRB_ERROR message <reason> while checking AP_REQ proposal <reason> while generating AP_REP sub-key <reason> while adding pending incoming SA for AP_REQ <reason> while adding pending outgoing SA for AP_REQ <reason> while computing SA_RECOV HMAC <reason> while committing SAs for AP_REQ <reason> while parsing AP_REQ <reason> while parsing KRB_AP_REQ <reason> while verifying AP_REQ <reason> while parsing SA RECOV <reason> while verifying SA RECOV <reason> while updating CLOCKSKEW <reason> when parsing name \"%s\" <reason> while updating server principal

Kerberos log reasons

Kerberos log reasons	Action
"No IPSEC policy match"	verify provisioning datafill; if required, configure an appropriate connection policy
"IPSEC ciphersuite is not supported"	verify encryption and authentication provisioning datafill
"No policy match for AP_REQ"	verify provisioning datafill
"Invalid SA lifetime"	verify provisioning datafill; make sure that the same values are configured on the GWC and the gateway
"Invalid ciphersuite"	verify provisioning datafill (encryption and authentication algorithms); make sure that the same values are configured on the GWC and the gateway
"No IPEC policy"	verify provisioning datafill
"Invalid IPSEC proposal"	verify provisioning datafill
"Invalid key length"	verify provisioning datafill
"Invalid renewal period"	verify provisioning datafill
"Ticket not yet valid"	synchronize the time between the GWC and KDC
"Clock skew too great"	synchronize the time between the GWC and the gateway
"Ticket expired"	no action required - gateway should automatically request a new ticket. If re-occurring, check the KDC status and configuration.
"Generic KRBKMP error'	information only
"Message out of order"	information only
"Generic error (see e-text)"	information only
For all other <reasons>, 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.

BITS300

Log report BITS300 indicates that a clock sync critical alarm has been raised for one of following: MTIE Performance, Alarm Indication Signal, Loss of Signal, or Out of Frame. Correlates with BITS600.

Format

The format for log report BITS300 is as follows:

```
MSH10_I06BE  ** BITS300 APR23 14:27:17 9809 TBL  BITS Fault Report
          TimeStamp  : APR 23 14:27:17.635
          Location   : SPM : 6  SRM : 1  BITSB
          Fault Type : Loss of Signal(LOS)
          Status     : Alarm Raised
          Location: SPM 6  Type: SMG4      Fabric: ATM
```

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.

BITS301

Log report BITS301 indicates that a clock sync non-critical alarm has been raised for one of the following: Timing Link Degradation, Bipolar Violation, or Cyclic Redundancy Check. Correlates with BITS601.

Format

The format for log report BITS301 is as follows:

```
MSH10_I06BE   * BITS301 APR20 15:13:55 0002 TBL  BITS Timing Link
Degradation
         TimeStamp  : APR 20 15:13:55.250
         Location   : SPM : 6  SRM : 0  BITSA
         Fault Type : Cyclical Redundancy Check(CRC)
         Status     : Alarm Raised
         Location: SPM 6  Type: SMG4      Fabric: ATM
```

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.

BITS500

Log report BITS500 indicates a BITS link state change capturing old/new states and reason for change (including degradation of carrier (LOS, LOF)).

Format

The format for log report BITS500 is as follows:

```
MSH10_I06BE     BITS500 APR23 14:27:17 9808 INFO BITS Timing Link State
Change
          TimeStamp  : APR 23 14:27:17.635
          Location   : SPM : 6   SRM : 1   BITSB
          From       : InSv
          To         : SysB
          Location: SPM 6  Type: SMG4      Fabric: ATM
```

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.

BITS600

Log report BITS600 indicates a BITS Fault Report Cleared; a critical alarm from BITS300 is cleared.

Format

The format for log report BITS600 is as follows:

```
MSH10_I06BE     BITS600 APR23 14:27:19 9813 INFO BITS Fault Report Cleared
          TimeStamp  : APR 23 14:27:19.905
          Location   : SPM : 6   SRM : 1   BITSB
          Fault Type : Loss of Signal(LOS)
          Status     : Alarm Cleared
          Location: SPM 6  Type: SMG4      Fabric: ATM
```

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.

BITS601

Log report BITS601 indicates that a BITS Fault Report Cleared; a non-critical alarm from BITS301 is cleared.

Format

The format for log report BITS601 is as follows:

```
MSH10_I06BE     BITS601 APR20 16:05:42 0037 INFO BITS Timing Link Degrada-
tion Cleared
          TimeStamp  : APR 20 16:5:42.815
          Location   : SPM : 6   SRM : 0   BITSA
          Fault Type : Timing Link Degradation (TLD)
          Status     : Alarm Cleared
          Location: SPM 6  Type: SMG4      Fabric: ATM
```

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.

BITS610

Log report BITS610 indicates that a BITS timing reference SSM value has changed.

Format

The format for log report BITS610 is as follows:

```
MSH10_I06BE     BITS610 APR23 14:27:17 9810 INFO Reference Quality Change
          TimeStamp  : APR 23 14:27:17.635
          Location   : SPM : 6   SRM : 1   BITSB
          From SSM   : STU
          To SSM     : NIL
          Location: SPM 6  Type: SMG4      Fabric: ATM
```

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.

BITS612

Log report BITS612 indicates that a BITS timing reference source switch has occurred.

Format

The format for log report BITS612 is as follows:

```
MSH10_I06BE     BITS612 APR21 13:10:55 5282 INFO BITS Reference Switch
          TimeStamp  : APR 21 13:10:55.695
          From       : SPM : 6   SRM : 0   NONE
          To         : SPM : 6   SRM : 0   BITSA
          Reason     : System Source Switch
          Location: SPM 6  Type: SMG4      Fabric: ATM
```

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.

IWBM500

Log report IWBM500 indicates that one of the following is out-of-service: C-side link, STS3cP carrier, ATM network state, or the ATM address state for the IW bridge software.

Format

The format for log report IWBM500 is as follows:

```
MSH10_I06BE  ** IWBM500 APR22 09:58:57 5023 SYSB IW_Bridges OOS
          Interworking Bridges Out Of Service.
            SPM Number: 2
            IW_Bridge Range: 1 through 2016
            Reason: ATM FrameWork NotOK.  All calls killed.
            Location: SPM 2  Type: IW        Fabric: ATM
```

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.

IWBM501

Log report IWBM501 indicates that the out-of-service item has returned to service.

Format

The format for log report IWBM501 is as follows:

```
MSH10_I06BE     IWBM501 APR22 09:59:17 5043 RTS  IW_Bridges INSV
          Interworking Bridges Recovered
            SPM Number: 2
            IW_Bridge Range: 1 through 2016
            Reason: ATM FrameWork State Reported OK.
            Location: SPM 2  Type: IW        Fabric: ATM
```

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.

IWBM502

Log report IWBM502 indicates that a Bsy command was requested for a set of IW SPM bridge terminals.

Format

The format for log report IWBM502 is as follows:

```
RTP708AK  ** IWBM502 AUG12 00:37:09 5900 INFO MBSY IW Bridge Terminals
          SPM Number: 3
          DS512 link: 3
          IW bridge group state changed from SYSB to MANB
          IW bridge terminal range: 1 through 504
          Reason: Manual Request
          Issued by: YD2
```

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.

IWBM503

Log report IWBM503 indicates that an Rts command was requested for a set of IW SPM bridge terminals.

Format

The format for log report IWBM503 is as follows:

```
RTP708AK     IWBM503 AUG12 00:37:19 6700 INFO RTS IW Bridge Terminals
          SPM Number: 3
          DS512 link: 0
          IW bridge group state changed from MANB to INSV
          IW bridge terminal range: 1513 through 2016
          Reason: Manual Request
          Issued by: YD2
```

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.

IWBM504

Log report IWBM504 indicates that an Offl command was requested for a set of IW SPM bridge terminals.

Format

The format for log report IWBM504 is as follows:

```
RTP708AK  ** IWBM504 AUG12 00:04:26 3200 INFO OFFL IW Bridge Terminals
          SPM Number: 3
          DS512 link: 3
          IW group terminal state changed from MANB to OFFL
          IW bridge terminal range: 1 through 504
          Reason: Manual Request
          Issued by: YD2
```

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.

IWBM505

Log report IWBM505 indicates that an Frls command was requested for a set of IW SPM bridge terminals.

Format

The format for log report IWBM505 is as follows:

```
RTP708AK  ** IWBM505 AUG12 00:37:51 8000 INFO FRLS IW Bridge Terminals
          SPM Number: 3
          DS512 link: 3
          IW bridge group state changed from INSV to MANB
          IW bridge terminal range: 1 through 504
          Reason: Manual Request
          Issued by: YD2
```

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.

IWBM600

Log report IWBM600 indicates the IW bridge receives an invalid terminal ID during an attempt to free a bridge. This causes a connectivity mismatch. An INFO log.

Format

The format for log report IWBM600 is as follows:

```
MSH10_I06BE     IWBM600 APR23 14:56:47 0029 INFO Connectivity Mismatch
          Invalid connection data provided.  Bridge NOT freed.
            SPM: 2
            IW_Bridge: 1050
            IWBM_MG4K_tid:
              Node: 53  TRMNL_NO:  4
            Connectivity_MG4K_tid:
              Node: 54  TRMNL_NO:  4
            Location: SPM 2  Type: IW        Fabric: ATM
```

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.

IWBM601

Log report IWBM601 indicates that an automatic system audit finds a problem and performs a corresponding action. An INFO log.

Format

The format for log report IWBM601 is as follows:

```
MSH10_I06BE     IWBM601 APR23 14:58:08 0036 INFO Audit Action
          Connectivity mismatch: Bridge RTSd
            SPM: 2
            IW_Bridge: 1050
            IWBM_ENET_tid:
              Node: 0  TRMNL_NO:  0
            IWBM_MG4K_tid:
              Node: 53  TRMNL_NO:  4
            Location: SPM 2  Type: IW        Fabric: ATM
```

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.

IWBM602

Log report IWBM602 indicates that no IDL bridges are available. An INFO log.

In SN07, and later releases, a bridge pool field displays the related bridge pool name from the NETBRDGE table. This field appears on the log when the MULTINET_DISPLAY_ACTIVE field in the OFCVAR table is set to Y.

Format

The format for log report IWBM602 is as follows:

```
MSH10_I06BR     IWBM602 JUN13 02:03:50 5442 INFO IWBM: No IDL Bridges
          No IDL Bridges on any FreeQueue.
          Number of IW call attempts lost: 52
          Bridge Pool: <bridge_pool_CLLI>
```

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.

IWBM603

Log report IWBM603 indicates that an IWBM audit is being performed. An INFO log.

Format

The format for log report IWBM603 is as follows:

```
OLSC_05BK     IWBM603 FEB23 12:27:41 0002 INFO IWBM Audit
IWBM Audit Started.



OLSC_05BK     IWBM603 FEB23 12:27:41 0003 INFO IWBM Audit
IWBM Audit Ended.
```

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.

IWBM700

Log report IWBM700 indicates that a maintenance action is being performed. An INFO log.

Format

The format for log report IWBM700 is as follows:

```
OLSC_06BB     IWBM700 FEB20 16:04:52 0000 INFO MTCE Action
          MTS cannot commuincate with SPM - msg not sent
            SPM: 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.

IWBM800

Log report IWBM800 indicates that the number of available IW bridges exceeds the first threshold (70%) when attempting to retrieve an IW-bridge ID from the IW bridge manager.

In SN07, and later releases, a bridge pool field displays the related bridge pool name from the NETBRDGE table. This field appears on the log when the MULTINET_DISPLAY_ACTIVE field in the OFCVAR table is set to Y.

Format

The format for log report IWBM800 is as follows:

```
MSH10_I06BE  ** IWBM800 APR22 09:58:57 5021      1st Threshold Exceeded
          The number of interworking bridges in use has
          exceeded 70 percent of all bridges in the pool.
            Total number of IW_Bridges:        2016
            Number of available IW_Bridges:           <NN>
            Bridge Pool: <bridge_pool_CLLI>
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

The IWBMNODE OM group provides IW SPM nodal bridge usage which may be summed to calculate the appropriate Bridge Pool usage.

Additional information

This log report requires no additional information.

IWBM801

Log report IWBM801 indicates that the number of available IW bridges falls to less than 65% of bridges in the pool in use. This log always occurs after IWBM800.

In SN07, and later releases, a bridge pool field displays the related bridge pool name from the NETBRDGE table. This field appears on the log when the MULTINET_DISPLAY_ACTIVE field in the OFCVAR table is set to Y.

Format

The format for log report IWBM801 is as follows:

```
MSH10_I06BE     IWBM801 APR22 09:59:17 5041      1st Threshold Cleared
          The number of interworking bridges in use has
          fallen below 65 percent of all bridges in the pool.
            Total number of IW_Bridges:        2016
            Number of available IW_Bridges:        2016
            Bridge Pool: <bridge_pool_CLLI>
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

The IWBMNODE OM group provides IW SPM nodal bridge usage which may be summed to calculate the appropriate Bridge Pool usage.

Additional information

This log report requires no additional information.

IWBM802

Log report IWBM802 indicates that the number of available IW bridges exceeds the second threshold (90%) when attempting to retrieve an IW-bridge ID from the IW bridge manager.

In SN07, and later releases, a bridge pool field displays the related bridge pool name from the NETBRDGE table. This field appears on the log when the MULTINET_DISPLAY_ACTIVE field in the OFCVAR table is set to Y.

Format

The format for log report IWBM802 is as follows:

```
MSH10_I06BE *** IWBM802 APR22 09:58:57 5022      2nd Threshold Exceeded
          The number of interworking bridges in use has
          exceeded 90 percent of all bridges in the pool.
            Total number of IW_Bridges:        2016
            Number of available IW_Bridges:           0
            Bridge Pool: <bridge_pool_CLLI>
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

The IWBM NODE OM group provides IW SPM nodal bridge usage which may be summed to calculate the appropriate Bridge Pool usage.

Additional information

This log report requires no additional information.

IWBM803

Log report IWBM803 indicates that the number of available IW bridges falls to less than 85% of bridges in the pool in use. This log always occurs after IWBM802.

In SN07, and later releases, a bridge pool field displays the related bridge pool name from the NETBRDGE table. This field appears on the log when the MULTINET_DISPLAY_ACTIVE field in the OFCVAR table is set to Y.

Format

The format for log report IWBM803 is as follows:

```
MSH10_I06BE  ** IWBM803 APR22 09:59:17 5042      2nd Threshold Cleared
          The number of interworking bridges in use has
          fallen below 85 percent of all bridges in the pool.
            Total number of IW_Bridges:        2016
            Number of available IW_Bridges:        2016
            Bridge Pool: <bridge_pool_CLLI>
```

Selected field descriptions

This log report has no selected fields.

Action

This log report requires no action.

Associated OM registers

The IWBMNODE OM group provides individual IW SPM nodal bridge usage which may be summed to calculate the appropriate Bridge Pool usage.

Additional information

This log report requires no additional information.

SPM313

Log report SPM313 generates when a fault is recorded in the Module Information Memory (MIM) on an SPM.

Format

The format for log report SPM313 is as follows:

```
MSH10_I06BE ** SPM313 NOV26 09:30:24 1013 TBL Fault
SPM <nodenumber> <circuitpack> <circuitpackno>:<activity> Time:<timestamp>
Source: <source> State: <state> Type: <type>
Reason: <reason>
Diagnostic: <diagnostic>
Comp: <component> RegAddr:<registerOrAddress> Exp:<expected> Act:<actual>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
nodenumber	0 to 63	This field displays the SPM number.
circuitpack	CEM, OC3, DSP, and VSP	This field displays the circuit pack type.
circuitpackno	0 to 27	This field displays the circuit pack unit number.
activity	A, I	
timestamp		This field displays the local time when the fault occurred.
source		This field displays the source of the fault.
state		This field displays the state when the fault occurred.
type		This field indicates the type of fault.
reason		This field displays the reason of the fault.
diagnostic		This field displays the diagnostic string.
component		This field displays the component.
registerOrAddress		This field displays the register or address.

Field	Value	Description
expected		This field displays the expected value.
actual		This field displays the actual value.

Action

Check the reason given in the log and take corrective action if necessary. For the reason "CPK MAC address doesn't match prov. data," change the MAC datafill in table MNCKTPAK to match that on the physical card. If card replacement is necessary, perform the procedure for replacing a CEM circuit pack in NN10076-911, MG 4000 Fault Management. If you are unclear as to what action to take, 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.

SYNC202

The SYNC202 log report generates when the system detects a synchronization problem in an office in the base configuration.

The SYNC202 log is an information log generated to convey

- any change in clock state
- timing link status
- an update to the tuning control for the system clock

Format

The format for the SYNC202 log report is as follows:

```
SYNC202  mmmdd hh:mm:ss ssdd  INFO System CNFG: SYNC Info
   CLOCK <clock_no>   <mastership>   <sync_log_event>
   CLK0, CLK1:  State = <sst0>, <sst1>  Tuning Control = <dac0>, <dac1>
                Alarm = <alm0>, <alm1>
    LK0, LK1:   State = <tlk0>, <tlk1>  Slip Count = <tls0>, <tls1>
                Carrier = <cst0>, <cst1>
  <log_reason>
   System Fault: <system_fault_description>
   Timing Ref 0 Fault: <timing_ref_fault_description>
   Timing Ref 1 Fault: <timing_ref_fault_description>
   Internal Clock 0 Fault: <internal_fault_description>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
INFO System CNFG: SYNC Info	Fixed	Indicates the system detected a synchronization problem
CLOCK	Fixed	
clock_no	0 or 1	Identifies the plane number of the affected clock
mastership	Master Clock, Slave Clock	Indicates whether the affected clock is the master clock or the slave clock
sync_log_event	Text string	Identifies the clock synchronization event that caused the log report

Field	Value	Description
CLK0, CLK1	Fixed	Indicates the information in the next field is for clock 0 and clock 1
sst0, sst1	Free (free-running), Sync (synchronized), Lkng (linking)	Indicates the synchronization state of the message switch (MS) clocks
dac0, dac1	0000 to FFFF	indicates the tuning control values of the clocks. The values are shown as four-digit hexadecimal numbers.
Alarm =	Fixed	Indicates alarm information follows

Field	Value	Description
alm0, alm1	Htr, Pwr, Phse, Sub, Tun, Ext, Al0, Al1, Beat, MM, . (dot)	Identifies the alarms associated with the clocks. The alarm codes are as follows: • Htr indicates an internal oscillator heater fault • Pwr indicates the failure of a clock card power converter • Phse indicates a malfunction of the phase detector circuitry • Sub indicates a problem with the subsystem clock • Tun indicates the clock is almost out of its tuning range • Ext indicates the state of the clock in the master-external office is free running, or the external reference signal has failed • Al0 indicates the external reference oscillator has failed • Al1 indicates the power supply of the emergency reference oscillator has failed • Beat indicates the beat frequency period of the two external reference signals is too short • MM indicates a clock data mismatch between the CM and MS • A dot (.) indicates there is no alarm
LK0, LK1	Fixed	Indicates DS-1 synchronization link information follows ***Note:*** This entry appears in the log report only if field OFF_CONF in table SYNCLK is datafilled as SLAVE.

Field	Value	Description
tlk0, tlk1	Lck (locked), Smp (sampling), Idl (idle)	Indicates the state of the two DS-1 links used for synchronizing ***Note:*** This field appears in the log report only if field OFF_CONF in table SYNCLK is datafilled as SLAVE.
Slip Count	Fixed	Indicates slip count information follow ***Note:*** This entry appears in the log report only if field OFF_CONF in table SYNCLK is datafilled as SLAVE.
tls0, tls1	0 to 32, 768	Indicates the accumulated slip count for the timing link since the clock system was synchronized
	NA	In the case of SPM SRM (LX44AA) timing mode, indicates slip count is not available. ***Note:*** This field appears in the log report only if field OFF_CONF in table SYNCLK is datafilled as SLAVE.
Carrier =	Fixed	Indicates carrier state information follows ***Note:*** This entry appears in the log report only if field OFF_CONF in table SYNCLK is datafilled as SLAVE.

Field	Value	Description
cst0, cst1	MBsy, SBsy, OOS, . (dot)	Indicates the state of the carriers. The carrier states are as follows: • MBsy indicates the carrier is manual busy • SBsy indicates the carrier is system busy • OOS indicates the carrier is out of service • A dot (.) indicates the carrier is in service ***Note:*** This field appears in the log report only if field OFF_CONF in table SYNCLK is datafilled as SLAVE.
log_reason	Text string	Describes the fault that caused the log report to be generated
System Fault:	Fixed	Indicates fault descriptions follow
system_fault_description	Text string	Describes the current system synchronization faults
Timing Ref n Fault	Fixed except that n = 0 or 1	Indicates timing reference fault information follows
timing_ref_fault_description	Text string	Describes the timing reference faults
Internal Clock n Fault	Fixed except that n = 0 or 1	Indicates internal clock fault information follows
internal_fault_description	Text string	Describes the internal clock faults

Action

User actions for messages in the system_fault_description field:

User actions for messages in the system_fault_description field

Message	User action
Clock unable to sync within time limit	Contact the next level of support
Phase error limit exceeded	Contact the next level of support
Stuck phase comparator detected	Contact the next level of support
Sync central/Local data mismatch	Contact the next level of support
Sync/maintenance mastership mismatch	Contact the next level of support
Sync system dropped sync within the last hour	No action required
Sync system switched carrier within the last hour	No action required
Sync system master within the last hour	No action required

User actions for messages in the timing_ref_fault_description field:

User actions for messages in the timing_ref_fault_description field

Message	User action
Sample continuity check failed	Contact the next level of support
Sample continuity check warning	No action required
Sample maximum-minimum check warning	No action required
Sample maximum-minimum check failed	Contact the next level of support
Sample range check warning	No action required
Sample range check failed	Contact the next level of support
Samples timed out in central	No action required
Samples timed out in local	No action required
Slips reported on this link	No action required

User actions for messages in the timing_ref_fault_description field

Message	User action
Unable to make link active	Contact the next level of support
Unable to start link sampling	No action required

This log report requires no additional information.User actions for messages in the internal_fault_description field

User actions for messages in the internal_fault_description field

Message	User action
DAC read failures exceed threshold	No action required
DAC write failures exceed threshold	Contact the next level of support

Associated OM registers

None

Additional information

None

XNET607

Log report XNET607 indicates that an IW SPM interworking bridge was not available for the connection request due to:

- a bridge exhaust condition on one of the bridge pools being involved in the connection request
- bridges not in-service, or provisioned, for one of the bridge pools involved with the connection request

Format

The format for log report XNET607 is as follows:

```
XNET607  mmmdd hh:mm:ss ssdd  INFO  IW Bridge Not Available
   Bridge Pool:  <ntbrdg_pool>
    From Agent  : <conn_source>
    From Bearer Network  : <net_source>
    To Bearer Network  : <net_dest>
     Location   : <SPM node_no> Type: <spm_type> Fabric: <fabric_type>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
ntbrdg_pool	Text string	The name of the bridge pool, as specified in the NETBRDGE table, that has the ‘trouble’ condition.
conn_source	Alpha numeric	Identifies the source party of the connection request which can be: • a LEN and DN • a PM type and PM number • a Node number and TID (terminal id) when an appropriate device type and device id cannot be determined • an “Unavailable” indication when the connection source was an ENET hosted party, but that party can no longer be determined.

Field	Value	Description
net_source	Text string	The bearer network name of the source party, as datafilled in the BEARNETS table.
net_dest	Text string	The bearer network name of the connection destination party, as datafilled in the BEARNETS table.

Action

Perform as needed:

- check for IWBM602 logs indicating a bridge exhaust condition
- verify that the bridge pool identified in the log is provisioned on an SPM in the MNNODE table
- verify that the bridges in the bridge pool identified in the log are in-service.
- use the EXTLOGCI command to disable the XNET607 log
- use LOGUTIL to SUPPRESS the XNET607 log

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NODE300

Integrated Node Maintenance (INM) generates log report NODE300 when a trouble condition is present with the node. This report indicates INM recovery actions when the node state is system busy.

The resource maintenance manager (RMM) reports faults to the INM when the system executes the QueryPM faults command at the MAP display.

Format

The log report format for NODE300 is as follows:

```
NODE300 mmmdd hh:mm:ss ssdd INFO TBL Warning
  Location=<node>
  Status=<trouble_status>
  Trouble=<trouble_code>
  Action=<user_action>
  Integrated Node Maintenance Detailed Information
  Trouble Reason=<INM trouble condition reason>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
trouble_code	variable	Identifies the reason for the problem.
user_action	variable	Identifies the action to take.
INM trouble condition reason	variable	Provides a reason for the trouble condition.

Action

Check the trouble field. Take action as indicated in the user action field.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NODE303

Log report NODE303 is generated to report the Wrong Application Data on the SPM.

Format

The format for log report NODE303 is as follows:

```
MSH10_I05BK     NODE303 JAN30 14:43:11 0000 TBL  Wrong Application Data
        Location: SPM 2 Unit 1
         Trouble:  CEM has Application Data of Mate CEM
         Action :  Check LINK300 Logs & Re-Connect DS-512 Links Correctly
         Integrated Node Maintenance Detailed Information
         Trouble Reason:  DS-512 Link/Links may be misconnected
         Trouble Detail:  CEM in Slot 7 has Application Data of CEM 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.

NODE323

Integrated Node Maintenance (INM) generates log report NODE323 when a REx request does not execute.

Format

The log report format for NODE323 is as follows:

```
NODE323 mmmdd hh:mm:ss ssdd TBL REx Fault
  Location: <location>
  Status: <alarm_status>
  Trouble: <trouble>
  Action: <action>
  REX did not run
  Units: <units_not_RExed>
  Reason: <reason>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
location	character string	Indicates the location of the PM to which the event applies.
alarm_status	alarm raised	Indicates an alarmed log. ***Note:*** An alarmed log means that double stars at the beginning of the format highlight the log report. An alarmed log does not mean a MAP alarm is present.
trouble	character string	Identifies the reason for the problem.
action	character string	Indicates the trouble log is for information only.
units_not_RExed	0, 1, 0 and 1	Indicates the units that did not run the REx.
reason	character string	Indicates the reason the REx did not run.

Action

Clear the reason that did not allow the REx to run. This reason can require a manual maintenance action or a waiting period for a system operation to clear a trouble condition. 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.

NODE326

Log report NODE326 indicates a hardware fault.

Format

The format for log report NODE326 is as follows:

```
MSH10_I06BE    NODE326 APR21 14:09:52 7606 TBL Hardware Fault
               Location: SPM 7 Unit 0
               Status: Alarm raised
               Trouble: Card fault
               Action: Restore communication with the Resource Processor
               Activity: I
                Integrated Detail Node Maintenance Information
               Trouble Reason: Loadname mismatch
               Trouble Detail: Link isolation condition
               Location: SPM 7  Type: SMG4      Fabric: ATM
```

Selected field descriptions

This log report has no selected fields.

Action

For a raised alarm, follow the recommended action.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NODE450

Integrated Node Maintenance (INM) generates log report NODE450 to summarize a series of event reports under one log header during a routine exercise (REX) test. The NODE450 log is never in alarm mode. This log is an abbreviated summary of the routine series of operations that compose a REX test.

The system reports all trouble events (faults) as separate logs to make them more accessible to mechanized downstream analysis. High priority events are logged as the events reach the central log system. Other events are logged following the generation of NODE450. Events of the INITIATE class appear only in NODE450, and never as separate logs.

Format

The log report formats for NODE450 are as follows:

Format 1

```
NODE450 mmmdd hh:mm:ss ssdd SUMM REX TEST SUMMARY
  Location: <entity name>
  Summary: REX Test Sequence Successful
```

Format 2

```
NODE450 mmmdd hh:mm:ss ssdd SUMM REX TEST SUMMARY
  Location: <entity name>
  Summary: REX Test Sequence Failed
  TIME            EVENT
  <hh:mm:ss>      <detailed event type>
  <hh:mm:ss>      <detailed event type>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	Symbolic text	Indicates the name of the hardware or software component or service involved.
Summary	REX Test Sequence Successful or REX Test Sequence Failed	Indicates success or failure of the REX test.
TIME	Integers	If REX test failed, indicates the time (hh:mm:ss).
EVENT	Symbolic text	If REX test failed, indicates the event.

Action

The NODE 450 log report helps log analysis by bringing together related events in one report, in the correct time sequence. The action required, if any, depends on the nature of the repeated events.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

NODE500

Log report NODE500 indicates a system node state change. Correlates to a SYSB alarm.

Format

The format for log report NODE500 is as follows:

```
MSH10_I06BE     NODE500 APR21 12:52:00 4563 INFO Node State Change
        Location: SPM 6 Unit 1
        From:     ISTb ( Connected, Active )
          To:     InSv ( Connected, Active )
```

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.

NODE600

Log report NODE600 indicates an INFO log that notifies a system recovery action.

Format

The format for log report NODE600 is as follows:

```
MSH10_I06BR     NODE600 JAN01 01:50:49 2496 INFO System Recovery Action
        Location: SPM 2 Unit 1
         System recovery is in progress
         Integrated Node Maintenance Detailed Information
                  INM SNEGO trigger received
                  Information for analysis, no immediate action required
```

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.

PM703

Log report PM703 is generated through the peripheral module (PM). This log records the time that an automated PM upgrade task failed. It also records the completion or failure of each node that the system upgrades during a task.

Format

The format for log report PM703 is as follows:

```
PM703 mmmdd hh:mm:ss ssdd INFO PM Upgrade
   TASK: <id> Report <cur_report> of <max_report>
   AUTOMATED:    <automation_flag>
   STATUS:       <status>
   NODES:        <node_name>
   LOADS:        <load_name>
   PATCHES FOR   <load_name>:
                 <patch_name>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value		Description
id	integer		Indicates the PM upgrade task
cur_report	integer		Indicates the number of this log report associated with the start of a task
max_report	integer		Indicates the total number of log reports associated with the start of a task
automation_flag	YES	NO	Indicates if the task is automated
status	FAILED	FAILED	Indicates the status of the task that is not successful
	(INTERNAL SYSTEM ERROR)		
	ABORTED	NOT	
	ATTEMPTED	NOT	
	SUPPORTED	UNKNOWN	
	RETURN CODE		

Field	Value	Description
node_name	text string of the format node_type site node_id	Indicates the type of node, the site of the node, and the number of the node. Site is an optional value.
load_name	text string	Indicates the name of the load associated with the task.
patch_name	text string	Indicates the patches associated with each load in the task. The patch heading is not displayed when the task does not have patches.

Action

If the upgrade task fails, examine the nodes that failed. The nodes can have a maintenance problem that does not relate to the PM upgrade. Troubleshoot the problem or 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.

VOIP800

The VOIP800 log indicates that a network traffic parameter has exceeded the threshold set by data network management personnel in table MNIPPARM.

Format

The format for log report VOIP800 is as follows:

```
VOIP800 May05 11:48:14 3100 INFO GEM RM Threshold Exceed
Location: SPM 2          Slot num: 10
Description: GEM has Lost Packets
statistic:              99   threshold:          50
interval:               10   pack_volum:    1276791
octet_volum:    277340435    voice_volum:        80
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Description	The value may consist of any of the following: • Cyclical Redundancy Check (CRC) alignment error • Undersize packets • Oversize packets • Fragments • Jabber • Drop events • Broadcast packets • Jitter • Latency • Packets lost • Decoder under run	The IW SPM IP system generates the VOIP800 log for a variety of reasons. The Description field indicates the reason for the log.
statistic	Integer	Highest percentage of RTP packet loss from any call during the 5 minute logging interval.
threshold	Integer	Value of the VPKTLOST parameter in the MNIPPARM table.
interval	Integer	Interval number.
pack_volum	Integer	Total number of packets during the interval.

Field	Value	Description
octet_volum	Integer	Total number of bytes during the interval.
voice_volum	Integer	Total number of RTP (voice) packets during the interval.

Action

Contact your data network management personnel.

Data network management personnel must monitor the IP network for conditions specific to the issue reported by the log (such as packets lost, or latency) and inspect and validate network traffic while the logs are generated. If the network continues to perform at acceptable levels, adjust the parameters in table MNIPPARM until the VOIP800 logs no longer appear.

This log is also generated when a gigabit ethernet module (GEM) switch of activity (SWACT) occurs with traffic over IW SPM IP nodes. Calls are not affected in this situation and no action is required.

Associated OM registers

Associated OM registers are MNGEMLNK and MNGEMTRE.

Additional information

The VOIP800 log displays the statistics of the call that experience the worst RTP packet loss during the 5 minute monitoring period.

IPOA301

Log report IPOA301 indicates loss of cell delineation (LCD). All messages on the link are lost.

The SAM21 Platform generates log report IPOA301.

Format

The format for log report IPOA301 is as follows:

```
OFC_NAME  *** IPOA301 JUL30 10:50:52 5423 CRIT FLT  ATM Interface Fault
   Location: sam21 1:CSAM01-02
   SC Slot: 9
   Fault Type: LCD (Loss of Cell Delineation)
   Fault Date: Tue Jul 30 09:29:29 EST 2002
```

Selected field descriptions

This log report has no selected fields.

Action

The situation clears when ATM cell delineation recovers.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IPOA302

Log report IPOA302 indicates a SONET Alarm indication signal (AIS) alarm. This alarm is raised against the line or the path. The SONET layer link between this node and the far end node is broken.

The SAM21 Platform generates log report IPOA302.

Format

The format for log report IPOA302 is as follows:

```
OFC_NAME *** IPOA302 JUL30 10:50:52 5423 CRIT FLT SONET Carrier Fault Raised
      Location: sam21 1:CSAM01-02
      SC Slot: 9
      Carrier Type: STS3CP
      Fault Type: AIS (Alarm Indication Signal)
      Fault Date: Tue Jul 30 08:09:54 EST 2002
```

Selected field descriptions

This log report has no selected fields.

Action

Check the fibers and connections between this node and the far end node.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IPOA303

Log report IPOA303 indicates an ATM connection fault. Virtual circuits (VC) associated with the affected carrier are lost. Only messages on the affected VCs are lost. The entire link is not necessarily affected. An ATM AIS alarm (not a SONET AIS alarm) is raised against the VCs. CC failure indicates continuity-check failure.

The SAM21 Platform generates log report IPOA303.

Format

The format for log report IPOA303 is as follows:

```
OFC_NAME  *** IPOA303 JUL30 10:50:52 5423 CRIT FLT  ATM Connecta
   Location: sam21 1:CSAM01-02
   SC Slot: 9
   Carrier Type: STS3CP
   Fault Type: CC Failure
   Fault Date: Tue Jul 30 08:09:54 EST 2002
```

Selected field descriptions

This log report has no selected fields.

Action

Check the connection member states at the ATM connections window.

If the alarms are raised against the link, check the fibers and connections between this node and the far end node.

If the alarms are not raised against the link, check VC provisioning at this node and the far end node.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IPOA304

Log report IPOA304 indicates connection members changed state and neither the active or inactive is available.

The SAM21 Platform generates log report IPOA304.

Format

The format for log report IPOA304 is as follows:

```
OFC_NAME  *** IPOA304 JUL30 10:50:52 5423 CRIT FLT  Alarm Raised
        Location: sam21 1:CSAM01-02:Connection Set:CC10 OAMP
        Time: Tue Jul 30 10:50:52 EST 2005
        Reason: ACT CM: FROM:Up TO:Up  INACT CM: FROM:Up To:Redi
        Category:communications
        Cause:performanceDegraded
```

Selected field descriptions

This log report has no selected fields.

Action

This log clears automatically when the connection members recover.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IPOA305

Log report IPOA305 indicates an ATM interface capacity threshold was crossed. Thresholds and severities are listed below:

- 70% - minor
- 80% - major
- 90% - critical

Format

The format for log report IPOA305 is as follows:

```
OFC_NAME *** IPOA305 JUN13 13:39:13 0184 CRIT FLT   Alarm Raised
   Location: SAM21 -0 0:CSAM00-00:shelf 1:slot 7:card 1:card ATMCard0
   Time: Fri Jun 13 08:39:24 EDT 2005
   Reason: 90% of ATM Capacity Reached
   Category:communications
   Cause:performanceDegraded
```

Selected field descriptions

This log report has no selected fields.

Action

Contact engineering to determine if traffic can be distributed differently or if additional capacity is needed.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

IPOA801

Log report IPOA801 indicates an ATM CRC32 threshold exceeded. A CRC calculation mismatch occurred on a cell and the cell was discarded.

The SAM21 Platform generates log report IPOA801.

Format

The format for log report IPOA801 is as follows:

```
OFC_NAME    * IPOA801 JUL30 10:50:52 5423 MINOR FLT ATM CRC32 Threshold
   Location: sam21 1:CSAM01-02
   SC Slot: 9
   Connection Set: CC04 Call Control
   Fault Date: Tue Jul 30 09:31:02 EST 2002
   Threshold: 37
```

Selected field descriptions

This log report has no selected fields.

Action

Check the fiber for dirt, misinsertion, and tight loops.

Check the ATM interfaces for failures or dirt.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU301

Log report SCU301 indicates the Extension Bridge in Slot 15/16 is Down/Up. One or both of the Extension Bridges has been delatched and/or removed.

The SAM21 Platform generates log report SCU301.

Format

The format for log report SCU301 is as follows:

```
OFC_NAME  *** SCU301 JUL30 10:50:52 5423 MAJOR FLT   Alarm Raised
        Location: sam21 1:CSAM01-02:shelf 1:slot 9:card 1
        Time: Thu Jul 30 10:50:45 EST 2005
        Reason: Extension Bridge in Slot 15 is Up, Extension
                Bridge in Slot 16 is Down
        Category:processingError
        Cause:adapterError
```

Selected field descriptions

This log report has no selected fields.

Action

Critical.

Check the Extension Bridges in slots 15 back and 16 back on the rear of the SAM21 shelf are seated. If the alarm persists, replace the failing extension bridge.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU306

Log report SCU306 indicates that the NFS Mount, GWC, 3PC, STORM and SAM21 fail.

Format

The format for log report SCU306 is as follows:

```
OFC_NAME    ** SCU306 JUL30 17:48:52 5000 MAJOR FLT    Alarm Raised
             Location: sam21 1:CSAM01-02:shelf 1:slot 9:card 1
             Time: Thu Feb 10 16:55:32 EST 2005
             Reason: NFS Mount gwc and sam21 fail
             Category:processingError
             Cause:communicationsSystemFailure
```

Selected field descriptions

This log report has no selected fields.

Action

Verify that the server is reachable and that the directories are exported.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU310

Log report SCU310 indicates that the CPU load is high. The severity is major if the one minute load average is greater than 20. It is critical if the five-minute load average is above 15 or the 15-minute load average is above seven.

The SAM21 Platform generates log report SCU310.

Format

The format for log report SCU310 is as follows:

```
OFC_NAME  *** SCU310 JUL30 17:48:52 5000 CRIT FLT     Alarm Raised
        Location: sam21 1:CSAM01-02:shelf 1:slot 9:card 1
        Time: Thu Jul 30 17:48:45 EST 2005
        Reason: CPU load high. One Minute Load is 16.92
        Category:equipment
        Cause:cpuCyclesLimitExceeded
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Reason	Range	See this field for the load average.

Action

If condition persists, ensure the Shelf Controller (SC) card is in an inactive state and then lock and unlock the SC card.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU315

Log report SCU315 indicates problems with temperature or temperature control in a sled, or that a diagnostic failed.

The SAM21 Platform generates log report SCU315.

Format

The format for log report SCU315 is as follows:

```
OFC_NAME   ** SCU315 JUL30 17:48:52 5000 MAJOR FLT    Alarm Raised
        Location: sam21 1:CSAM01-02:sled 1
        Time: Thu Jul 30 17:48:45 EST 2005
        Reason: Fan in Sled 1 is down
        Category:equipment
        Cause:equipmentMalfunction
```

Selected field descriptions

This log report has no selected fields.

Action

Critical

If the fan has failed, check the cables connecting the fan to the power supply. Replace the fan or replace the sled if the problem persists.

If the log indicates that the temperature in the sled has reached about 50 degrees, Check for blockage, and ambient heat.

Major

A diagnostic was run and the board failed at least one of the tests, replace the board.

If a diagnostic was interrupted by a SWACT, re-run the diagnostic.

If the diagnostic failed (eleven possible reasons), re-run the diagnostic. If the fault persists, call Technical Support.

If the fan has been removed from the sled, or the entire sled has been removed, re-insert the fan or sled. Replace if the problem persists.

If the log indicates that the temperature in the sled has reached about 40 degrees, Check for blockage, and ambient heat.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU329

Log report SCU329 indicates a loss of shelf controller communications. The severity can be minor, major, or critical, depending on the cause of the fault.

The SAM21 Platform generates log report SCU329.

Format

The format for log report SCU329 is as follows:

```
OFC_NAME  *** SCU329 JUL30 17:48:52 5000 CRIT FLT    Alarm Raised
        Location: sam21 1:CSAM01-02:shelf 1:slot 9:card 1
        Time: Thu Jul 30 17:48:45 EST 2005
        Reason: Loss of Communications: Mate Ethernet, Serial
                Connection 1, Serial Connection 2 is down or unreachable
        Category:communications
        Cause:lossOfSignal
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Reason	Serial connection (#) Mate Ethernet; Remote Network; ISCS; Local Ethernet Interface; combination	This field identifies the entity or entities causing the loss of communication.

Action

Critical faults

Mate Ethernet, Serial Connection 1, Serial Connection 2 are down (Active SC only) are down. Both the lower and upper serial cables and the mate's Ethernet are not connected. Verify cables, lock and unlock inactive Shelf Controller.

Mate Ethernet, ISCS, Serial Connection 1, Serial Connection 2 are down (Active SC only). Both the lower and upper serial cables and the mate's Ethernet are not connected. Verify cables.

Local Ethernet Interface is down (Inactive SC only). Shelf can not ping its mate or the SDM through the Ethernet interface. Verify cable.

Local Ethernet Interface, Serial Connection 1 is down (Inactive SC only). Both Ethernet interface and the upper serial cable connection are down. Verify cables.

Local Ethernet Interface, Serial Connection 2 is down (Inactive SC only). Both Ethernet interface and the upper serial cable connection are down. Verify cables.

Local Ethernet Interface, ISCS, Serial Connection 2 is down (Inactive SC only). Both Ethernet interface and the upper serial cable connect ion are down. Verify cables.

All Communication Paths Down (Inactive SC only). The shelf can not see out at all. In reality no one will ever see this alarm from SAM21 EM. Verify cables and Accelar switch.

Major faults

Serial Connection 1, Serial Connection 2 is down. The upper and lower serial cable connections are down. Verify connection of cables in the back.

Mate Ethernet is Down (Active SC only). The upper and lower serial cable connections are down. Verify connection of cables in the back.

Mate Ethernet is Down (Active SC only). This shelf controller can not ping its mate through the ethernet interface. Verify ethernet cable for shelf controller.

Remote Network is Down (Inactive SC only). The shelf controller can not ping the SDM, but can ping its mate. Route table on Shelf is probably bad, or SDM is unreachable.

Mate Ethernet, Serial Connection 1 is down (Active SC only). Both the lower (upper) serial cable and the mate's Ethernet are not connected. Verify cables.

Mate Ethernet, Serial Connection 2 is down (Active SC only). Both the lower serial cable and the mate's Ethernet are not connected. Verify cables.

ISCS, Mate Ethernet, Serial Connection 2 is down (Active SC only). Both the lower serial cable and the mate's Ethernet are not connected. Verify cables.

Remote Network, Serial Connection 1(2) is down (Inactive SC only). The shelf controller can not ping the SDM, but can ping its mate. The upper (lower) serial cable connection is down. Verify cables.

Remote Network, Serial Connection 1, Serial Connection 2 is down (Inactive SC only). Both serial cable connections are down. Verify cables.

Loss of Communications: Boot Server is down or unreachable. Verify IP of the boot server, or check to see if SDM or CBM is alive or not.

Minor faults

Serial Connection 1(2) is down. The upper (lower) serial cable connection is down. Verify connection of cables in the back.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU332

Log report SCU332 indicates that the memory usage is high. The severity is major if the total free memory has fallen below 15%. It is critical if the total free memory has fallen below 10%.

The SAM21 Platform generates log report SCU332.

Format

The format for log report SCU332 is as follows:

```
OFC_NAME   ** SCU332 JUL30 17:48:52 5000 CRIT FLT    Alarm Raised
        Location: sam21 1:CSAM01-02:shelf 1:slot 9:card 1
        Time: Thu Jul 30 17:48:45 EST 2005
        Reason: Memory usage high. Less than 12 Percent free.
        Category:equipment
        Cause:outOfMemory
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Reason	Range	See this field for the % of free memory.

Action

If the condition persists and reaches critical severity, ensure the SC card is in an inactive state and then lock and unlock the SC card.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU335

Log report SCU335 indicates problems with power.

The SAM21 Platform generates log report SCU335.

Format

The format for log report SCU335 is as follows:

```
OFC_NAME  *** SCU335 JUL30 17:48:52 5000 CRIT FLT    Alarm Raised
        Location: sam21 1:CSAM01-02:powerfeed A
        Time: Thu Jul 30 17:48:45 EST 2005
        Reason: Power Feed A is down
        Category:processingError
        Cause:powerProblem
```

Selected field descriptions

This log report has no selected fields.

Action

Critical

The Power Supply in Sled 1/2/3 has failed. Re-insert the sled. Replace if the problem persists.

Power Feed 1/2 is down. Either the feed has failed, or the cable has been removed. Check power cables in back. Be careful, significant power is passing through the cables.

Major

The Power Supply in Sled 1/2/3 has been removed. Re-insert the sled. Replace if the problem persists.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU344

Log report SCU344 indicates that a lock or unlock request at the CS 2000 SAM21 Manager client has taken longer than 3 minutes to complete. A major alarm is raised against the shelf in addition to the log report.

Format

The format for log report SCU344 is as follows:

```
OFC_NAME   ** SCU344 JUL30 17:48:52 5000 MAJOR FLT   Alarm Raised
        Location: sam21 1:CSAM01-02:shelf 1:slot12:card 1
        Time: Thu Jul 30 17:48:45 EST 2005
        Reason: Unlock action exceeded expected duration. Please
                check the state window for errors
        Category:qualityOfService
        Cause:responseTimeExcessive
```

Selected field descriptions

This log report has no selected fields.

Action

Monitor the request from the States tab of the Card View window at the CS 2000 SAM21 Manager. The alarm clears when the card completes the request or the card is reseated in the shelf.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU346

Log report SCU346 indicates that many processes have abnormally terminated or there is a problem with firmware flashing. The severity can be critical or major.

The SAM21 Platform generates log report SCU346.

Format

The format for log report SCU346 is as follows:

```
OFC_NAME   ** SCU346 JUL30 17:48:52 5000 CRIT FLT    Alarm Raised
        Location: sam21 1:CSAM01-02:shelf 1:slot 2:card 1
        Time: Thu Jul 30 17:48:45 EST 2005
        Reason: Large Number of Processes Abnormally Terminated
        Category:processingError
        Cause:softwareError
```

Selected field descriptions

This log report has no selected fields.

Action

Critical

If the log indicates processes have abnormally terminated and critical severity, ensure the SC card is an inactive state and then lock and unlock the SC card.

If firmware Flashing could not connect to the board, either there is another process currently attached to the board, or the bus is too busy to allow the request. Auto Flash is now turned off on the Shelf Controller for this slot. You must resend the provisioning information to flash again.

If Firmware Flashing failed at downloading firmware, then the firmware file does not exist on the SDM, or has incorrect parameters. Check Firmware file on SDM. You must resend the provisioning information to flash again.

If Firmware Flashing failed at validating firmware, then the firmware file is corrupt on the SDM, or there was an error in the transfer. Check Firmware file on SDM. Try re-applying fileset. You must resend the provisioning information to flash again.

If Firmware Flashing failed at backing up firmware, then the copy operation from one bank to the other failed. Possible bad memory. If the condition persists, replace the board.

If Firmware Flashing failed flash, remove and re-insert the board. If the condition persists, replace the board. You may want to consider dis-allowing flash on the other boards of this type. Auto Flash is now turned off on the Shelf Con-troller for this slot. You must resend the provisioning information.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU348

Log report SCU348 indicates that provisioning of the board failed due to some system problem. The system may have been abnormally busy.

The SAM21 Platform generates log report SCU348.

Format

The format for log report SCU348 is as follows:

```
OFC_NAME  *** SCU348 JUL30 17:48:52 5000 CRIT FLT    Alarm Raised
        Location: sam21 1:CSAM01-02:shelf 1:slot 1:card 1
        Time: Thu Jul 30 17:48:45 EST 2005
        Reason: Provisioning failed, connection lost
                unexpectedly, please reseat/replace the card
        Category:processingError
        Cause:softwareProgramError
```

Selected field descriptions

This log report has no selected fields.

Action

Critical

Re-attempt provisioning. If the problem persist and this is the only board in the chassis that is having difficulty, replace the board.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU349

Log report SCU349 indicates that disk usage is high. The severity is major if the total free space on the root file system has fallen below 10%. It is critical if the total free space on the root file system has fallen below 5%.

The SAM21 Platform generates log report SCU349.

Format

The format for log report SCU349 is as follows:

```
OFC_NAME   ** SCU349 JUL30 17:48:52 5000 CRIT FLT    Alarm Raised
        Location: sam21 1:CSAM01-02:shelf 1:slot 9:card 1
        Time: Thu Jul 30 17:48:45 EST 2005
        Reason: Disk usage high. Root file system has 4.96
                Percent free space
        Category:equipment
        Cause:storageCapacityProblem
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Reason	Range	See this field for the % of free disk space.

Action

If the condition persists and reaches critical severity, ensure the SC card is in an inactive state and then lock and unlock the SC card.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU356

Log report SCU356 indicates that the mate shelf controller is down and the system is operating in simplex mode. The inactive SC has been delatched, or Mama on the active has not received a ping from the inactive in 20 seconds. The log can also indicate that the application is out of service or is being recovered.

The SAM21 Platform generates log report SCU356.

Format

The format for log report SCU356 is as follows:

```
OFC_NAME  *** SCU356 JUL30 17:48:52 5000 CRIT FLT        Alarm Raised
        Location: sam21 1:CSAM01-02:shelf 1:slot 7:card 1
        Time: Thu Jul 30 17:48:45 EST 2005
        Reason: Mate Shelf Controller Unavailable. Operating in Simplex.
        Category:equipment
        Cause:underlyingResourceUnavailable
```

Selected field descriptions

This log report has no selected fields.

Action

Critical faults

Mate Shelf Controller Unavailable. Operating in Simplex. Check the latch on the inactive SC. If the alarm persists, lock and unlock the inactive SC. If you are unable to Unlock the mate controller, contact Nortel support personnel.

Major faults

Application is out of service. Unlock the NSS card.

Application is out of service and being recovered. The application is already being recovered when the alarm is raised. The alarm clears automatically and no action is required.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU398

Log report SCU398 indicates that a TELCO alarm is raised at the SAM21 shelf.

Format

The format for log report SCU398 is as follows:

```
OFC_NAME  *** SCU398 JUL30 10:50:52 5423 CRIT FLT    Alarm Raised
        Location: sam21 1:CSAM01-02
        Time: Thu Jul 30 10:50:45 EST 2005
        Reason: Alarm condition on shelf
        Category:equipment
        Cause:equipmentMalfunction
```

Selected field descriptions

This log report has no selected fields.

Action

Determine the reason for the alarm at the CS 2000 SAM21 Manager alarm browser. If the reason for the alarm is not available at the CS 2000 SAM21 Manager, investigate the alarm at the SAM21 shelf.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU399

Log report SCU399 indicates that communication between the Shelf Controllers and the CS 2000 SAM21 Manager server application is unavailable. The CS 2000 SAM21 Manager client exits when communication between the Shelf Controllers and the CS 2000 SAM21 Manager server is unavailable.

Format

The format for log report SCU399 is as follows:

```
OFC_NAME  *** SCU399 JUL30 17:48:52 5000 CRIT FLT     Alarm Raised
        Location: sam21 1:CSAM01-02
        Time: Thu Jul 30 17:48:45 EST 2005
        Reason: Remote Node Communication Failure
        Category:communications
        Cause:unknownCause
```

Selected field descriptions

This log report has no selected fields.

Action

Verify Ethernet connectivity and router configuration between the host that provides the CS 2000 SAM21 Manager server application and the Shelf Controllers.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SCU500

Log report SCU500 indicates a change in state of a card. The new state can be Unlocked, Enabled, or None.

Format

The format for log report SCU500 is as follows:

```
MSH10_I06BR      SCU500  JUN5 14:14:09 2175 INFO  State Change
        Location:   SAM21 -0 0:CSAM00-00:shelf 1:slot 2:card 1
        New state:  Unlocked/Disabled/None
```

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.

SCU501

Log report SCU501 indicates an equipment insertion specifying the shelf, card, and slot.

Format

The format for log report SCU501 is as follows:

```
MSH10_I06BE      SCU501 APR28 14:35:11 4060 INFO  Card Insertion
        Location:  SAM21 -0 0:CSAM00-00:shelf 1:slot 5
```

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.

SCU502

Log report SCU502 indicates an equipment removal specifying the shelf, card, and slot.

Format

The format for log report SCU502 is as follows:

```
MSH10_I06BE      SCU502 APR28 14:34:50 4059 INFO  Card Removal
        Location:  SAM21 -0 0:CSAM00-00:shelf 1:slot 5:card 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.

STM300

The STORage Management (STM) unit generates an STM300 log report to indicate a fault with the fiber channel connection between the STORM cPCI unit and the RAID device.

Format

The log report format for STM300 is as follows:

```
STM300 *** FEB14 11:52:33 0135 CRIT Fault
       Status: Alarm raised
       Reason: Fibre channel link is down.
```

Selected field descriptions

This log report has no field descriptions.

Action

Refer to Communication:Communications subsystems failure alarm.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STM301

The STORage Management (STM) unit generates an STM301 log report to indicate a disk related fault.

Format

The log report format for STM301 is as follows:

```
STM301   * FEB14 11:52:33 0135 MINOR INIT
       Array: '/dev/md1' (stormvg)
       Status: Array is currently being rebuilt.
```

Selected field descriptions

This log report has no field descriptions.

Action

Refer to Equipment:Performance degraded alarm.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STM302

The STORage Management (STM) unit generates an STM302 log report to indicate a hardware fault.

Format

The log report format for STM302 is as follows:

```
STM302  ** FEB14 11:52:33 0135 MAJ Fail
       Power control fault detected. Power
       subsystem fault detected.
```

Selected field descriptions

This log report has no field descriptions.

Action

Refer to Equipment:Equipment malfunction alarm.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STM800

The STORage Management (STM) unit generates an STM800 log report to indicate that the CPU load average exceeds expected levels or that the CPU load average has returned to expected levels.

Format

The log report format for STM800 is as follows:

```
STM800   * FEB14 11:52:33 0135 THR  Threshold exceeded
       Status: Alarm raised. One minute load
       average is 14.32. One minute load
       threshold is 14.00.
```

Selected field descriptions

This log report has no field descriptions.

Action

Refer to Quality of service:Threshold Crossed alarm section CPU usage.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STM801

The STORage Management (STM) unit generates an STM801 log report to indicate that memory usage has crossed a threshold.

Format

The log report format for STM801 is as follows:

```
STM801 *** FEB14 11:52:33 0135 CRIT Threshold exceeded
       Status: Alarm raised. Used memory percentage is
       x.xx. Critical alarm threshold value is y.yy.
```

Selected field descriptions

This log report has no field descriptions.

Action

Refer to Quality of service:Threshold Crossed alarm section Memory usage.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STM802

The STORage Management (STM) unit generates an STM802 log report to indicate that filesystem usage has crossed a threshold or a filesystem has a fault.

Format

The log report format for STM802 is as follows:

```
STM802 *** FEB14 11:52:33 0135 CRIT Threshold exceeded
       Status: Alarm raised. Filesystem is < / >.
       Used filesystem percentage is x.xx. Critical
       alarm threshold is yy.yy.

STM802   * DEC11 09:41:03 2345 MIN Filesystem error
       Status: Alarm raised. Filesystem is < / >.
       Test results: Stat (Success) CreateDir(Success)
       CreateFile(Success) WriteFile(No space left
       on device) ReadFile(Success) RemoveFile(Success)
       RemoveDir(Success)
```

Selected field descriptions

This log report has no field descriptions.

Action

Refer to Quality of service:Threshold Crossed alarm section Filesystem usage.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

STM803

The STORage Management (STM) unit generates an STM803 log report to indicate that the number of zombie processes has crossed a threshold.

Format

The log report format for STM802 is as follows:

```
STM803 *** FEB14 11:52:33 0135 CRIT Threshold exceeded
       Status: Alarm raised. Number of zombie(s) is x.
       Critical alarm threshold is y.
```

Selected field descriptions

This log report has no field descriptions.

Action

Refer to Quality of service:Threshold Crossed alarm section Zombie processes.

Associated OM registers

This log report has no associated OM registers.

Additional information

This log report requires no additional information.

SOCK525

Log report SOCK525 indicates that the SOCKS program has been started manually.

The SOCKS service generates log report SOCK525 when it is started.

Format

The format for log report SOCK525 is as follows:

```
MSH10 ** SOCK525 SEP09 15:13:35 1009 INFO SOCKS started
         The SOCKS service has been started using port 10080
```

Action

No action is required for this log report.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

SOCK526

Log report SOCK526 indicates that the SOCKS program has been stopped manually.

The SOCKS service generates log report SOCK526 when it is stopped.

Format

The format for log report SOCK526 is as follows:

```
MSH10 ** SOCK526 SEP09 16:19:04 1635 INFO SOCKS stopped
         The SOCKS service has been stopped.
```

Action

No action is required for this log report.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

SPFS310

Log report SPFS310 indicates one of the following events:

- loss of network connectivity
- fan failure
- disk failure
- high temperature
- power supply unit failure
- cluster node failover
- cluster node out of sync

Note: Log report SPFS310 also indicates when any of the above events is cleared.

Format

The format for log report SPFS310 is as follows:

```
**SPFS310 JUL17 22:20:05 0805 Alarm raised or updated
 Location: SSPFS - <host>
 Time: Thu Jul 17 22:20:05 EDT 2003
 Category: Equipment
 Cause: <character string>
 ProbableCause: <character string>
 Component ID: <alphanumerical string>
 Description: <character string>
 Recovery Action: <character string>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	SPFS followed by a character string	Indicates the host name of the SPFS-based server the log applies to.
Category	Equipment or Hardware	Indicates the log category.

Field	Value	Description
Cause	character string	Indicates the reason the log was raised, which can be any one of the following: • network interface down • fan failure • disk failure • temperature threshold exceeded • PSU input unavailable • cluster node failed over • cluster nodes out of sync
Probable cause	character string	Indicates the probable cause of the error.
component ID	character string	Indicates the component for which the log was raised or cleared.
description	character string	Indicates a brief description of why the log was raised or cleared.
recovery action	character string	Indicates the corrective action.

Action

The following table lists the causes and suggested actions:

Cause	Suggested action
Loss of network connectivity.	Check the Ethernet cable. Contact the next level of support if necessary.
Fan failure.	Check the fan. If required, replace the fan using the document that came with your server. Contact the next level of support if necessary.

Cause	Suggested action
Disk failure.	Check the disk. If required, replace the disk using procedure "Replacing a failed disk drive in-service" in the ATM/IP Solution-level Fault Management document, NN10408-900. Contact the next level of support if necessary.
Temperature threshold exceeded.	Reduce the temperature of the environment.
Power supply unit failure	Check the power supply unit. If required, replace the PSU using the document that came with your server. Contact the next level of support if necessary.
Cluster node failover	None.
Cluster node out of sync	Contact the next level of support.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

SPFS320

Log report SPFS320 indicates when an automated data backup has failed, and when an automated data backup failure has cleared.

Format

The format for log report SPFS320 is as follows:

```
SPFS320 JUL17 22:20:05 0000 MINOR TBL Alarm raised or updated
Location: SSPFS - <host>
Time: Thu Jul 17 22:20:05 EDT 2003
Category: Data Backup
Cause: Drive/Media error
ProbableCause: Drive not ready or invalid media
Component ID: SSPFS_BKUP
Description: Data Backup Failure
```

Selected field descriptions

This log report has no selected fields.

Action

When the log indicates that the data backup failed, ensure the correct media is in the drive.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

SPFS330

Log report SPFS330 indicates when there is no active cluster node.

Format

The format for log report SPFS330 is as follows:

```
**SPFS330 JUL17 22:20:05 0093 TBL SPFSHA Warning:
No active cluster node.
User intervention required!
```

When the alarm has cleared, the format for log report SPFS330 is as follows:

```
**SPFS330 JUL17 23:00:05 0093 TBL SPFSHA
<host>  cluster started on <host>-unit<n>
```

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

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

SPFS350

Log report SPFS350 indicates one of the following events:

- File system not mounted
- File system usage threshold exceeded
- File system read/write check failed
- File system read failed
- CPU load threshold exceeded
- swap space usage threshold exceeded
- memory usage threshold exceeded
- password expiration

Note: Log report SPFS350 also indicates when any of the above events is cleared.

Format

The format for log report SPFS350 is as follows:

```
**SPFS350 JUL17 22:20:05 0805 TBL Alarm raised or updated
 Location: SSPFS - <host>
 Time: Thu Jul 17 22:20:05 EDT 2003
 Category: QualityOfService
 Cause: <character string>
 ProbableCause: <character string>
 Component ID: <alphanumerical string>
 Description: <character string>
 Recovery Action: <character string>
```

Selected field descriptions

The following table explains selected fields in the log report:

Field	Value	Description
Location	SPFS followed by a character string	Indicates the host name of the SPFS-based server the log applies to.

Field	Value	Description
Cause	character string	Indicates the reason the log was raised, which can be any one of the following: • file system not mounted • file system usage threshold exceeded • file system write failed • file system read failed • CPU load average threshold exceeded • swap space usage threshold exceeded • memory usage threshold exceeded • password expiration
Probable cause	character string	Indicates the probable cause of the error.
component ID	character string	Indicates the component for which the log was raised or cleared.
description	character string	Indicates a brief description of why the log was raised or cleared.
recovery action	character string	Indicates the corrective action.

Action

The following table lists the causes and suggested actions:

Cause	Suggested action
File system not mounted	Contact the next level of support.
File system usage threshold exceeded	Contact the next level of support.
File system write failed	Contact the next level of support.
File system read failed	Contact the next level of support.

Cause	Suggested action
CPU load average threshold exceeded	Check the system for runaway processes.
Swap space usage threshold exceeded	Contact the next level of support.
Memory usage threshold exceeded	Contact the next level of support.
Password expiration	Change the password of the specified user account using the procedure "Changing a user password on an SSPFS-based server". ***Note:*** This alarm will clear in a maximum of 30 minutes after the password change.

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz

SPFS400

Log report SPFS400 indicates the total number of alarms that were raised on the SPFS-based server through alarmd. The log indicates the total number of minor, major, and critical alarms, and indicates the system on which the most recent alarm in each severity category (if any), has occurred.

Format

The format for log report SPFS400 is as follows:

```
Aug  6 14:03:37 <host> alarmd[753]:
_V2_~I=SDM~H=<host>~A=alarmd ~S=0022~ SPFS400 NONE INFO Alarm
Summary Log.^M       ^M       TimeStamp: Fri Aug 06 14:03:36
2004^M        Minor: 3^M        Major: 3^M        Critical:
2^M Most Recent Minor: iemscs2k=<hos>t;NODE=<host>-unit1^M
Most recent Major:^M
iemscs2k=<host>;NODE=<host>-unit0;CLASS=NET;NETTYPE NODE^M
Most Recent Critical:^M
iemscs2k=<host>;NODE=<host>-unit0;CLASS=SYS;SYSTYPE=FSMon;FS
Mon^M        Name=FSUsage;FSName=/data^M
```

Selected field descriptions

This log report has no selected fields.

Action

None

Associated OM registers

This log report has no associated OM registers.

Additional information

Customer logs are filed in the directory /var/log/customerlog. The archived versions of these logs are filed in a compressed format in the same directory.

Example
/var/log/customerlog.0.gz