UAS Fault Management

Fault management activities that are performed to maintain and monitor the Universal Audio Server (UAS) and the Audio Provisioning Server (APS) include:

- retrieving logs and responding to the system faults that caused them to be generated

- retrieving alarms and responding to the system faults that caused them to be generated

- replacing system hardware

- restoring database files

- rebooting

The tools and utilities used to perform UAS and APS fault management are described in the section, Tools and utilities on page 1. The procedures and tasks that enable you to perform UAS and APS fault management tasks are grouped by application and are listed in tables shown in the section, UAS and APS fault management procedures on page 2.

Tools and utilities

UAS fault reporting is based on Simple Network Management Protocol. Both alarm or log retrieval and system correction are performed either through the CS 2000 Management Tool Universal Audio Server Manager or through commands entered at the command line or Windows interface.

Note 1: Running the Universal Audio Server Manager cannot be restricted exclusively to a single user. Therefore, system network managers must coordinate their configuration and maintenance activities performed through this tool.

Note 2: The Universal Audio Server Manager cannot be used for configuration or maintenance of the Media Server 2000 Series.

UAS and APS fault management procedures

The following table lists UAS and APS alarm retrieval procedures.

UAS and APS alarm retrieval procedures

Procedure and page	Interface or Tool used
UAS alarms on page 6	not applicable
Viewing UAS alarms on page 50	UAS Manager
APS alarms on page 51	not applicable
Viewing APS system alarms and logs on page 54	Command line

The following table lists UAS and APS log retrieval procedures.

UAS and APS log retrieval procedures

Procedure and page	Interface or Tool used
UAS logs on page 55	not applicable
APS logs on page 166	not applicable
Viewing UAS logs through the Universal Audio Server Manager in a telnet session on page 183	UAS Manager
Viewing UAS events through the dumpel tool on page 186	dumpel
Viewing UAS logs through Windows Event Viewer on page 184	Windows Event Viewer
Viewing APS system alarms and logs on page 54	Command line
Configuring the log distribution profile on page 216	UAS Manager

The following table lists UAS fault management procedures.

UAS fault management procedures (Sheet 1 of 3)

Procedure and page	Interface or Tool used
Checking system visual indicators on page 210	not applicable
Viewing Component states on page 189	UAS Manager

UAS fault management procedures (Sheet 2 of 3)

Procedure and page	Interface or Tool used
Rebooting a UAS through the Universal Audio Server Manager on page 218	UAS Manager
Rebooting an audio server remotely through a telnet session on page 219	Command line
Rebooting an audio server through a Windows interface on page 220	Windows desktop interface
Restarting a UAS through the Universal Audio Server Manager on page 221	UAS Manager
Stopping and Restarting Universal Audio Server applications through the command line interface on page 222	Command line
Stopping and Restarting Universal Audio Server applications through the Windows interface on page 224	Windows desktop interface
Resetting a processor on the mate UAS domain on page 225	Command line
Changing the Admin state on page 226	UAS Manager
Adding a CG6000 to a UAS node on page 227	UAS Manager Windows desktop interface LCI GUI
Removing a CG6000 from a UAS node on page 231	UAS Manager Windows desktop interface LCI GUI
Replacing CG6000 cards on page 235	UAS Manager
Adding an AG4000 card to a UAS node on page 241	UAS Manager Windows desktop interface LCI GUI
Removing an AG4000 from a UAS node on page 245	UAS Manager Windows desktop interface LCI GUI
Replacing AG4000 cards on page 249	UAS Manager Windows desktop interface

UAS fault management procedures (Sheet 3 of 3)

Procedure and page	Interface or Tool used
Replacing a SCSI Controller (CPV8540) card on page 253	UAS Manager Windows desktop interface
Replacing a CPV5350 Processor card on page 257	UAS Manager Windows desktop interface
BIOS Settings for CPV5350 SCSI on page 260	not applicable
Replacing a CPV5370 Processor card on page 265	UAS Manager Windows desktop interface
BIOS Settings for CPV5370 SCSI on page 268	not applicable
Replacing a Hot Swap Controller card on page 273	UAS Manager Windows desktop interface
Replacing a BX4000c (S007) ATM interface card on page 275	UAS Manager Windows desktop interface
Replacing a PA200 card on page 279	UAS Manager Windows desktop interface
Replacing a UAS disk drive on page 283	UAS Manager Windows desktop interface
Restoring UAS configuration files on page 286	Windows desktop interface Command line

The following table lists APS fault management procedures.

APS fault management procedures (Sheet 1 of 2)

Procedure and page	Interface or Tool used
APS troubleshooting guide on page 290	not applicable
Trouble-shooting the APS provisioner on page 292	Command line
Removing provisioner lock files on page 296	Command line
Checking for active audio provisioner processes on page 297	Command line
Troubleshooting APS login problems on page 298	Command line

APS fault management procedures (Sheet 2 of 2)

Procedure and page	Interface or Tool used
[Starting the APS Oracle database on page 304](#)	Command line
[Restoring audio files to a UAS node on page 305](#)	APS GUI
[Rebooting an APS on page 306](#)	Command line

UAS alarms

Alarms inform system administrators that a fault condition has occurred and requires corrective action. Normally, an alarm is cleared only when the condition that caused the alarm no longer exists. If the alarm cannot be cleared, a log is issued to flag the condition.

Alarms are viewed through the UAS Manager.

Note: The ProbableCause field in the following alarm descriptions contains a numeric code that indicates the cause of the alarm condition. These codes include:

- 1 (adapter error)
- 7 (configuration or customization error)
- 8 (congestion)
- 15 (equipment malfunction)
- 17 (file error)
- 46 (software error)
- 56 (underlying resource unavailable)
- 115 (procedural error)

Node alarms

This section contains Node alarms.

6145 NODE_NO_INSTALLED_CARDS

Severity = "critical"

ProbableCause = "56"

ProblemType="equipment"

Message="There are no NMS cards installed."

Probable Cause: An ATM-based system requires at least one NMS AG4000 card and an IP-based system requires at least one NMS CG6000 card. An extraction has occurred and there are no AG4000 or CG6000 cards in the system.

Corrective Action: If this is a UAS media server, shut down the node, insert the cards(s) and restart the node. If this is a PRI gateway, insert a card(s).

Clear Condition: In a UAS media server, the alarm is cleared when the node is restarted. In a PRI gateway, the alarm is cleared when a card is inserted.

Object Class: software

Service Affecting: SA

Call Agent Connection alarms

This section contains Call Agent Connection alarms.

8193 THREAD_DEATH_ALARM

ProbableCause = "46"

ProblemType="processingError"

Message="MGCIF <messageDirection> messaging thread died multiple times and was not restarted."

Probable Cause: Either the "ingoing" or "outgoing" messaging thread is unable to restart because of some undetermined problem.

Corrective Action: Look for error logs that might indicate what the problem is.

Clear Condition: Cleared at next startup of call processing application

Object Class: software

Service Affecting: SA

8194 UDP_INIT_FAIL_ALARM

Severity = "Critical"

ProbableCause = "46"

ProblemType="processingError"

Message="UDP Initialization Failed: <reason>."
<reason>: MGC IP address is not datafilled.

Probable Cause: The uas.conf file either does not exist, is unreadable or is missing an entry for "CallAgentIPAddress".

Corrective Action: Fix the configuration file.

Clear Condition: Cleared at next startup of call processing application

Object Class: software

Service Affecting: SA

8194 UDP_INIT_FAIL_ALARM

Severity = "Critical"

ProbableCause = "46"

ProblemType="processingError"

Message="UDP Initialization Failed: <reason>."
<reason>: MGC IP address is not valid.

Probable Cause: The call agent IP address obtained from the config file is not valid.

Corrective Action: Fix the IP address in the config file.

Clear Condition: Cleared at next startup of call processing application

Object Class: software

Service Affecting: SA

8194 UDP_INIT_FAIL_ALARM

Severity = "Critical"

ProbableCause = "46"

ProblemType="processingError"

Message="UDP Initialization Failed: <reason>."
<reason>: Bad return code from WSAStartup =<errorCode>.

Probable Cause: An attempt was made to initialize the Windows socket library, but failed.

Corrective Action: Report the full text of the alarm to the support group.

Clear Condition: Cleared at next startup of call processing application

Object Class: software

Service Affecting: SA

8194 UDP_INIT_FAIL_ALARM

Severity = "Critical"

ProbableCause = "46"

ProblemType="processingError"

Message="UDP Initialization Failed: <reason>."
<reason>: WinSock version is <majorVersion>.<minorVersion>, not 1.1 as expected.

Probable Cause: An attempt was made to initialize the Windows socket library, but failed because of a version mismatch.

Corrective Action: Report the full text of the alarm to the support group.

Clear Condition: Cleared at next startup of call processing application

Object Class: software

Service Affecting: SA

8194 UDP_INIT_FAIL_ALARM

Severity = "Critical"

ProbableCause = "46"

ProblemType="processingError"

Message="UDP Initialization Failed: <reason>."
<reason>: Unable to create socket; error =<errorCode>.

Probable Cause: An attempt was made to create a UDP communications socket, but failed.

Corrective Action: Report the full text of the alarm to the support group.

Clear Condition: Cleared at next startup of call processing application

Object Class: software

Service Affecting: SA

8194 UDP_INIT_FAIL_ALARM

Severity = "Critical"

ProbableCause = "46"

ProblemType="processingError"

Message="UDP Initialization Failed: <reason>."
<reason>: Unable to bind client name to socket; error = <errorCode>.

Probable Cause: An attempt was made to bind the communications socket to the port specified in the uas.conf configuration file. Another callp program may already be running.

Corrective Action: Ensure that another callp program is not running.

Clear Condition: Cleared at next startup of call processing application

Object Class: software

Service Affecting: SA

8194 UDP_INIT_FAIL_ALARM

Severity = "Critical"

ProbableCause = "46"

ProblemType="processingError"

Message="UDP Initialization Failed: <reason>."
<reason>: Unable to connect to call agent socket; error = <errorCode>.

Probable Cause: An attempt was made to associate the communications socket with the address of the call agent, but failed.

Corrective Action: Report the full text of the alarm to the support group.

Clear Condition: Cleared at next startup of call processing application

Object Class: software

Service Affecting: SA

8195 SOCKET_ERROR_ALARM

Severity = "Warning/Minor/MajorCritical" This is a threshold-based alarm, with a different threshold for each severity level.

ProbableCause = "46"

ProblemType="processingError"

Message="UDP Socket errors are being detected."

Probable Cause: The subsystem which sends messages to the call agent is experiencing send/receive errors on its local communications port (socket).

Corrective Action: The corrective action would be to lock the network element and then perform a system reboot. If problem persists, contact Nortel support group.

Clear Condition: Cleared when the rate of socket send/receive errors drops below the warning threshold.

Object Class: software

Service Affecting: SA

8196 RETRANS_ALARM

Severity = "Warning/Minor/MajorCritical" This is a threshold-based alarm, with a different threshold for each severity level.

ProbableCause = "46"

ProblemType="processingError"

Message="Retransmissions are being detected."

Probable Cause: The subsystem which sends messages to the call agent is performing an abnormally high number of retransmissions. Messages are retransmitted when the subsystem fails to receive an acknowledgement. There may be a network problem or the Media Gateway Controller (MGC) is not responding to messages.

Corrective Action: Ensure that the MGC is in service. Ensure that there are no network problems. Ensure that the primary call agent IP address is configured properly.

Clear Condition: Cleared when the rate of retransmissions drops below the warning threshold.

Object Class: software

Service Affecting: SA

8197 EXCEED_MAX_RETRANS_ALARM

Severity = "Warning/Minor/MajorCritical" This is a threshold-based alarm, with a different threshold for each severity level.

ProbableCause = "46"

ProblemType="processingError"

Message="The number of retransmissions has now exceeded the maximum number of retransmissions."

Probable Cause: The system attempts to retransmit a message up to N times until an acknowledgement is received from the Media Gateway Controller (MGC). If N is exceeded an abnormally high number of times, then this alarm is raised. There may be a network problem or the MGC is not responding to messages.

Corrective Action: Ensure that the MGC is in service. Ensure that there are no network problems. Ensure that the primary call agent IP address is configured properly.

Clear Condition: Cleared when the rate of retransmissions drops below the warning threshold.

Object Class: software

Service Affecting: SA

Call Engine alarms

This section contains Call Engine alarms.

The following alarm is associated with call processing or maintenance state machines.

12290 CALLP_THREAD_NOT_RESTARTED

Severity = "Major"

ProbableCause = "46"

ProblemType="processingError"

Message = "Call processing thread for endpointId <endpointId> died too quickly - not restarting. ConnectionId=<connectionId>, CallId=<callId>, TransId=<transactionId>, State=<callState>, CurrEvent=<event>."

Probable Cause: The call processing software thread associated with <endpointId> died due to an unhandled software error, and was not restarted because it died too quickly after the previous start. Additional information is included to assist in correlation with logs on other nodes. <connectionId> is the connectionId for the active connection on this endpointId. <callId> is the callId for the active connection on this endpointId. <transactionId> is the most recently received transactionId. <callState> is the current state of the call processing thread. <event> is the type of the event most recently received by the call processing thread.

Corrective Action: Escalate this issue to Nortel support, providing any other logs that might have occurred.

Clear Condition: Cleared at next startup of call processing application.

Object Class: software

Service Affecting: SA

The following alarm is associated with configuration problems.

12291 CALLP_CFG_INVALID

Severity = "Critical"

ProbableCause = "7"

ProblemType="processingError"

Message = "Invalid endpointId configuration. Check endpointId configuration in rm.resources file"
Probable Cause: The resource configuration for endpointId in C:\uas\etc\rm.resources is not valid.

Corrective Action: Correct the configuration for endpointId in the rm.resources file, and restart the call processing application.

Clear Condition: Cleared at next startup of call processing application

Object Class: software

Service Affecting: SA

The following alarms are related to call processing usage of the resource manager.

12292 CALLP_CANT_RELEASE

Severity = "Major"

ProbableCause = "46"

ProblemType="processingError"

Message = "Failed to release endpointId <endpointId>. Check ResMgr on UAS."

Probable Cause: Failed to release <endpointId> because of a lost connection to ResMgr

Corrective Action: Verify that ResMgr process is still running.

Clear Condition: Cleared at next startup of call processing application.

Object Class: software

Service Affecting: SA

12295 AUDIO_VFSDIR_NOT_SET

Severity = "Critical"

ProbableCause = "46"

ProblemType="processingError"

Message = "VFSDIR variable is not set. VFS has not been installed or is installed incorrectly on the node."

Probable Cause: The environment variable VFSDIR is not set to the home directory of the VFS hierarchy.

Corrective Action: Verify that the VFS software is correctly installed.

Clear Condition: Cleared at next start of the call processing application.

Object Class: software

Service Affecting: SA

12296 CALLP_CONFIG_PROB

Severity = "Critical"

ProbableCause = "7"

ProblemType="processingError"

Message = "Waiting for valid configuration."

Probable Cause: A serious configuration problem has been detected. The Audio Server is unable to initialize. A configuration file is probably in error. Look for an error log to determine the exact cause of the problem.

Clear Condition: The alarm is cleared after the configuration problem is fixed.

Object Class: software

Service Affecting: SA

12297 CALLP_NO_CARDS_AVAILABLE

Severity = "Critical"

ProbableCause = "7"

ProblemType="processingError"

Message="There are no NMS cards available for use."

Probable Cause: The card maintenance subsystem initialized and found no available AG4000 or CG6000 cards. At least one AG4000 card is required in an ATM-based UAS and at least one CG6000 card is required in an IP-based UAS.

Corrective Action: Reseat existing cards or add new cards. Ensure that there is at least one working AG4000 or CG6000 card in the system.

Clear Condition: Cleared at next start of the call processing application if at least one card is available.

Object Class: software

Service Affecting: SA

12298 CALLP_AUDIO_RESYNC_FAILURE

Severity = "Major"

ProbableCause = "46"

ProblemType="processingError"

Message="Failed to communicate with aliasServer. Check audio installation and aliasServer."

Probable Cause: During initialization of the call processing application, the attempt to establish communications with the aliasServer failed.

Corrective Action: Verify that the aliasServer application is running. If it is not running, verify that the apmvfs directory exists under the d:\directory, and that this directory is populated correctly with the default audio directories and files.

Clear Condition: Cleared at next start of the call processing application.

Object Class: software

Service Affecting: SA

AG4000 Service-level alarms

These alarms are associated with conditions that affect the service-level functionality of the AG4000 card.

14337 AG_GENERIC_ALARM

Severity = "major"

ProbableCause = "15"

ProblemType="equipment"

Message="Problem with AG4000 card in slot <slot>: initialization error"

Probable Cause: An attempt was made to load software onto the card and to start the card. The attempt failed.

Corrective Action: Stop the applications, reseat the card and then restart the applications. If the problem persists, contact the Nortel support group.

Clear Condition: The alarm is cleared when the applications are restarted and the operation succeeds.

Object Class: card

Service Affecting: SA

14338 AG_SURPRISE_EXTRACTION

Severity = "major"

ProbableCause = "115"

ProblemType="equipment"

Message="Improper extraction of AG4000 card in slot <slot>"

Probable Cause: An unlocked card was extracted from the shelf. Any existing calls on that card are terminated. The proper procedure for removing a card is to first lock it.

Corrective Action: Reinsert the card and check the states of the card at the Element Manager to ensure that the administrative state goes to "unlocked" and the operational state goes to "enabled."

Clear Condition: The alarm is cleared when the card is reinserted.

Object Class: card

Service Affecting: SA

14339 AG_CARD_DISABLED

Severity = "major"

ProbableCause = "115"

ProblemType="equipment"

Message="AG4000 card in slot <slot> disabled until next application restart"

Probable Cause: An unlocked AGcard was extracted from the shelf. Any existing calls on that card are terminated. The proper procedure for removing a card is to first lock it. This board does not support Hot Swap in this configuration.

Corrective Action: Reinsert the card and check the states of the card at the Element Manager to ensure that the administrative state goes to "unlocked" and the operational state goes to "disabled."

Clear Condition: The alarm is cleared upon application restart.

Object Class: card

Service Affecting: SA

14340 AG_SHOWERQ_ALARM

Severity = "major"

ProbableCause = "15"

ProblemType="software"

Message="card in slot <slot> has reached error threshold, removing from service"

Probable Cause: An issue occurred in the UAS software, that caused this board to fail.

Corrective Action:

1 Stop any applications that may be running.

   a) Access the "Services" window as follows: select Start -> Programs -> Administrative Tools ->Services

   b) Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

2 Shut down the system.

   a) select Start -> Shut Down

b) On the Shut Down Windows screen, select "Shut down this computer." When the shutdown is complete, the system displays a message indicating it is safe to turn off the computer.

Do not turn off power to the computer when you see the message indicating it is safe to turn off the computer.

Clear Condition: The alarm is cleared upon application restart.

Object Class: card

Service Affecting: SA

NodeMtc alarms

These alarms are generated by the callp application if the NMS CT daemon and NMS Clock Fallback Manager services fail to stop or start successfully.

20481 CTDAEMON_SERVICE_FAILURE

Severity = "critical"

ProbableCause = "46"

ProblemType="processingError"

Message="Unable to successfully start/stop the NMS Ctdaemon service.."

Probable Cause: Either the NMS CT daemon service is not installed as a service, or it is in a service state where it cannot accept start and stop service requests.

Corrective Action: Make sure that the NMS CT daemon service is installed. Stop, uninstall and re-install the service if need be.

Clear Condition: The alarm is cleared once the NMS CT daemon service has been successfully started or stopped.

Object Class: software

Service Affecting: SA

20482 CFBM_SERVICE_FAILURE

Severity = "critical"

ProbableCause = "46"

ProblemType="processingError"

Message="Unable to successfully start/stop the NMS Clock Fallback Manager service.."

Probable Cause: When the NMS CT daemon service is started, it should automatically start the NMS Clock Fallback Manager service (The NMS Clock Fallback Manager service it not automatically stopping the NMS CT daemon service.). If the NMS Clock Fallback Manager service is not automatically started for some reason, either the NMS Clock Fallback Manager service is not installed as a service for it to be started or stopped, or it is in a service state where it cannot accept start and stop service requests.

Corrective Action: Make sure that the NMS Clock Fallback Manager service is installed. Stop, uninstall and re-install the service if need be.

Clear Condition: The alarm is cleared once the NMS Clock Fallback Manager service has been successfully started or stopped.

Object Class: software

Service Affecting: SA

20483 SERVICE_FAILURE

Severity = "critical"

ProbableCause = "46"

ProblemType="processingError"

Message="The <service-name> service could not be <action>."

Probable Cause: Either the specified service is not installed, or it is in a state where it cannot accept start and stop requests. The only possible value for <service-name> currently is "w32time", the NTP time service. The possible values for <action> are "stopped" and "started".

Corrective Action: Make sure that the service is installed. Stop, uninstall and re-install the service.

Clear Condition: The alarm is cleared once the service has been successfully started or stopped.

Object Class: software

Service Affecting: SA

ConfigMgr alarms

This section lists the ConfigMgr alarms.

26625 CM_CONFIG_ERROR

Severity = "Critical"

ProbableCause = "7"

ProblemType="processingError"

Message = "Configuration error: <reason>" See <reason> list below.

Probable Cause: A serious configuration problem has been detected. The Audio Server is unable to initialize. A configuration file is probably in error. Look for an error log to determine the exact cause of the problem.

Clear Condition: The alarm is cleared after the configuration problem is fixed.

Object Class: software

Service Affecting: SA

<reason>: template file(s) missing: <listOfConfigTemplateFiles>.

Probable Cause: The specified configuration template files are missing from c:\uas\cfg\templates

Corrective Action: Restore the missing files.

<reason>: Configuration file is missing: <filename>

Probable Cause: The specified configuration file is missing.

Corrective Action: Restore the missing file.

<reason>: invalid trunk and carrier configuration file: ugw.conf

Probable Cause: The ugw.conf file is invalid.

Corrective Action: Fix the configuration.

<reason>: error in the ugw.conf config file. Card configured for bad slot (<slot>)

Probable Cause: A card is configured for an invalid IO slot number.

Corrective Action: Fix the configuration.

<reason>: card configured for slot <slot> in ugw.conf is not configured in uas.conf

Probable Cause: Card configuration date in the two config files is inconsistent.

Corrective Action: Fix the configuration.

<reason>: unable to access bearer config data

Probable Cause: ConfigMgr attempted to access config data but failed.

Corrective Action: Contact the support group.

<reason>: could not set config key: <parameterName>

Probable Cause: ConfigMgr was unable to update the uas_pending.conf file. The file may have had incorrect permissions or the disk is full.

Corrective Action: Check file permissions. Check to see if the disk is full.

<reason>: failed to create synchronization object

Probable Cause: ConfigMgr attempted to create a kernel object but encountered an error.

Corrective Action: Contact the support group.

<reason>: could not copy file

Probable Cause: ConfigMgr was unable to copy a file. The file may have had incorrect permissions or the disk is full.

Corrective Action: Look at logs to determine which file caused the problem. Check file permissions. Check to see if the disk is full.

<reason>: The number of AG cards could not be determined.

Probable Cause: ConfigMgr could not automatically determine how many AG cards there are in the system.

Corrective Action: Ensure that the NMS blocate utility is present and is working properly.

<reason>: could not update number of ag cards

Probable Cause: ConfigMgr could not update the uas.conf file with the number of AG cards.

Corrective Action: Check file permissions. Check to see if the disk is full.

<reason>: <filename> failed validation

Probable Cause: A configuration parameter is missing or has an invalid value.

Corrective Action: Look at logs to determine which configuration parameters are missing.

<reason>: failed to set synchronization object

Probable Cause: ConfigMgr attempted to operate on a kernel object but encountered an error.

Corrective Action: Contact the support group.

<reason>: The number of cards configured (<num-cards-configured>) is inconsistent with the number of bearer cards in the system (<num-cards-in-system>)

Probable Cause: There is a configuration mismatch.

Corrective Action: Change the bearer card configuration to be consistent with the bearer cards that are installed in the system.

<reason>: There is a <card-type> board configured for slot <slot> but no card is installed in that slot.

Probable Cause: There is a configuration mismatch.

Corrective Action: Change the bearer card configuration to be consistent with the bearer cards that are installed in the system.

CG6000 Service-level alarms

These alarms are associated with conditions that affect the service-level functionality of the CG6000 card.

30721+ CG_GENERIC_ALARM

Severity = "major"

ProbableCause = "15"

ProblemType="equipment"

Message="Problem with CG6000 card in slot <slot>: initialization error"

Probable Cause: An attempt was made to load software onto the card and to start the card. The attempt failed.

Corrective Action: Stop the applications, reseat the card and then restart the applications. If the problem persists, contact the Nortel support group.

Clear Condition: The alarm is cleared when the applications are restarted and the operation succeeds.

Object Class: card

Service Affecting: SA

30721+ CG_GENERIC_ALARM

Severity = "critical"

ProbableCause = "15"

ProblemType="equipment"

Message="Problem with CG6000 card in slot <slot>: Error threshold reached on card. Taking out of service."

Probable Cause: The application software attempted to use the services of a card, but experienced too many failures.

Corrective Action: Restart the card by taking these steps: Perform a service-level lock, a base-level loc, a base-level unlock, and then a service-level unlock. If the problem persists, contact the Nortel support group.

Clear Condition: The alarm is cleared when the card is restarted.

Object Class: card

Service Affecting: SA

30722 CG_ETHERNET_CONN_ALARM

Severity = "Critical"

ProbableCause = "15"

ProblemType="equipment"

Message = "<n> failed ethernet connection(s) on CG6000 card in slot <slot>."

Probable Cause: The specified number of ethernet connections <n> (1 or 2) have failed.

Corrective Action: Ensure that ethernet cables are attached to both network jacks on the card. Determine if there is a local area network problem.

Clear Condition: The alarm is cleared when either an ethernet cable is attached or when the network problem clears up.

Object Class: card

Service Affecting: SA

30723 CG_SURPRISE_EXTRACTION

Severity = "major"

ProbableCause = "115"

ProblemType="equipment"

Message= "improper extraction of CG6000 card in slot <slot>"

Probable Cause: An unlocked card was extracted from the shelf. Any existing calls on that card are terminated. The proper procedure for removing a card is to first lock it.

Corrective Action: Reinsert the card and check the states of the card at the Element Manager to ensure that the administrative state goes to unlocked and the operational state goes to enabled.

Clear Condition: The alarm is cleared when the card is inserted.

Object Class: card

Service Affecting: SA

30726 CG_SHOWERQ_ALARM

Severity = "major"

ProbableCause = "15"

ProblemType="software"

Message= "CG6000 card in slot <slot> has reached error threshold, removing from service."

Probable Cause: An issue occurred in the UAS software that caused this board to fail.

Corrective Action: Reinsert the card and check the states of the card at the Element Manager to ensure that the administrative state goes to unlocked and the operational state goes to enabled.

Clear Condition: The alarm is cleared upon application restart.

Object Class: card

Service Affecting: SA

ATM service alarms

This section contains ATM service alarms.

34817 ATM_MISSING_CARD

Severity = "Critical"

ProbableCause = "1"

ProblemType="processingError"

Message = "The ATM card <ATM card description> in slot <slot number> is missing"

Probable Cause: Either the ATM card has been pulled or it has experienced a catastrophic failure and is unable to register with the cPCI chassis.

Corrective Action: A working ATM card must be inserted into the slot. Alternatively, all the VCs may be deleted which are associated with the missing card.

Clear Condition: Cleared at next start of call processing application.

Object Class: software

Service Affecting: SA

34818 ATM_MISMATCH_CARD

Severity = "Critical"

ProbableCause = "1"

ProblemType="processingError"

Message = "The ATM card <ATM card description> in slot <slot number> does not match card <ATM card description> in the saved configuration"

Probable Cause: The ATM card has been replaced with a different model ATM card.Corrective Action: Place the correct ATM card back in the slot which originally contained the S007 card. Alternatively, all the VCs may be deleted which are associated with the mismatched card.

Clear Condition: Cleared at next start of call processing application.

Object Class: software

Service Affecting: SA

34819 ATM_H110_FAILURE

Severity = "Critical"

ProbableCause = "1"

ProblemType="equipment"

Message = "The ATM card detected an H.110 bus failure"

Probable Cause: This alarm may be caused by a bad AG driving the H.110 bus clock or more than one card is trying to drive the clock on the bus.

Corrective Action: Check the clocking configuration and the AG cards.

Clear Condition: Clears at the next start of the call processing application.

Object Class: software

Service Affecting: SA

34820 ATM_OUTDATED_FIRMWARE

Severity = "Major"

ProbableCause = "1"

ProblemType="processingError"

Message = "The ATM card in slot <slot number> has outdated firmware ver.:<versin> recommended version <version>. Please run the ATMFirmware command to upgrade the firmware"

Probable Cause: This alarm is seen if the ATM card has outdated firmware.

Corrective Action: Run 'ATMFirmware -upgrade' command to upgrade the firmware.

Clear Condition: Clears at the next start of the call processing application, after the firmware has been upgraded.

Object Class: software

Service Affecting: SA

34821 ATM_FIRMWARE_NON_UPGRADABLE

Severity = "Major"

ProbableCause = "1"

ProblemType="processingError"

Message = "The ATM card in slot <slot number> has outdated firmware ver.:<version>. This firmware needs to be manually updated. Please load the card with a firmware version which is 2.1.0 or later."

Probable Cause: This alarm is seen when the firmware on the ATM card is outdated and cannot be automatically upgraded.

Corrective Action: Follow appropriate procedure to manually download an up-to-date firmware to the card or call first tier support.

Clear Condition: Clears at the next start of the call processing application, after the firmware has been upgraded.

Object Class: software

Service Affecting: SA

34822 ATM_HW_API_TOO_MANY_FAILURES

Severity = "Critical"

ProbableCause = "1"

ProblemType="processingError"

Message = "The number of consecutive API call failures to the ATM card in slot <slot number> has exceeded the threshold of <threshold>. The card is being taken out of service."

Probable Cause: This alarm is seen when too many consecutive API calls to the ATM card fail.

Corrective Action: Restart the system. If the error persists then replace ATM card or call first tier support.

Clear Condition: Clears at the next start of the call processing application.

Object Class: software

Service Affecting: SA

ATM port alarm

This section contains ATM port alarms.

38913 ATM_PORT_LOC

Severity = "Critical"

ProbableCause = "1"

ProblemType="processingError"

Message = "ATM port <port number> in slot <slot number> has experienced a loss of connectivity"

Probable Cause: The fiber connecting the ATM port to the network has either been unplugged or damaged.

Corrective Action: Plug the fiber back in, or replace it if it was damaged.

Clear Condition: Cleared at next start of call processing application.

Object Class: software

Service Affecting: SA

Carrier alarms

This section contains Carrier alarms.

40962 CARRIER_RAISE_ALARM

Severity = "critical"

ProbableCause = "6"

ProblemType="communications"

Message="CARRIER ALARM: %s on carrier (board %d , trunk %d)."

Probable Cause: One of the carrier alarms raised: RAI, AIS, LOF, LOS, E1 LOMFS, and E1 16 AIS.These carrier alarms are defined in GR820.

Corrective Action: Based on the different alarm types check T1/E1 carrier for the cause. Refer to GR820 for each alarm case.

Clear Condition: CARRIER_CLR_ALARM event is received

Object Class: software

Service Affecting: SA

Activity Manager alarms

This section contains Activity Manager alarms. The Activity Manager is part of the Global Server base software.

53249 AM_COLD_START_NOT_SENT_CEM ----not raised in UAS06----

Severity = "Critical"

Message = "[am_001] Cold Start SNMP trap message not sent"

ProbableCause = "2"

ProblemType = "processingError"

Probable Cause: CEM processes unavailable.

Corrective Action: Reboot domain.

Clear Condition: Cleared after reboot.

Object Class: software

Service Affecting: SA

53250 AM_COLD_START_NOT_SENT_SWACT----not raised in UAS06----

Severity = "Critical"

Message = "[am_002] Cold Start SNMP trap message not sent."

ProbableCause = "2"

ProblemType = "processingError"

Probable Cause: SWACT Mgr processes unavailable.

Corrective Action: Reboot domain.

Clear Condition: Cleared after reboot.

Object Class: software

Service Affecting: SA

53251 AM_SWACT_FAILURE ----not raised in UAS06----

Severity = "Critical"

Message = "[am_003] Requested SWACT failed to complete in expected time."

ProbableCause = "44"

ProblemType = "qualityOfService"

Probable Cause: SWACT Mgr is hung.

Corrective Action: Reboot domain.

Clear Condition: Cleared after reboot.

Object Class: software

Service Affecting: SA

53252 AM_ERM_FAILURE

Severity = "Critical"

Message = "[am_004] ERM failed to notify AM with Mate State Synch or Mate is Dead message in expected time"

ProbableCause = "44"

ProblemType = "qualityOfService"

Probable Cause: Event Relay Manager is hung.

Corrective Action: Reboot domain.

Clear Condition: Cleared after reboot.

Object Class: software

Service Affecting: SA

53253 AM_ED_SOCK_FAILURE

Severity = "Major"

Message = "[am_005] AM failed to open socket to EventDistributor. AM is exiting."

ProbableCause = "6"

ProblemType = "communications"

Probable Cause: OS Resources Used up.

Corrective Action: Reboot domain.

Clear Condition: Cleared after reboot.

Object Class: software

Service Affecting: SA

53254 AM_CONFIG_ERROR_NOFILE

Severity = "Minor"

Message = "[am_027] Error accessing AM Config file <filename>. Using default configuration values."

ProbableCause = "6"

ProblemType = "processingError"

Probable Cause: Configuration file does not exist.

Corrective Action: Restore file.

Clear Condition: Cleared after reboot, after file is restored.

Object Class: software

Service Affecting: SA

Power Supply, Fan Maintenance, Cooling system, and Disk Drive alarms

This section contains power supply, fan maintenance, cooling system, and disk drive alarms.

57345 FAN_RAISE_ALARM

Severity = "major"

ProbableCause = "35"

ProblemType="equipment"

Message="ALARM: Raising alarm on fan<unit #>, due to <reason>."

Probable Cause: HA Monitor received a Fan Fault Tag, and informed the PsFanMtc subsystem. This could be due to a faulty fan in the chassis, that has gone down.

Corrective Action: Replace the module containing the failed fan unit.

Clear Condition: Receive a Fan Fault tag with the "Fan Fault" bit unset, to indicate that this fault has been cleared.

Object Class: software

Service Affecting: SA

59393 POWER_SUPPLY_RAISE_ALARM
Severity = "major"

ProbableCause = "35"

ProblemType="equipment"

Message="ALARM: Raising alarm on power supply <unit #>, due to <reason>."

Probable Cause: HA Monitor received a Power Supply Fault Tag, and informed the PsFanMtc subsystem. This could be due to a faulty power supply system in the chassis, that has gone down.

Corrective Action: Replace the module containing the failed power supply.

Clear Condition: Receive a Power Supply Fault tag with the "Power Good" bit set, to indicate that this fault has been cleared.

Object Class: software

Service Affecting: SA

61441 COOLING_SYSTEM_RAISE_ALARM

Severity = "major/critical"

ProbableCause = "50"

ProblemType="environmental"

Message="ALARM: Raising alarm on Cooling System, due to <Cooling Alarm/Fault>."

Probable Cause: In the case of a cooling fault, this is due to a high temperature at air intake to the chassis. In the case of a Cooling alarm, it is due to an extremely high temperature at air intake to the chassis.

Corrective Action: Check air flow and cooling equipment.

Clear Condition: A GlobalServer Equipment fault tag with a 'cleared' alarm condition.

Object Class: software

Service Affecting: SA

63489 DISKDRIVE_RAISE_ALARM

Severity = "critical"

ProbableCause = "23"

ProblemType="equipment"

Message="ALARM: Problem detected on Domain <A/B> <hard/cd-rom> disk drive, chassis peripheral <peripheral#>, due to <>."

Probable Cause: Hard Disk Drive Peripheral fault detected. The key on the disk drive may have been turned.

Corrective Action: The key on the disk drive may have been turned to its unlocked position, so ensure that the key on the disk drive is turned to its locked position. Else check or replace the peripheral disk drive unit.

Clear Condition: A GlobalServer Peripheral OK Chassis Fault event(Turning the key on the peripheral disk drive to its locked position).

Object Class: software

Service Affecting: SA

I/O Card Base-level alarms

These alarms are associated with conditions that affect the base-level functionality of I/O cards such as the AG4000 and CG6000.

65537 CD_SURPRISE_SLOT_POWER_OFF

Severity = "major"

ProbableCause = "15"

ProblemType="equipment"

Message="Surprise power off on slot <slot>"

Probable Cause: A surprise power off on a slot can be caused by a chassis hardware problem or by a software error.

Corrective Action: The problem may clear up after a reboot. Stop the applications and perform a reboot. If the problem does not clear up, then you may be able to workaround the problem by moving the card to another slot. Refer to the appropriate card maintenance and configuration procedures.

Clear Condition: The alarm clears when power is restored to the slot.

Object Class: card

Service Affecting: SA

65538 CD_SURPRISE_CARD_EXTRACTION

Severity = "major"

ProbableCause = "15"

ProblemType="equipment"

Message="Surprise card extraction on slot <slot>"

Probable Cause: A card was improperly extracted from the specified slot.

Corrective Action: The applications will need to be restarted. Peform these actions: 1) stop the applications 2) reinsert the card 3) restart the applications

Clear Condition: The alarm clears when the card is reinserted and the applications are restarted.

Object Class: card

Service Affecting: SA

65539 CD_LOAD_SCRIPT_FAILURE

Severity = "major"

ProbableCause = "15"

ProblemType="equipment"

Message="Firmware load script failure on card in slot <slot>"

Probable Cause: An attempt was made to load firmware onto the card in the specified slot.

Corrective Action: The applications should be stopped, the card reseated and the applications restarted. If the problem persists, then contact the Nortel support group.

Clear Condition: If reseating of the card fixes the problem, then the alarm will clear when the applications are restarted.

Object Class: card

Service Affecting: SA

65540 CD_SLOT_VERIFY_SCRIPT_FAILURE

Severity = "major"

ProbableCause = "15"

ProblemType="equipment"

Message="Verify script failure on card in slot <slot>"

Probable Cause: An attempt was made to verify that the card contains the correct firmware version.

Corrective Action: The applications should be stopped, the card reseated and the applications restarted. If the problem persists, then contact the Nortel support group.

Clear Condition: If reseating of the card fixes the problem, then the alarm will clear when the applications are restarted.

Object Class: card

Service Affecting: SA

65541 CD_GENERIC_CARD_ALARM

Severity = "major"

ProbableCause = "15"

ProblemType="equipment"

Message="Problem with card in slot <slot>: <error>"

Probable Cause: A problem occurred with the card in the specified slot. A brief description of the problem is supplied.

Corrective Action: NA

Clear Condition: NA

Object Class: card

Service Affecting: SA

Chassis Event Manager alarms

This section contains Chassis Event Manager alarms. The Chassis Event Manager is part of the Global Server base software.

75791 CEM_CONFIG_ERROR_NOFILE

Severity = "Minor"

Message = "[cfm_config_error_nofile] Error accessing CEM Config file %s. Using default configuration values."

ProbableCause = "6"

ProblemType = "processingError"

Probable Cause: Config file is missing.

Corrective Action: Restore missing Config file.

Clear Condition: Cleared after restore of the file and reboot.

Object Class: software

Service Affecting: SA

Local Resource Manager alarms

This section contains Local Resource Manager alarms. The Local Resource Manager is part of the Global Server base software.

81921 LRM_CPU_C

Severity = "Critical"

Message = "[cpu_overload_critical] CPU usage critical. (<percent>% used)"

ProbableCause = "10"

ProblemType = "processingError"

Probable Cause: CPU cycles limit exceeded.

Corrective Action: Close some unused process.

Clear Condition: Cleared when CPU usage no longer exceeds critical limit.

Object Class: software

Service Affecting: SA

81922 LRM_CPU_M

Severity = "Major"

Message = "[cpu_overload_major] CPU usage high. (<percent>% used)"

ProbableCause = "10"

ProblemType = "processingError"

Probable Cause: CPU cycles limit exceeded.

Corrective Action: Close some unused process.

Clear Condition: Cleared when CPU usage returns to normal levels.

Object Class: software

Service Affecting: SA

81923 LRM_MEM_C

Severity = "Critical"

Message = "[mem_usage_high_critical] Memory usage critical. (<percent>% used)"

ProbableCause = "32"

ProblemType = "processingError"

Probable Cause: Out of memory.

Corrective Action: Free some non-used memory.

Clear Condition: Cleared when memory usage no longer exceeds critical limit.

Object Class: software

Service Affecting: SA

81924 LRM_MEM_M

Severity = "Major"

Message = "[mem_usage_high_major] Memory usage high. (<percent>% used)"

ProbableCause = "32"

ProblemType = "processingError"

Probable Cause: Out of memory.

Corrective Action: Free some non-used memory.

Clear Condition: Cleared when memory usage returns to normal levels.

Object Class: software

Service Affecting: SA

81925 LRM_DISK_C

Severity = "Critical"

Message = "[disk_usage_critical] File system %s usage critical. (<percent>% used)"

ProbableCause = "49"

ProblemType = "processingError"

Probable Cause: Storage capacity problem. Debug logs are turned on.

Corrective Action: Turn off debug logging.

Clear Condition: Cleared when disk usage no longer exceeds critical limit.

Object Class: software

Service Affecting: SA

81926 LRM_DISK_M

Severity = "Major"

Message = "[disk_usage_major] File system %s usage high. (<percent>% used)"

ProbableCause = "49"

ProblemType = "processingError"

Probable Cause: Storage capacity problem. Debug logs are turned on.

Corrective Action: Turn off debug logging.

Clear Condition: Cleared when disk usage returns to normal levels.

Object Class: software

Service Affecting: SA

81927 LRM_CONFIG_FILE_ERR

Severity = "Minor"

Message = "[lrm_config_file_err] Error (rc = [<error-code>]) accessing LRM Config file [<filename>]. Using default configuration values."

ProbableCause = "49"

ProblemType = "processingError"

Probable Cause: Config file is missing.

Corrective Action: Restore missing config file.

Clear Condition: Cleared on reboot after file is restored.

Object Class: software

Service Affecting: SA

Program Manager alarms

This section contains Program Manager alarms. The Program Manager is part of the Global Server base software.

83971 c_FAILED_MALLOC

Severity = "Critical"

Message = "[prm003] PMGR is unable to allocate memory. Error = <error_code>."

ProbableCause = "32"

ProblemType = "processingError"

Probable Cause: Out of Memory. Check error number.

Corrective Action: Correct memory problem and restart PMGR

Clear Condition: Cleared on restart of program manager.

Object Class: software

Service Affecting: SA

83987 c_BAD_FORK

Severity = "Critical"

Message = "[prm019] The fork() function failed to create new (criticality = <code>) process <pid>. Error = <code>."

ProbableCause = "2"

ProblemType = "processingError"

Probable Cause: The system has run out of resources.

Corrective Action: Perform a reboot.

Clear Condition: Cleared when the applications are restarted.

Object Class: software

Service Affecting: SA

83989 c_BAD_EXEC
Severity = "Critical"

Message = "[prm021] The execl() function failed for <program_name>. Error = <code>."

ProbableCause = "2"

ProblemType = "processingError"

Probable Cause: The system has run out of resources.

Corrective Action: n/a

Clear Condition: n/a

Object Class: software

Service Affecting: SA

83998 c_CRIT_DEATH

Severity = "Critical"

Message = "[prm030] Type <type> critical process <pid> died (status = <code>)."

ProbableCause = "47"

ProblemType = "processingError"

Probable Cause: A process has died due to a software error.

Corrective Action: Report the problem to the support group. The process will be restarted automatically.

Clear Condition: n/a

Object Class: software

Service Affecting: SA

83999 c_MAX_RETRIES

Severity = "Critical"

Message = "[prm031] PMGR has reached the maximum of <n> retries for <program_name>. Failure has become critical."

ProbableCause = "47"

ProblemType = "processingError"

Probable Cause: The process is encountering the same software error on each restart.

Corrective Action: Contact the support group.

Clear Condition: n/a

Object Class: software

Service Affecting: SA

84000 c_MAX_RETRIES_NO_RESTART

Severity = "Minor"

Message = "[prm032] PMGR has reached the maximum of <n> retries for <program_name>. No further restarts will be attempted."

ProbableCause = "47"

ProblemType = "processingError"

Probable Cause: The process is encountering the same software error on each restart.

Corrective Action: Contact the support group.

Clear Condition: n/a

Object Class: software

Service Affecting: SA

84009 c_FIFO_ERROR

Severity = "Critical"

Message = "[prm041] PMGR encountered an error communicating with a child process."

ProbableCause = "2"

ProblemType = "processingError"

Probable Cause: The system has run out of resources or the child process is encountering a software error.

Corrective Action: n/a

Clear Condition: n/a

Object Class: software

Service Affecting: SA

Ethernet Interface alarms

This section contains Ethernet Interface alarms. The alarm below applies to the host network adapter, which is used for messaging to call

control and device management. The host network adapter has two physical interfaces. The adapter is run in Adapter Fault Tolerance (AFT) mode, which provides automatic redundancy. If the primary adapter fails, the secondary takes over.

88065 E1_LINK_DOWN

Severity = "Critical"

Message = "Link on host network interface is down."

ProbableCause = "6"

ProblemType = "communications"

Probable Cause: One of the links on the host network adapter has failed. Either the cable is disconnected or there is a problem with the network, possibly a network switch or cable.

Corrective Action: Reconnect the cable or fix the network problem.

Clear Condition: Alarm is cleared when the network connection is restored.

Object Class: software

Service Affecting: SA

Event Server alarms

The Event Server is part of the Global Server base software.

96257 LOCAL_SRVSOCK_CREATION_FAILED

Severity = "critical"

Message = "[es_alrm_001] Unable to setup Server Socket for LOCALHOST system name. Exiting."

ProbableCause = "6"

ProblemType = "communications"

Probable Cause: System resources are not available.

Corrective Action: Reboot system.

Clear Condition: Alarm is cleared when applications are stopped.

Object Class: Software

Service Affecting: SA

96258 REMOTE_SRVSOCK_CREATION_FAILED

Severity = "major"

Message = "[es_alrm_002] Unable to setup Server Socket for the remote system name."

ProbableCause = "25"

ProblemType = "communications"

Probable Cause: System resources are not available.

Corrective Action: Reboot system.

Clear Condition: Alarm is cleared when applications are stopped.

Object Class: software

Service Affecting: SA

96259 SYSTEM_RESOURCE_ERR

Severity = "critical"

Message = "[es_alrm_003] Processing Error accessing connection data. Exiting."

ProbableCause = "32"

ProblemType = "ProcessingError"

Probable Cause:

Corrective Action:

Clear Condition:

Object Class: software

Service Affecting: SA

96260 CONFIG_ERR

Severity = "minor"

Message = "[es_alrm_004] Error in reading configuration data file [<filename>]. Using default values."

ProbableCause = "17"

ProblemType = "ProcessingError"

Probable Cause: Configuration file is missing.

Corrective Action: Restore the missing config file.

Clear Condition: Cleared on reboot after file is restored.

Object Class: software

Service Affecting: SA

96261 HAMODE_CHECK_FAILED

Severity = "critical"

Message = "[es_alrm_005] Unable to determine HA mode of system from file [<filename>] (rc = [<error-code>]). Exiting."

ProbableCause = "17"

ProblemType = "ProcessingError"

Probable Cause: Configuration file is missing.

Corrective Action: Restore the missing config file.

Clear Condition: Cleared on reboot after file is restored.

Object Class: software

Service Affecting: SA

96262 MATE_EVTSVR_CONN_LOST

Severity = "minor"

Message = "[es_alrm_006] Lost connection to mate EventServer for active alarm synchronization."

ProbableCause = "25"

ProblemType = "communications"

Probable Cause: The applications on the mate unit are down.

Corrective Action: Restart the applications on the mate unit.

Clear Condition: The alarm is cleared when the applications on the mate unit are started.

Object Class: software

Service Affecting: SA

Viewing UAS alarms

The CS 2000 call server provides a fault management sub-system which is used by various call server-based element managers, including the UAS Manager. Alarms occurring in a network element managed by the call server, like the UAS, are forwarded to the call server fault management sub-system using standard SNMP traps. The call server consolidates the alarms from its managed network elements and provides you the ability to monitor both active and historical alarms through a user interface.

For complete instructions on using a call server application user interface to retrieve and view UAS alarms, refer to your solution's Fault Management document.

APS alarms

Alarms, which are viewed from the Universal Audio Server Manager or, for the APS, also through a command line interface, inform system administrators that a fault condition has occurred and requires corrective action. An APS alarm consists of a five-character alphanumeric alarm identifier and the alarm text. In certain instances, the alarm ID, or the alarm text, may contain a two-digit alphabetic character code that identifies the component responsible for generating the alarm. These alarm identifiers are shown in the table below.

APS software components and associated alarm IDs

APS Software Component	Alarm ID
APS Administration	CM
APS Audio Management	AM
APS File Upload	FT
APS Servlet Requests	DB
IPS Trouble Conditions	FT

Additional detail about each APS software alarm is presented in associated fields, described in the table below.

APS software alarm fields (Sheet 1 of 2)

Field	Description
alarm text	alarm text that displays
Severity	Provides a level of severity for the alarm: - critical, which indicates that the event causing the alarm affects service and requires immediate corrective action - major, which indicates that the event causing the alarm does not reduce the systems' engineered capacity, but still requires immediate corrective action - minor, which indicates that the event causing the alarm does not affect service, but still requires corrective action - informational, which indicates only that a system event occurred

APS software alarm fields (Sheet 2 of 2)

Field	Description
Probable cause	Provides the cause for the alarm being issued, in the form of a representative integer from a range of standardized values from the NORTEL-NMI-TC-MIB. The possible causes and their representative values include: - 1 (adapter error) - 7 (configuration error) - 8 (congestion) - 17 (file error) - 46 (software error)
Problem Type	Categorizes the alarm. The possible categories includes: - communication - environmental - equipment - quality of service - processing error
Message	Explains the meaning of the alarm

APS Administration Alarms

This section contains APS Administration alarms.

26625 CM_DB_CONNECT_ERR

Severity = "critical"

ProbableCause = "46"

ProblemType="communications"

Message="DB is not available, or the user cannot get a connection to the DB"

APS File Upload Alarms

This section contains APS File Upload alarms.

43009 FT_DB_CONNECT_ERR

Severity = "critical"

ProbableCause = "46"

ProblemType="communications"

Message="DB is not available, or the user cannot get a connection to the DB"

APS Audio Management Alarms

This section contains APS Audio Management alarms.

28673 AM_DB_CONNECT_ERR

Severity = "critical"

ProbableCause = "46"

ProblemType="communications"

Message="DB is not available, or the user cannot get a connection to the DB"

Viewing APS system alarms and logs

Viewing APS system alarms and logs

In a telnet connection to the APS server

1   Open an xterm window and log in to the server as the root user.

2   Enter the following command to view the syslog file:

```
more /var/adm/messages
```

     Note 1: The syslog file will contain APS logs, and alarms, only if, during APS installation, or when you perform the procedure "Configuring the SNMP Agent" in the document, NN10095-511, entitled "UAS Configuration Management," you specify that the SNMP agent is to forward alarms/logs to syslog.

     Note 2: For information about the APS logs and alarms that display, see APS alarms on page 51.

3   You have completed this procedure.

UAS logs

Logs are similar to alarms in that they inform system administrators about fault conditions. Logs provide the following:

- notification about error conditions that cannot be cleared

- additional information about an existing alarm condition

- a system operation history

- information used in troubleshooting

Logs are viewed through the UAS Manager. Logs for the UAS can also be viewed through the command line interface.

Audio Access logs

This section contains Audio Access logs.

2049 AUDIO_BAD_INPUT_DATA

Message = 'Invalid input data: . Provisioning mismatch with existing audio'

EventType='error'

Probable Cause: Generated when the system is unable to play the requested audio. The segment ID or alias does not exist, or there is some other provisioning error associated with this segment.

Corrective Action: Provision the desired audio with the correct segment identifier, alias, or segment structure for sets and sequences.

2050 AUDIO_PROGRAM_ERROR

Message = 'Unexpected code condition: <some error>'

EventType='error'

Probable Cause: Generated when an unexpected condition occurs in the code. These events are considered to be very unlikely, and are due to programming errors within the system.

Corrective Action: This error will require a code change to correct.

2051 AUDIO_LANGUAGE_NOT_SET

Message = 'Language selector not set'

EventType='error'

Probable Cause: Cannot play a variable without knowing the language.

Corrective Action: The play request should be corrected to follow the documented method for specifying the language for an audio variable in a play request.

2052 PROTOCOL_VALUE_INVALID

Message = 'Parameter <parameter name> has invalid or out of range value in <value>'

EventType='error'

Probable Cause: Generated when the value of a parameter in the play message is invalid or out of range. This error covers any case where an input parameter for a play message does not match the protocol specification or the parameter.

Corrective Action: The play request should be corrected to pass valid values according to the published protocol.

2053 PROTOCOL_DISALLOWED_OPTIONAL_PARM

Message = 'Parameter <parameter 1> not allowed with parameter <parameter 2> in <command> command'

EventType='error'

Probable Cause: Generated when an MGCP message contains a parameter that makes another parameter invalid, and that invalid parameter is present. In the Audio Access feature, specifying an audio segment through its segment identifier and its alias is an invalid combination.

Corrective Action: The play request should be corrected to pass valid parameters. The play message should use either the segment identifier or the alias, but not both.

2054 AUDIO_NFS_MOUNT_ERROR

Message = 'Unable to mount directory from db server'

EventType='error'

Probable Cause: Error mounting the APS directory used to hold record or override audio. The database server has not been configured correctly to interwork with the audio server.

Corrective Action: The database server should be installed correctly

2055 AUDIO_DBSERVER_HOSTNAME_NOT_SET

Message = 'DB server hostname not found in conf_lookup file'

EventType='error'

Probable Cause: System not configured with hostname of db server. The audio server has not been installed correctly.

Corrective Action: The audio server should be installed correctly to interwork with the database server.

2056 AUDIO_NEW_AUDIO_ID_ERROR

Message = 'DB Server request for new id fails'

EventType='error'

Probable Cause: Error getting new audio ID from web server. The web server is probably not available on the network.

Corrective Action: Make sure the web server is working correctly and available on the network.

2057 AUDIO_ALIASSERVER_CONNECT_ERROR

Message = 'Cannot connect to alias server to get segid for alias <alias>'

EventType='error'

Probable Cause: The aliasServer process is not running.

Corrective Action: Make sure the aliasServer process is installed on the UAS and working correctly.

2058 AUDIO_RESYNC_ERROR

Message = 'Resync audio on restart failed for reason: <error description>'

EventType='error'

Probable Cause: The primary APS (and secondary, if it exists) is not online.

Corrective Action: Make sure the APS is working correctly. Once the APS is back online, use the APS GUI to provision audio to the UAS.

IVR Service logs

This section contains IVR Service logs. The logs appear in the following groups:

- initialization group
- miscellaneous group

Initialization group

These logs are generated during IVR Service initialization. Once the NMS CT daemon and Clock Fallback Manager services are started, the NMS oamsys program is invoked to load and initialize the NMS cards. A number of logs are generated in the process. If any failures are encountered, the callp application reattempts the operation.

4097+ IVR_ERROR_LOG

EventType='error'

Message='call to start ctdaemon failed'

Probable Cause: An attempt was made to start the ctdaemon core process, but the attempt failed.

Corrective Action: This error is likely due to a mis-installation of the UAS software. First, reboot the UAS to see if the error recurs, then uninstall and reinstall the UAS.

4097+ IVR_ERROR_LOG

EventType='error'

Message='call to oamsys failed'

Probable Cause: An attempt was made to invoke oamsys to load and initialize the NMS cards, but the attempt failed.

Corrective Action: This error is likely due to amis-installation of the UAS software. First , reboot the UAS to see if the error recurs, then uninstall and reinstall the UAS.

4098+ IVR_INFO_LOG

EventType='information'

Message='call to stop ctdaemon failed or ctdaemon was not running'

Probable Cause: This log can occur in two situations. 1) The ctdaemon was running, but the attempt to stop it failed 2) The ctdaemon was not running previously. This is the normal case on a system reboot.

Corrective Action: None. In the absence of other logs, this represents an error condition that is corrected automatically.

4098+ IVR_INFO_LOG

EventType='information'

Message='call to stop ctdaemon succeeded'

Probable Cause: The ctdaemon was running and it was successfully stopped.

Corrective Action: None. This is a normal condition on initialization of the UAS.

4098+ IVR_INFO_LOG

EventType='information'

Message='call to start ctdaemon succeeded'

Probable Cause: The ctdaemon was successfully started.

Corrective Action: None. This is a normal condition on initialization of the UAS.

4098+ IVR_INFO_LOG

EventType='information'

Message='call to oamsys succeeded'

Probable Cause: The invocation of oamsys was successful. The NMS boards were loaded and initialized.

Corrective Action: None. This is a normal condition on initialization of the UAS.

Miscellaneous group

The following logs are generated when various errors occur.

4099 PC_BAD_REGULAR_EXPRESSION_FORMAT

Message = 'Invalid regular expression for play collect: <regular expression string>'

EventType='error'

Probable Cause: The gateway controller has sent a badly formatted string that the parser accepted as valid, but the play-collect code perceives as invalid.

Corrective Action: Open an SR against the gateway controller.

4100 PC_COLLECT_DIGITS_FAILED

Message = 'adiCollectDigits failed'

EventType='error'

Probable Cause: There is a problem with the hardware or ctdaemon.

Corrective Action: Check for existing hardware alarms.

4101 PR_ALLOCATE_RECORD_BUFFER_FAILED

Message = 'allocate memory for record operation failed'

EventType='error'

Probable Cause: The system has run out of free memory.

Corrective Action: Reboot the system, and open an sr against the UAS.

4102 PR_RECORD_OPERATION_FAILED

Message = 'record operation failed'

EventType='error'

Probable Cause: There is a problem with the UAS or NMS software.

Corrective Action: Check for existing hardware alarms, and open an sr against the UAS.

4103 PR_RECORD_MISSING_AUDIO

Message = 'record operation failed because <prompt indicator> audio was not present'

EventType='error'

Probable Cause: The announcement used for the prompt has not been provisioned.

Corrective Action: Provision the audio in the APS and wait for audio distribution to the UAS.

4104 PR_RECORD_ID_ALREADY_USED

Message = 'record operation rejected because id <record id> is already in use'

EventType='error'

Probable Cause: An announcement with the specified id has already been provisioned or the id has been used for a temporary recording.

Corrective Action: Open an sr against the call server.

4105 IVR_SOFTW_FAILURE

Message = 'Unknown failure - <failure description>'

EventType = 'error'

Probable Cause: An unexpected software error has occurred in the hardware interface software.

Corrective Action: If the problem persists, contact the next level of support.

4108 HW_NMS_KEYWORD_CONFIG_ERROR

Message = 'NMS oam error for keyword <keyword>.'

EventType = 'error'

Probable Cause: There is a problem with an NMS configuration file.

Corrective Action: If the problem persists contact the next level of support.

30721 CG6K_ETHERNET_HALF_DUPLEX

Message = 'Interface %d on CG6000C in slot %d is in HALF-DUPLEX mode. For optimal performance, it should be in FULL-DUPLEX mode.\nPlease check network configuration'

EventType = 'error'

Probable Cause: An ethernet port on the CG6000C is connected to either a hub or to a switch port configured for half-duplex operation.

Corrective Action: Plug the CG6000C into a full-duplex switch port.

30722 CG6K_ETHERNET_10BT

Message = 'Interface %d on CG6000C in slot %d is in 10-baseT mode. This will limit capacity. For optimal performance, it should be in 100-baseT mode.\nPlease check network configuration'

EventType = 'error'

Probable Cause: An ethernet port on the CG6000C is connected to a 10-baseT port on a switch or hub.

Corrective Action: Reconfigure the port on the switch for 100BaseT operation.

H.248 Call Agent Connection logs

This section contains H.248 Call Agent Connection logs.

8193+ SW_ERR_LOG

EventType='error'

Message='Software error: <messageDirection> message thread died and was restarted.'

Probable Cause: Internal software error

Corrective Action: If a pattern of these logs develops, contact the next level of support.

8193+ SW_ERR_LOG

EventType='error'

Message='Software error: Inter-thread messaging error; queue write failed.'

Probable Cause: Internal software error

Corrective Action: If a pattern of these logs develops, contact the next level of support.

8193+ SW_ERR_LOG

EventType='error'

Message='Software error: Interface object was null after parse.'

Probable Cause: Internal software error.

Corrective Action: If a pattern of these logs develops, contact the next level of support.

8193+ SW_ERR_LOG

EventType='error'

Message='Software error: Command in progress timer expired: tid=<transactionId>.'

Probable Cause: Internal software error.

Corrective Action: If a pattern of these logs develops, contact the next level of support.

8194 + SYNTAX_ERR_LOG

EventType='error'

Message='Syntax error: premature end of message. In message: <message>'

Probable Cause: Incoming message was incomplete.

Corrective Action: Contact the next level of support with the full text of the log..

8194 + SYNTAX_ERR_LOG

EventType='error'

Message='Syntax error: bad audio package segment id parameter. In message <message>'

Probable Cause: Syntax error in an audio package sid=<> parameter portion of an incoming message.

Corrective Action: Contact the next level of support with the full text of the log.

8194 + SYNTAX_ERR_LOG

EventType='error'

Message='Syntax error - bad request." In message: <message> Near <message fragment>

Probable Cause: Syntax error at the request level of an incoming message.

Corrective Action: Contact the next level of support with the full text of the log.

8194 + SYNTAX_ERR_LOG

EventType='error'

Message='Syntax error - bad transaction. In message: <message> Near: <message fragment>"'

Probable Cause: Syntax error at the transaciton level of an incoming message.

Corrective Action: Contact the next level of support with the full text of the log.

8194 + SYNTAX_ERR_LOG

EventType='error'

Message='Syntax error - bad action. In message:<message> Near <message fragment>'

Probable Cause: Syntax error at the action level of an incoming message.

Corrective Action: Contact the next level of support with the full text of the log.

8194 + SYNTAX_ERR_LOG

EventType='error'

Message='Syntax error - bad command. In message: <message> Near: <message fragment>'

Probable Cause: Syntax error at the command level of an incoming message.

Corrective Action: Contact the next level of support with the full text of the log.

8195 VALIDATE_ERR_LOG

EventType='error'

Message='Message validation failed: <messageText>'

Probable Cause: An incoming message was invalid.

Corrective Action: Find the related Call Processing Log that explains the reason for the failure and contact the next level of support.

8196 SM_PROBLEM_LOG

EventType='error'

Message='Unable to <action> state data.'

Probable Cause: <action> is either "allocate" or "locate" Either a new state data block cannot be allocated to process a new call or the state data block assigned to an existing call cannot be located.

Corrective Action: Find the related Call Processing Log and contact the next level of support.

MGCP Call Agent Connection logs

This section contains MGCP Call Agent Connection logs.

8193+ SW_ERR_LOG

EventType='error'

Message='Software error: <messageDirection> message thread died and was restarted.'

Probable Cause: The "ingoing" or "outgoing" message processing thread has died and an attempt will be made to restart it.

Corrective Action: If a pattern of these logs develops, contact the next level of support.

8193+ SW_ERR_LOG

EventType='error'

Message='Software error: Inter-thread messaging error; queue write failed.'

Probable Cause: An error was encountered while the callp program attempted to insert a message on the queue of outgoing messages.

Corrective Action: If a pattern of these logs develops, contact the next level of support.

8193+ SW_ERR_LOG

EventType='error'

Message='Software error: Parser panic (<optional error msg from parser>) near token <token> on line <line> and token <token> on line <line> in message: <messageText>'

Probable Cause: The message parser found itself in an unknown or unrecoverable state.

Corrective Action: n/a. The parser will exit and will be restarted. If a pattern of these logs develops, contact the next level of support.

8193+ SW_ERR_LOG

EventType='error'

Message='Software error: Lexer panic (<optional error msg from lexer>) near token <token> on line <line> and token <token> on line <line> in message: <messageText>'

Probable Cause: The lexer component of the message parser found itself in an unknown or unrecoverable state.

Corrective Action: n/a. The parser will exit and will be restarted. If a pattern of these logs develops, contact the next level of support.

8193+ SW_ERR_LOG

EventType='error'

Message='Software error: Token object panic (<optional error msg from token object>) near token <token> on line <line> and token <token> on line <line> in message: <messageText>'

Probable Cause: The token object component of the message parser found itself in an unknown or unrecoverable state.

Corrective Action: n/a. The parser will exit and will be restarted. If a pattern of these logs develops, contact the next level of support.

8193+ SW_ERR_LOG

EventType='error'

Message='Software error: Interface object was null after parse.'

Probable Cause: Internal software error.

Corrective Action: Contact the next level of support.

8193+ SW_ERR_LOG

EventType='error'

Message='Internal parser error: NoToken.'

Probable Cause: Internal software error.

Corrective Action: Contact the next level of support.

8194 + SYNTAX_ERR_LOG

EventType='error'

Message='Syntax error near token <token> on line <line> and token <token> on line <line> in message: <messageText>'

Probable Cause: The message parser detected a syntax error in an incoming message. Tokens that the parser thinks are near the error are provided. Sometimes the log will not correctly indicate the location of the syntax error, but quite often it will. The text of the message is also provided.

Corrective Action: Contact the next level of support with the full text of the log.

8195 VALIDATE_ERR_LOG

EventType='error'

Message='Message validation failed: <messageText>'

Probable Cause: An incoming message was invalid. The text of the message is provided.

Corrective Action: Find the related Call Processing Log that explains the reason for the failure and contact the next level of support.

8196 SM_PROBLEM_LOG

EventType='error'

Message='Unable to <action> state machine.'

Probable Cause: <action> is either "allocate" or "locate" Either a state machine cannot be allocated to process a new call or the state machine assigned to an existing call cannot be located.

Corrective Action: Find the related Call Processing Log that explains the reason for the failure and contact the next level of support.

8197 GWC_RESTART_LOG

EventType='information'

Message='Restart of GWC <gwc-name> detected.'

Probable Cause: the GWC <gwc-name> has informed the UAS that it (the GWC) is restarting.

Corrective Action: This log is only for information and does not require an action.

8198 GWC_FAILOVER_LOG

EventType='information'

Message='Failover to GWC <gwc-name> was successful.'

Probable Cause: the UAS has switched its controller to GWC <gwc-name>.

Corrective Action: This log is only for information and does not require an action.

8199 GWC_FAILOVER_ERROR_LOG

EventType='information'

Message='Could not failover to invalid GWC <gwc-name>.'

Probable Cause: The UAS has been asked to switch to GWC <gwc-name> as its active controller, but <gwc-name> has not been datafilled on the UAS as a potential controller.

Corrective Action: Check datafill of GWC controller on the UAS.

Call Engine logs

This section contains Call Engine logs.

12289 PROTOCOL_PARM_DUPLICATE

Message = 'Parameter <parm_name> already set in <operation>.'

EventType='error'

Probable Cause: Generated during parsing of an incoming MGC-MG control message, this log indicates that the specified control operation contained <parm_name> multiple times, and this parameter may not be duplicated within this operation.

Corrective Action: Check the control messaging being sent from the MGC for errors.

12290 PROTOCOL_VALUE_INVALID

Message = 'Parameter <parm_name> has invalid or out of range value in <operation>'

EventType='error'

Probable Cause: Generated during parsing of an incoming MGC-MG message, this log indicates that the indicated <operation> contained an invalid or out of range value for the parameter <parm_name>.

Corrective Action: Check the control messaging being sent from the MGC for errors.

12291 PROTOCOL_UNSUPPORTED_PROTOCOL

Message = 'Unsupported protocol version : <version>'

EventType='error'

Probable Cause: Generated during parsing of an incoming MGC-MG message, this log indicates that the specified protocol <version> is not supported by the UAS.

Corrective Action: Check the control messaging being sent from the MGC for incorrect protocol version.

12292 PROTOCOL_UNSUPPORTED_PARAMETER

Message = 'Unsupported parameter <parm_name> received in <operation> command'

EventType='error'

Probable Cause: Generated during parsing of an incoming MGC-MG control message, this log indicates that the message contained <parm_name>, which is unsupported for the specified <operation>.

Corrective Action: Check the control messaging being sent from the MGC for errors.

12293 PROTOCOL_MISSING_MANDATORY_PARM

Message = 'Mandatory parameter <parm_name> missing from <operation>"

EventType='error'

Probable Cause: Generated during parsing of an incoming MGC-MG control message, this log indicates that the specified <operation> is missing the mandatory parameter <parm_name>.

Corrective Action: Check the control messaging being sent from the MGC for errors.

12294 PROTOCOL_MISSING_OPTIONAL_PARM

Message = 'Parameter <parm_name1> required with parameter <parm_name2> in <operation> command'

EventType='error'

Probable Cause: Generated during parsing of an incoming MGC-MG control message, this log indicates that the specified <operation> contained the optional parameter <parm_name2>, but is missing the optional parameter <parm_name1>, and both parameters must be specified together.

Corrective Action: Check the control messaging being sent from the MGC for errors.

12295 PROTOCOL_DISALLOWED_OPTIONAL_PARM

Message = 'Parameter <parm_name1> not allowed with parameter <parm_name2> in <operation> command'

EventType='error'

Probable Cause: Generated during parsing of an incoming MGC-MG control message, this log indicates that the specified <operation> contained the optional parameters <parm_name1> and <parm_name2>, and they may not be specified in the same operation.

Corrective Action: Check the control messaging being sent from the MGC for errors.

12296 PROTOCOL_BAD_WILDCARD

Message = 'Wildcard endpointID not allowed for <operation> command'

EventType='error'

Probable Cause: Generated during parsing of an incoming MGC-MG control message, this log indicates that the specified <operation> contained a wildcard endpointId (or terminationId), which is not allowed in this operation.

Corrective Action: Check the control messaging being sent from the MGC for errors.

The following is a list of call processing and Maintenance State Machines logs.

12297 CALLP_BAD_EXTERNAL_EVENT

Message = 'Invalid event <operation> received from MGC'

EventType='error'

Probable Cause: The specified <operation> was received from the MGC during the processing of a call, and this operation is not supported by the UAS.

Corrective Action: Check the control messaging being sent from the MGC for unsupported operations.

12298 CALLP_BAD_INTERNAL_EVENT

Message = 'Invalid event <event_type> received from internal component'

EventType='error'

Probable Cause: The specified <event_type was received from an internal UAS software component during the processing of a call, and the event type is unknown. This indicates a software error.

Corrective Action: Contact the next level of support.

12299 CALLP_SEND_FAILURE

Message = 'Couldn't send message to MGC - internal error'

EventType='error'

Probable Cause: The call processing software could not send a message through the parser to the MGC. This indicates a software error.

Corrective Action: Contact the next level of support.

12300 CALLP_CONN_DELETED

Message = 'Command received for connection already deleted. EndpointId=<endpointId>, CurrConnectionId=<currConnectionId>, RecvConnectionId=<recvConnectionId>, CallId=<callId>, TransId=<transactionId>,State=<callState>, CurrEvent=<event>'

EventType='error'

Probable Cause: An MGC-MG control operation was received from the MGC for an <endpointId> which is inactive, but for a connection ID that is no longer active. <currConnectionId> is the connectionId of the current connection on this <endpointId>, if any. <recvConnectionId> is the connectionId received in <event>. <callId> is the callId of the current connection active on <endpointId>, if any. <transactionId> is the transactionId of the <event>. <callState> is the state of the active connection on <endpointId>, if any.

Corrective Action: This is an error from the UAS/UGW perspective because the message cannot be processed, but is not necessarily an error form the MGC perspective, as it may be encountered during cleanup type situations.

12301 CALLP_INVALID_FOR_STATE

Message = 'Command <operation> not valid in state <state>. EndpointId=<endpointId>, ConnectionId=<connectionId>, CallId=<callId>, TransId=<transactionId>.'

EventType='error'

Probable Cause: The specified MGC-MG control <operation> was received from the MGC during call processing of the thread for <endpointId>, and this operation is not valid in the current <state>. <connectionId> is the connectionId of the currently active connection for <endpointId>. <callId> is the callId of the currently active connection for <endpointId>. <transactionId> is the transactionId of <operation>. This may happen when the MGC does not correctly react to an error from a previous MGC-MG control operation.

Corrective Action: Check the control messaging being sent from the MGC for invalid call flow.

12302 CALLP_THREAD_RESTARTED

Message = 'Call processing thread for endpointId <endpointId> died - restarting. ConnectionId=<connectionId>, CallId=<callId>, TransId=<transactionId>, State=<callState>, CurrEvent=<event>.'

EventType='error'

Probable Cause: The call processing software thread associated with <endpointId> died due to an unhandled software error, but was restarted. <connectionId> is the connectionId of the current connection on this <endpointId>. <callId> is the callId of the current connection active on <endpointId>. <transactionId> is the transactionId of the

<event>. <callState> is the state of the active connection on <endpointId>.

Corrective Action: Contact the next level of support.

12303 CALLP_MGC_NOT_RESPONDING

Message = 'Call cleared due to no response from MGC. EndpointId=<endpointId>, ConnectionId=<connectionId>, CallId=<callId>, TransId=<transactionId>'

EventType='error'

Probable Cause: During processing of a connection, the UAS/UGW originated a message to the MGC, but never received an acknowledgement within the defined time period. <endpointId> is the endpointId of the call which was cleared. <connectionId> is the connectionId of the call, <callId> is the callId of the call, and <transactionId> is the transactionId of the operation which timed out. This may indicate a network problem with messages not reaching the intended destination or an application problem in the MGC where it does not respond to the message.

Corrective Action: Check for network failures. Contact the next level of support to troubleshoot potential MGC problems.

12304 CALLP_SOFTW_FAILURE

Message = 'Unknown failure - <failure text>'

EventType='error'

Probable Cause: An unexpected software error occurred during call processing. <failure text> provides the details of the failure.

Corrective Action: Contact the next level of support.

12305 CALLP_MTCE_THREAD_RESTARTED

Message = 'Maintenance thread died - restarting. TransId=<transactionId>, CurrEvent=<event>.'

EventType='error'

Probable Cause: The maintenance thread died due to an unhandled software error, but was restarted. <transactionId> is the transaction of the received <event> that was being processed when this occurred.

This typically indicates a software problem.

Corrective Action: Contact the next level of support.

12306 CALLP_MGC_NOT_RESPONDING_FOR_MTCE

Message = 'Retransmitting startup operation due to no response from MGC.'

EventType='error'

Probable Cause: During initiation of the MGC-MG connection, the UAS/UGW sends a startup operation to notify that the UAS/UGW is becoming available. When multiple timeouts occur waiting for the response to this operation, the UAS/UGW will retransmit the startup operation with a new transactionId. This typically indicates that the MGC is not ready, but it may also indicate a network problem.

Corrective Action: Check status of MGC. Check for network failures.

12307 CALLP_INITIALIZATION_PROBLEM

Message = 'Failed to initialize callp component: <specificComponent>'

EventType='error'

Probable Cause: During initialization of the callp application, the <specificComponent> failed to initialize, preventing the application from coming into service.

Corrective Action: Check for additional logs indicating the specific problem.

12308 CALLP_INITIALIZATION_IN_PROGRESS

Message = 'Call processing is initializing'

EventType='information'

Probable Cause: The call processing application is initializing all of its subcomponents after starting the process.

Corrective Action: n/a. This is to inform of normal initialization.

12309 CALLP_READY_BUT_LOCKED

Message = 'Call processing is ready, but waiting for response from MGC'

EventType='information'

Probable Cause: The call processing application is ready (either completed initialization or returning from administrative locked state), but is not yet allowing new connections because the call agent has not responded to the restart operation.

Corrective Action: None at this point. This is to inform of normal initialization. This log should be closely followed by log 12310 to indicate successful initialization. If there is no response from the MGC, log 12306 will be generated when the timeout condition occurs.

12310 CALLP_ALLOWING_CONNECTIONS

Message = 'Call processing is allowing new connections'

EventType='information'

Probable Cause: The call processing application is now allowing new connections.

Corrective Action: n/a. This is to inform of normal initialization.

12311 CALLP_IS_BEING_LOCKED

Message = 'Call processing is being locked by administrative action'

EventType='information'

Probable Cause: An administrative request has been made to put the call processing application into locked state. It will be moved to locked state after all existing connections have ended.

Corrective Action: n/a. This is to inform of action taken by an administrator.

12312 CALLP_IS_ADMIN_LOCKED

Message = 'Call processing is now in administrative locked state'

EventType='information'

Probable Cause: An administrative request was made to put the call processing application into locked state, and all existing connection

have ended.

Corrective Action: n/a. This is to inform of action taken by an administrator.

12313 CALLP_TERMINATION_REQUESTED

Message = 'Call processing shutting down at the request of the program manager'

EventType='information'

Probable Cause: Call processing receiving a request from the program manager to terminate.

Corrective Action: n/a. This is to inform of normal system shutdown.

12314 CALLP_ABNORMAL_TERMINATION

Message = 'Call processing is terminating for reason: <termination_reason>'

EventType='error'

Probable Cause: Call processing is terminating in some abnormal way. When the termination reason is known, it will be shown as <termination_reason>; otherwise the value "unknown" will be shown.

Corrective Action: Contact the next level of support.

12315 CALLP_CONFIGURATION_VALID

Message = 'Call processing configuration is valid'

EventType='information'

Probable Cause: During call processing initialization, the configuration has been determined to be valid.

Corrective Action: n/a. This is to inform of normal initialization.

12316 CALLP_IS_ADMIN_UNLOCKED

Message = 'Call processing is now in administrative unlocked state'

EventType='information'

Probable Cause: An administrative request was made to put the call processing application into the unlocked state. This will result in a startup message to the MGC, and new connections will be allowed once the call MGC has acknowledged the restart message.

Corrective Action: n/a. This is to inform of action taken by an administrator.

12317 CALLP_CONNECTIONS_DELETED

Message = 'Call processing is deleting <numconns> remaining active connections to change to administrative locked state'

EventType='information'

Probable Cause: Following an administrative request to put the call processing application into locked state, a timer is started based on the delay specified in the request. At the expiration of this timer, all active connections are forcibly terminated. <numconns> indicates the number of connections active at expiration of the timer.

Corrective Action: n/a. This is to inform of normal events following the UAS/UGW being put in administrative locked state.

12318 CALLP_THREAD_CLEANED

Message = 'Call processing thread for endpointId <epid> was automatically deleted due to timeout. ConnectionId=<connid>, CallId=<callid>, TransId=<transid>, State=<state>, CurrEvent=<currevent>'

EventType= 'error'

Probable Cause: Call server either created a bearer endpoint that was never used, or failed to delete a bearer endpoint.

Corrective Action: If problem persists, issue sr for UAS design investigation.

12319 CALLP_WAIT_FOR_CM_INIT

Message = 'Main callp thread waiting for the card maintenance subsystem to complete card initialization. Elapsed time: <n> seconds.'

EventType='information'

Probable Cause: The main call processing thread waits for the card maintenance subsystem to complete card initialization before allowing other parts of the system to initialize. This is an log to flag that the main thread is waiting. This is not a problem unless card maintenance is unable to complete card initialization. This log is generated once per minute until card initialization is completed. <n> is the number of seconds since the startup of card maintenance.

Corrective Action: If card initialization does not complete, then report the problem to the support group.

Conferencing Service logs

This section contains Conferencing Service logs.

18433 CONF_LISTEN_INUSE

Message = 'Conference::listen inuse <numPortsInuse> max <numPortsReserved>'

EventType='error'

Probable Cause: call server request exceeds available capacity. Probable call server software error.

Corrective Action: attempt a new conference.

18434 CONF_UNLISTEN_INUSE

Message = 'Conference::unlisten inuse <numPortsInuse>'

EventType='error'

Probable Cause: Issue SR UAS conferencing

Corrective Action: attempt a new conference.

18435 CONF_CANT_DOWNSIZE

Message = 'Conference::modify - cant downsize numPorts below curr usage'

EventType='error'

Probable Cause: call server request is invalid. Issue SR against call server.

Corrective Action: none needed

18436 CONF_DELETE_MONPORT_ERROR

Message = 'Conference::modify - cant del monport with listeners'

EventType='error'

Probable Cause: call server request is invalid. Issue SR against call server

Corrective Action: none needed

18437 CONF_CANT_LOCATE_POOL

Message = 'ConferenceManager::create cant locate pool <poolnum>'

EventType='error'

Probable Cause: NMS service not started

Corrective Action: restart callp manually

18438 CONF_RESERVE_PORT_ERROR

Message = 'ConferenceManager::create cant reserve n ports. Possibly full'

EventType='error'

Probable Cause: conferencing limits reached. call server should know that, so issue SR to them

Corrective Action: none needed

18439 CONF_INVALID_POOLNUM

Message = 'ConferenceManager::validate cant locate pool <poolnum>'

EventType='error'

Probable Cause:NMS service not started

Corrective Action: restart callp manually

18440 CONF_RESOURCE_UNAVAILABLE

Message = 'ConferenceManager::validate -not enough free resources. free: <freeSize> requested: <totalPorts>'

EventType='error'

Probable Cause: conferencing limits reached. call server should know that, so issue SR to them

Corrective Action: none needed

18442 CONF_UNKNOWN_POOLNUM

Message = ' cant find pool. num: <poolNum>'

EventType='error'

Probable Cause: unknown. SR UAS conf

Corrective Action: restart callp if persists

18443 CONF_DELETE_UNKNOWN_CONFID

Message = 'ConferenceManager::destroy - no conf - conId:'

EventType='error'

Probable Cause: conference already deleted. May be a timing issue

Corrective Action: none needed

18444 CONF_NULL_CONFPOOL

Message = ' confpool null'

EventType='error'

Probable Cause: NMS service not started

Corrective Action: restart callp manually

18445 CONF_MISSING_CONF_MANAGER

Message = 'ConferenceStateMachine ctor - no conf mgr'

EventType='error'

Probable Cause: Unknown

Corrective Action: Restart callp. If the problem persists, contact UAS support.

18446 CONF_NULL_COMMAND_HEADER

Message = 'command object, command header null'

EventType='error'

Probable Cause: unknown.

Corrective Action: Issue an SR for UAS design investigation.

18447 CONF_UNKNOWN_MGCP_MESSAGE

Message = "unknown MGCP message <MessageCode>'

EventType='error'

Probable Cause: protocol mismatch. Issue SR.

Corrective Action: check for call server/UAS software version incompatibility

18448 CONF_CREATE_BAD_SIGNAL

Message = 'CRCX wrong sig <signalType>'

EventType='error'

Probable Cause: protocol mismatch. Issue SR.

Corrective Action: Check for call server/UAS software version incompatibility

18449 CONF_CREATE_INVALID_CONF

Message = 'ConferenceStateMachine::handleCRCXEvent conf create. cant locate conf'

EventType='error'

Probable Cause: unknown.

Corrective Action: Issue an SR for UAS design investigation.

18450 CONF_CREATE_RESPONSE_ERROR

Message = 'can't build response to CRCX <connection ID>'

EventType='error'

Probable Cause: unknown

Corrective Action: restart callp if persists

18451 CONF_RESPONSE_PROB_ALLCONFS

Message = 'can't build response to DLCX while deleting all confs'

EventType='error'

Probable Cause: unknown

Corrective Action: restart callp if persists

18452 CONF_DELETE

Message = 'ConferenceStateMachine::handleDLCXEvent deleting conf <connectionId>'

EventType='information'

Probable Cause: conference already deleted. May be a timing issue

Corrective Action: none needed

18453 CONF_DELETE_RESPONSE_ERROR

Message = 'can't build response to DLCX <connection ID>'

EventType='error'

Probable Cause: unknown

Corrective Action: restart callp if persists

18454 CONF_MODIFY_NULLCONF

Message = ' handle MDCX - Conf null'

EventType='error'

Probable Cause:config mismatch between UAS and call server

Corrective Action: run call server audit or restart

18455 CONF_POOL_CONFID_MISMATCH

Message = ' pool/confid mismatch: <confId1>/<poolId1> vs <confId2>/<poolId2>'

EventType='error'

Probable Cause:config mismatch between UAS and call server

Corrective Action: Run call server audit or restart.

18456 CONF_MODIFY_NO_SIGNAL

Message = ' MDCX - no signal present'

EventType='error'

Probable Cause: protocol mismatch

Corrective Action: Check version incompatibility between call server and UAS.

18457 CONF_MODIFY_BAD_SIGNAL

Message = 'MDCX wrong sig <signalType>'

EventType='error'

Probable Cause: protocol mismatch

Corrective Action: check version incompatibility between call server and UAS

18458 CONF_MODIFY_ATTRIBUTES_ERROR

Message = 'can't modify attributes for conf <connection ID."

EventType='error'

Probable Cause: unknown. look for other err logs

Corrective Action: Issue an SR for UAS design investigation.

18459 CONF_MODIFY_UNRESERVE_ERROR

Message = 'ConfPool::modify - can't unreserve %d'

EventType='error'

Probable Cause: software error

Corrective Action: Issue an SR for UAS design investigation.

18460 CONF_EVENT_COMMAND_UNSET

Message = 'EventCommand in AUCX is UNSET'

EventType='error'

Probable Cause: protocol mismatch

Corrective Action: Check version incompatibility between call server and UAS

18461 CONF_INVALID_EVENT_COMMAND

Message = 'EventCommand in AUCX is invalid type: <commandCode>'

EventType='error'

Probable Cause: protocol mismatch

Corrective Action: Check version incompatibility between call server and UAS

18462 CONF_MODIFY_RESPONSE_ERROR

Message = 'can't build response to MDCX <connection ID>'

EventType='error'

Probable Cause: unknown

Corrective Action: restart if persists

18463 CONF_THREAD_DEATH

Message = 'ConferenceStateMachine::threadCallback - death of thread'

EventType='error'

Probable Cause: trap or exception. check for other err logs. Issue SR

Corrective Action: none needed. Self correcting.

18464 CONF_INIT_FAILURE

Message = 'hw init fail'

EventType='error'

Probable Cause: unknown

Corrective Action: restart

18465 CONF_CREATE_ERROR

Message = 'ConfMgr::create new conf'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for UAS design investigation.

18466 CONF_INVALID_MODIFY_OPERATION

Message = 'Conference::modifying play port criteria not supported'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for UAS design investigation.

18467 CONF_MODIFY_RESERVE_ERROR

Message = 'ConfPool::modify - cant reserve <num ports>'

EventType='error'

Probable Cause: there are not enough ports available for the request

Corrective Action: none

18468 CONF_RESERVE_NOTICE

Message = 'ConfPool::reserve %d %d %d'

EventType='information'

Probable Cause:

Corrective Action: none

18469 CONF_UNRESERVE_NOTICE

Message = 'ConfPool::unreserve size=%d numports to unreserve=%d'

EventType='information'

Probable Cause:

Corrective Action:

18470 CONF_INVALID_HARDWARE

Message = 'ConferenceManager::instance -- DCB no longer supported'

EventType='error'

Probable Cause: Programming error

Corrective Action: Issue SR

18471 CONF_DELETE_ERROR

Message = 'threadHandleEvent - unable to destroy conf <conference id>')'

EventType='error'

Probable Cause: protocol mismatch

Corrective Action: check version incompatibility between call server and UAS

18472 CONF_EVENT_ERROR

Message = 'handle event complete. err rc=<return code>'

EventType='error'

Probable Cause: unknown

Corrective Action: restart if persists

18473 CONF_INVALID_RESPONSE

Message = 'conferenceStateMachine::sendResponse - cant validate response'

EventType='error'

Probable Cause: trap or exception. check for other err logs. Issue SR

Corrective Action: none needed. Self correcting.

18474 CONF_NMS_ERROR

Message = 'NMS Error: <error code>'

EventType='error'

Probable Cause: a call to the underlying NMS software produced an error

Corrective Action: restart

18475 CONF_NMSCONFMGR_HW_ERROR

Message = 'NMSConfMgr ctor - cant init hw'

EventType='error'

Probable Cause: underlying NMS software problems prevents system from coming up

Corrective Action: check system configuration and restart

18476 CONF_NMS_HW_INIT_ERROR

Message = 'NMS hw init fail'

EventType='error'

Probable Cause: underlying NMS software problems

Corrective Action: check system configuration and restart

18477 CONF_NMS_NO_MON_PORT_RESERVED

Message = 'NMSConference::monitor - no mon port reserved'

EventType='error'

Probable Cause: attempting to add listen only members to conference, but no monitor port active

Corrective Action: problem in Gateway

18478 CONF_NMS_MON_PORT_ERROR

Message = 'NMSConference::monitor - no real listen()er. conf not estab'

EventType='error'

Probable Cause:

Corrective Action:

18479 CONF_NMS_MONITOR_FAIL

Message = 'NMSConference:monitor fail'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for design investigation.

18480 CONF_NMS_UNMONITOR_ERROR

Message = 'NMSConference::unmonitor - ep not found in mon list'

EventType='error'

Probable Cause: gateway and audio server out of sync

Corrective Action: Issue an SR for design investigation.

18481 CONF_MDCX_ONOFF_ERROR

Message = 'MDCX onoff sig without requestid'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18482 CONF_AUCX_RESPONSE_ERROR

Message = 'can't build response to AUCX <connection id>'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18483 CONF_CSM_BAD_SIGNAL

Message = 'ConferenceStateMachine::handleSignalRequest wrong sig <signal type>'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18484 CONF_SRF_ABORTED

Message = 'ConferenceStateMachine::srfAborted - thread not running'

EventType='error'

Probable Cause: nms error

Corrective Action: restart callp. check h/w if persists

18485 CONF_SRF_COMPLETED

Message = 'ConferenceStateMachine::srfComplete - thread not running'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Restart callp. If problem persists, contact UAS support.

18486 CONF_SRF_COMPLETE_NTFY_PROB

Message = 'ConferenceStateMachine::handleSrfCompleteEvent- cant build ntfy'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18487 CONF_SRF_SEND_NTFY_ERROR

Message = 'ConferenceStateMachine::handleSrfCompleteEvent - Unable to send NTFY message'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18488 CONF_SRF_MISSING_REASON

Message = 'ConferenceStateMachine::handleSrfCompleteEvent completionReason missing'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18489 CONF_SRF_REASON_INVALID

Message = 'ConferenceStateMachine::handleSrfCompleteEvent- cant validate reason'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18490 CONF_SRF_BRIEF_SIGNAL_UNSUPPORTED

Message = 'brief sig not curr supported in conferencing srf'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for design investigation.

18491 CONF_NMS_ADD_PLAY_ERROR

Message = 'NMSConference:create play member fail'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18492 CONF_CMGR_CREATE_INVALID_CONF

Message = 'ConfMgr::conf create. cant locate conf for connection <connection id>'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18493 CONF_DELETE_PMROW_ERROR

Message = 'ConfMgr - unable to destroy pm row for conf <conference id>'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18494 CONF_MODIFY_PMROW_ERROR

Message = 'ConfMgr - unable to modify pm row for conf <conference id>'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18495 CONF_ALL_PORTS_BUSY

Message = 'Conference - get_ep_port fails: all reserved ports in use'

EventType='error'

Probable Cause: All reserved ports for the conference are in use. Mismatch in tracking ports between the call server and the UAS.

Corrective Action: SR against UAS/call server

18496 CONF_MEMBER_NOT_FOUND

Message = 'NMSConference::release_ep_port - ep not found in active port list'

EventType='error'

Probable Cause: Cannot find the target endpoint leaving the conference. Mismatch in tracking ports between the call server and the UAS.

Corrective Action: SR against UAS/call server.

18497 CONF_NO_PLAY_PORT_FOR_CONFERENCE

Message = 'ConferenceStateMachine: cannot complete play for conf <conference id>: no play port'

EventType='error'

Probable Cause: The gateway controller requested a conference without a play port, and is now requesting a play.

Corrective Action: SR against UAS/gateway controller.

18498 CONF_CONFMGR_DELETE_ALL

Message = 'ConferenceStateMachine::handleDLCXEvent deleting ALL conf'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18499 CONF_INIT_HW_FAILURE

Message = 'ConfMgr ctor - cant init hw'

EventType='error'

Probable Cause: configuration or other problem is preventing hardware from initializing correctly

Corrective Action: try to restart the system

18500 CONF_GENERAL_ERROR

Message = 'General conferencing error: <more specific error string>'

EventType='error'

Probable Cause: unknown

Corrective Action: Issue an SR for design investigation.

18501 CONF_DELETE_PLAYPORT_ERROR

Message = 'Conference::modify - cant del play port with play active'

EventType='error'

Probable Cause: Call server is modifying a conference while an audio play is active

Corrective Action: issue sr against Call Server

18502 CONF_DELETE_NULLCONF

Message = 'handle DLCX - Conf null'

EventType='error'

Probable Cause: call server and UAS are out of sync

Corrective Action: Issue an SR for design investigation.

18503 CONF_DELETE_BY_INTERNAL_AUDIT

Message = 'ConfMgr - deleted conference conf/confpool <conference id>/<conf pool> due to timeout. Connection ID=<connection ID>'

EventType='error'

Probable Cause: call server either created a conference that was never used, or neglected to delete a completed conference

Corrective Action: If problem persists, issue an SR for design investigation.

Main Subagent logs

Main subagent logs do not have numbers assigned to them. These logs are put into the Windows Event Log, but are not sent as SNMP traps to the element manager. The logs are divided into the following groups:

- communications error group
- file system group
- internal error group
- invalid application request group
- rapid request group
- startup and termination group

Note: Main Subagent logs do not have numbers to identify them.

Communications error group

The system generates the logs in this section when miscellaneous communications problems exist.

Message = 'MainSubagentThread::main: message received is corrupt, length=<value>'

EventType='error'

Probable Cause: Either a socket communications error occurred or the Audio Server application sent an invalid request.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'MainSubagentThread::main: receive error, code=<value>'

EventType='error'

Probable Cause: The main subagent encountered a windows socket error. The numeric error code is provided in the message.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'deregister and reinitialize in main loop'

EventType='error'

Probable Cause: The main subagent may have lost its connection to the EMANATE master agent.

Corrective Action: Ensure that the EMANATE master agent service is running.

Message = 'send packet error, error code: <errorText>'

EventType='error'

Probable Cause: The main subagent failed in an attempt to send a message to another UAS process. The nature of the error is supplied in the <errorText> field.

Corrective Action: Contact the next level of support with the full text of the log.

Invalid application request group

When the main subagent receives an invalid request from an application, the system generates the logs in this section. An alarm notification ID displayed in the log can identify the component that is sending the alarm. A software problem in the application usually generates this group of logs. The logs should be reported to the support group.

Message = 'bad severity on an alarm, notification id=<id>'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'received a raise for already active alarm, notification id=<id>'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'received bad update-alarm message from application'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'received bad state change message from application'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'update alarm request made with same severity level. Request ignored, notification id =<id>'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'bad severity on update alarm message, notification id=<id>'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'update alarm request made for inactive alarm, notification id =<id>'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'received bad clear-alarm message from application'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'force clears are not supported, discarding clear with correlation id: <correlation id list>'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'normal clear, but no active alarms in correlation id list: <correlation id list>'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'received bad send-log message from application'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'received bad mo-init message from application'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'Removed <number> alarm(s) from active alarm table for component <component>. Application process probably restarted. '

EventType='information'

Probable Cause: An application performed an abnormal restart.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'received bad raise-alarm message from application'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'Unknown message type received'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'can't find notification id for update alarm request, notification id =<id>'

EventType='error'

Probable Cause: An application sent an invalid request to the main subagent.

Corrective Action: Contact the next level of support with the full text of the log.

Startup and termination group

The system generates the logs in this section during normal and abnormal startups of, and terminations to, the main subagent.

Message = 'MainSubagentThread.initPtmNameAndPort: host lookup error, code=<value>'

EventType='error'

Probable Cause: The main subagent could not determine the host name and its IP address. This may result in problems with the delivery of alarms and logs to the element manager.

Corrective Action: Contact the next level of support with the full text of the log.

Message = 'Master agent port number is <portNumber>'

EventType='information'

Probable Cause: The main subagent writes this log when it initializes.

Corrective Action: n/a

Message = 'failed to init socket, delay then try again ...'

EventType='error'

Probable Cause: The main subagent is unable to initialize the communications socket, which is used for communicating with Audio Server applications. This log is generated once a minute until the socket is initialized. This log would be generated if another main subagent was already running.

Corrective Action: Ensure that another main subagent is not running.

Message = 'Subagent shutting down at the request of the program manager'

EventType='information'

Probable Cause: This is normally the result of a system shut down or a program manager shut down.

Corrective Action: n/a

Message = 'Main subagent process initializing'

EventType='information'

Probable Cause: This log is generated when the main subagent is started with no command-line options.

Corrective Action: n/a

Message = 'Main subagent process initializing, program arguments: <arguments>'

EventType='information'

Probable Cause: This log is generated when the main subagent is started with the command-line options, which are included in the log.

Corrective Action: n/a

Message = 'Failed to get the name of the event message file'

EventType='error'

Probable Cause: When the main subagent processes each event in the Windows event log, it searches the registry for the name of the event message file that contains the static text for this event. This log is reported if the main subagent fails in its search of the registry. The main subagent terminates processing of the event and waits for the next event.

Corrective Action: Contact the next level of support with the full text of the log.

Node Mtc logs

This section contains Node Mtc logs. Node Mtc logs are generated by the Node Mtc thread, which runs as part of the callp application.

When the callp application initializes, it attempts to stop the NMS CT daemon and NMS Clock FallBack Manager services, which may or may not be running at the time. It then attempts to start the NMS CT daemon service (which in turn starts the NMS Clock Fallback Manager service), checking to make sure that both these NMS services have been successfully started. A number of logs are generated in the process. If any service failures are encountered, the callp application reattempts the operation, until both of these NMS services have been restarted successfully.

20481 NODEMTC_UNLOCK_REQ_EVENT

Message = 'Node Mtc subsystem received a UnLock Request event, whilst in a locked state.'

EventType='information'

Probable Cause: The Node Mtc sub-system received a request to unlock the node.

Corrective Action: n/a

20482 NODEMTC_LOCK_REQ_EVENT

Message = 'Node Mtc subsystem received a Lock Request event, whilst in a unlocked state.'

EventType='information'

Probable Cause: The Node Mtc sub-system received request to lock the node.

Corrective Action: n/a

20483 NODEMTC_LOCK_COMP_EVENT

Message = 'Node Mtc subsystem received a Lock Complete event, whilst in a shutting-down state.'

EventType='information'

Probable Cause: The Node Mtc sub-system has successfully completed locking the node, during a shutdown of the node.

Corrective Action: n/a

20484 NODEMTC_UNLOCK_COMP_EVENT

Message = 'Node Mtc subsystem received a UnLock Complete event, whilst in a initializing state.'

EventType='information'

Probable Cause: The Node Mtc sub-system has successfully completed unlocking the node, during node initialization.

Corrective Action: n/a

20485 NODEMTC_INSTANCE_ERROR

Message = 'Unable to create the instance of Node Mtc subsystem.'

EventType='error'

Probable Cause: Memory exhaustion.

Corrective Action: Free up system resources.

20486 CTDAEMON_SERVICE_SUCCESS

Message = 'The NMS CT daemon service was successfully <started/stopped>.'

EventType='information'

Probable Cause: UAS initialization

Corrective Action: n/a

20487 CFBM_SERVICE_SUCCESS

Message = 'The NMS Clock Fallback Manager service was successfully <started/stopped>.'

EventType='information'

Probable Cause: UAS initialization

Corrective Action: n/a

20488 SERVICE_SUCCESS

Message = 'The <name-of-service> service was successfully <started/stopped>.'

EventType='information'

Probable Cause: UAS initialization

Corrective Action: n/a

Callp Subagent logs

This section contains Callp Subagent logs. The logs are divided into the following groups:

- miscellaneous group
- pending config group

Miscellaneous group

The call subagent generates logs in this section.

24577 MTC_OPERATION_LOG

Message = 'Performing <operation> operation on <resource_name>'

Probable Cause: The Element Manager has requested a lock or unlock operation on the specified resource. Possible values for <operation> are LockForce, LockGraceful, and Unlock. <resource_name> identifies the resource being locked. The resource can be the node, a trunk group, a card, a carrier, a trunk (DS0) or an ATM port.

EventType='information'

24578 SA_STARTUP

Message = 'Callp subagent starting. Build timestamp is <timestamp>. Network element name is <name>.'

Probable Cause: The subagent thread, which is part of the callp process, is initializing. The build timestamp (software version) and the network element name are provided in the log.

EventType='information'

24581+ GENERIC_ERROR_LOG

Message = 'Call subagent error: could not read build stamp file'

EventType='error'

Probable Cause: The build stamp file may be missing or unreadable. The build stamp file is c:\uas\etc\BuildStamp.txt.

Corrective Action: Ensure that the file is present and is readable.

24586 APP_RESTART_LOG

Message = 'Restarting all applications'

EventType='information'

Probable Cause: A user at the UAS Element Manager requested an application restart. The callp subagent writes this log immediately before performing the restart.

Corrective Action: n/a

24587 SYS_REBOOT_LOG

Message = 'Rebooting the system'

EventType='information'

Probable Cause: A user at the UAS Element Manager requested a system reboot. The callp subagent writes this log immediately before performing the reboot.

Corrective Action: n/a

24588 NTP_SERVER_SET_LOG

Message = 'Setting the NTP server IP address to <IP-address>'

EventType='information'

Probable Cause: The IP address of the NTP server has been set by request from the Element Manager.

Corrective Action: n/a

Pending config group

The system generates the following logs during the processing of the config pending file, c:\uas\etc\uas_pending.conf. The reason for the failures include:

- overwriting an existing pending config file

- the pending config file is not writable

24583 PENDING_EXISTS

Message = 'Detected possible loss of configuration changes. Existing file will be overwritten: <filename>'

Probable Cause: see group description

EventType='warning'

24584 PENDING_BACKUP_FAILED

Message = 'Failed to backup pending configuration file: <filename>'

Probable Cause: see above

EventType='warning'

24585 PENDING_CREATE_FAILED

Message = 'Failed to create pending configuration file: <filename>'

Probable Cause: see above

EventType='error'

ConfigMgr logs

This section contains ConfigMgr logs. The logs are divided into the following groups:

- startup and termination group

- miscellaneous group

Startup and Termination group

These logs are generated when the ConfigMgr initializes and terminates. These are all informational or warning messages.

26625 CM_INIT_LOG

Message = 'ConfigMgr process initializing, program arguments: <arguments>.'

EventType='information'

Probable Cause: n/a

Corrective Action: n/a

26626 CM_SHUTDOWN_LOG

Message = 'ConfigMgr shutting down at the request of the program manager.'

EventType='information'

Probable Cause: n/a

Corrective Action: n/a

26627 CM_GENERIC_ERROR_LOG

Message = 'ConfigMgr error: failed to create synchronization object'

EventType='error'

Probable Cause: The ConfigMgr process was initializing and failed to create a system synchronization object. This object is used to communicate with other processes in the system.

Corrective Action: Reboot the system. If the problem persists, contact Nortel support.

26630 CM_MANUAL_TERMINATION

Message = 'ConfigMgr terminated manually instead of via program manager'

EventType='warning'

Probable Cause: ConfigMgr was manually terminated. This flags an abnormal termination of ConfigMgr. The process was most likely in a critical alarm state, waiting for the configuration to be fixed.

Corrective Action: n/a

26632 CM_TERMINATION_STATUS

Message ='ConfigMgr termination status: <status>

EventType='information'

Probable Cause: ConfigMgr terminated normally. The status should always be "Success". If a configuration problem is encountered, ConfigMgr will wait forever until the problem is fixed or until the program manager is restarted.

Corrective Action: n/a

Miscellaneous group

These are miscellaneous logs generated by the ConfigMgr.

26629 CM_COPY_FILE

Message = 'Cannot copy file from <sourceFilename> to <destinationFilename>'

EventType='error'

Probable Cause: ConfigMgr was unable to make a copy of a file. Possible reasons for the failure are: the program does not have permission to write the file, or the disk is full.

Corrective Action: Check permissions on the file. Check for a full disk.

26631 CM_MANUAL_EDIT

Message = 'Manual edits of uas.conf could be inconsistent with pending config file changes'

EventType='warning'

Probable Cause: The ConfigMgr has detected that the uas.conf file has been manually edited and that there are pending changes in uas_pending.conf. The pending changes are those made from the UAS EM. These changes are not written to the uas.conf file until the program manager is restarted. The pending changes could be inconsistent with the changes that were made when editing the file. Changes made at the UAS EM override any manual edits of the file.

Corrective Action: No action is required if the changes were consistent.

26633 CM_CREATE_FILE

Message = 'Could not create file: <filename>'

EventType='error'

Probable Cause: ConfigMgr was unable to create a configuration file. Possible reasons for the failure are: the program does not have permission to write the file, or the disk is full.

Corrective Action: Check permissions on the file. Check for a full disk.

26634 CM_CG_DETECTED

Message = 'The bearer type is ATM, but the hardware probe detected a CG6000 card'

EventType='warning'

Probable Cause: ConfigMgr found a CG6000 card in a system configured for an ATM bearer type. The bearer type may be incorrect or the system was converted from an IP bearer to an ATM configuration and a CG6000 card was left in the system.

Corrective Action: The UAS will still function with a CG6000 card in an ATM configuration, but will not use the card. The overall NMS card configuration should be inspected to ensure that it is valid.

26635 CM_AG_DETECTED

Message = 'The bearer type is IP, but the hardware probe detected an AG4000 card'

EventType='warning'

Probable Cause: ConfigMgr found an AG4000 card in a system configured for an IP bearer type. The bearer type may be incorrect or the system was converted from an ATM bearer to an IP configuration and an AG4000 card was left in the system.

Corrective Action: The UAS will still function with an AG4000 card in an IP configuration, but will not use the card. The overall NMS card configuration should be inspected to ensure that it is valid.

26636 CM_EXTRA_ AG_DETECTED

Message = 'One or more extra AG4000 cards were detected. The extra card(s) will not be used'

EventType='warning'

Probable Cause: ConfigMgr found an extra AG4000 card in a system configured for ATM BCT.

Corrective Action: No action is required.

26637 CM_IMS_LOCK_FILE_PRESENT

Message = 'IMS lock file (<lock_file_name>) detected. Initialization suspended until lock file is removed.'

EventType='information'

Probable Cause: On startup, the IMS application creates a lock file, generates UAS configuration files, and when completed, removes the lock file. ConfigMgr will not attempt to read the UAS configuration files if the lock file is present. ConfigMgr generates this log if it detects the presence of the lock file. ConfigMgr will then check periodically to see if the lock file has been removed. When it detects that the lock file has been removed, it will continue its initialization and will run to completion.

Corrective Action: No action is required.

26638 CM_IMS_LOCK_FILE_REMOVED

Message = 'IMS lock file (<lock_file_name>) is no longer present. Initialization resumed.'

EventType='information'

Probable Cause: ConfigMgr generates this log upon removal of a lock file that it previously detected. See the previous log description for more information.

Corrective Action: No action is required.

Audio Processing Module logs - unassociated

This section contains Audio Processing Module (APM) logs. The APM unassociated logs are logs that are not associated with a recognized managed object. The system generates **APM** logs from the Call Processing application and the vfs daemon (vfsapp). When APM logs are generated from the Call Processing application, the component name is "AudioAccessAPM." When APM logs are generated from the vfs daemon, the component name is "AudioManagementAPM."

32768 URL000

Message = 'apm_init: static memory allocation error <error number> for ap_ch_data'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32769 URL001

Message = 'validate_channel: Invalid channel <channel> (should be 0 - <max channel value>) in apm request for function <function number>.'

EventType='error'

Probable Cause: This log should not be seen, because the default channel (0) is always used.

Corrective Action: Issue an SR for UAS design investigation.

32770 URL002

Message = 'apl_request: Unknown Function <function number> in apm request'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32771 URL003

Message = 'chk_main_tmplt: Main Template count is 0 in apm message'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32772 URL004

Message='get_main_tmplt: No Main Template in apm message'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32773 URL005

Message = 'proc_main_tmplt: Invalid Index file VocID <directory number>, Index <index> in apm message'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32774 URL006

Message = 'proc_main_tmplt: Invalid Directory VocID <directory number>, Index <index> in apm message'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32775 URL007

Message = 'proc_main_tmplt: Could not find VFS Directory ID <directory number>, Index <index>'

EventType='error'

Probable Cause: Expected audio has either not been provisioned or the UAS has not been updated with the latest audio from the system database server.

Corrective action: If the audio has been provisioned on the database server, make sure thte UAS gets updated with the latest audio. If the audio has not been provisioned, use the APS provisioning system to add the audio.

32776 URL008

Message = 'get_rec_info: No Record template param in apm message'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32777 URL009

Message='proc_vocab_info: Invalid Record Directory ID<directory number> Type <type number>'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32778 URL010

Message = 'proc_vocab_info: Could not find Record Directory ID <directory number>'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32779 URL011

Message = 'apl_speak: Found null external data address for Substitution ID <substitution id> in apm message'

EventType='error'

Probable Cause: Should not be seen, because substitution ids are not used in the UAS.

Corrective Action: Issue an SR for UAS design investigation.

32780 URL012

Message = 'apl_speak: Missing Substitution ID <substitution id> parameter for Variable Speak in apm message'

EventType='error'

Probable Cause: Should not be seen, because substitution ids are not used in the UAS.

Corrective Action: Issue an SR for UAS design investigation.

32781 URL013

Message = 'dig_speak: Missing Substitution ID <substitution id>parameter for Digit Speak in apm message'

EventType='error'

Probable Cause: Should not be seen, because substitution ids are not used in the UAS.

Corrective Action: Issue an SR for UAS design investigation.

32782 URL014

Message='upd_play_seg: couldn't get memory for play_list status <status number>'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32783 URL015

Message = 'upd_play_seg: Play seg count is <count>"

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32784 URL016

Message = 'opnab_dealloc: mma_dealloc error <error number> for opnab buffer'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32785 URL017

Message = 'validate_channel: Play List de-allocate err <error number>'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32786 URL018

Message = 'speak_vfs: Invalid Directory for VocID <directory number>, Index <index> '

EventType='error'

Probable Cause: This should not occur.

Corrective Action: If this error occurs, it indicates an error in the provisioning software on the database server.

32787 URL019

Message='speak_vfs: Could not find VFS Directory ID <directory number>, Index <index>'

EventType='error'

Probable Cause: Attempt to play audio that has not been provisioned.

Corrective Action: Provision audio in system database, and make sure the audio has been distributed to the target audio server.

32788 URL020

Message = 'validate_channel: disk read buffer de-allocate err <error number>"

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32789 URL021

Message = 'dsproc: Could not find Digit Rule Directory <directory id> '

EventType='error'

Probable Cause: Should not be seen, because digit rules are not used in the UAS.

Corrective Action: Issue an SR for UAS design investigation.

32790 URL022

Message = 'dsproc: Invalid digit group <group number> in apm message '

EventType='error'

Probable Cause: Should not be seen, because digit rules are not used in the UAS

Corrective Action: Issue an SR for UAS design investigation.

32791 URL023

Message = 'dsproc: Invalid digit <digit> in apm message '

EventType='error'

Probable Cause: Should not be seen, because digit rules are not used in the UAS.

Corrective Action: Issue an SR for UAS design investigation.

32792 URL024

Message='dsproc: Could not find VFS Directory ID <directory id> Index <index>'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32793 URL025

Message = 'process_set_segment: cannot resolve set segment (dir <directory id>), (index <index>)'

EventType='error'

Probable Cause: The set has not been provisioned or has been provisioned to the UAS without a default. The situation where a set does not have a default indicates an error in the software on the database server.

Corrective Action: Ensure that the set has been provisioned on the database, and that the UAS has been updated with the latest audio from the system database.

32794 URL026

Message = 'process_multilang_var: missing value for variable <variable segment id> (dir <directory id>), (index <index>)'

EventType='error'

Probable Cause: The provisioned variable does not have a value supplied either during provisioning or during the runtime access.

Corrective Action: Supply a value through the provisioning system or in the runtime call to play the variable.

32795 URL027

Message = 'processVar: Invalid variable type <variable type> in play message '

EventType='error'

Probable Cause: The provisioning system is applying invalid variable types to variables or the runtime call is incorrect.

Corrective Action: Verify the provisioning system is working correctly and also that the runtime service is building valid calls to the runtime system.

32796 URL028

Message = 'processString: Invalid char <character code> in play message '

EventType='error'

Probable Cause: An attempt has been made to play an invalid character. There is an error either in the provisioning system or in the service supplying the runtime value.

Corrective Action: Correct the provisioning error or the runtime call as appropriate.

32797 URL029

Message='processWeekday: Invalid value <weekday number> in play message '

EventType='error'

Probable Cause: The weekday value is out of range (1 - 7). There is an error either in the provisioning system or in the service supplying the runtime value.

Corrective Action: Correct the provisioning error or the runtime call as appropriate.

32798 URL030

Message = 'processMonth: Invalid value <month number> in play message >'

EventType='error'

Probable Cause: The month value is out of range (1 - 12). There is an error either in the provisioning system or in the service supplying the runtime value

Corrective Action: Correct the provisioning error or the runtime call as appropriate.

32799 URL031

Message = 'processDN: Invalid subtype <subtype> in play message '

EventType='error'

Probable Cause: The dn subtype is invalid. There is an error either in the provisioning system or in the service supplying the runtime value

Corrective Action: Correct the provisioning error or the runtime call as appropriate.

32800 URL032

Message = 'processNADN: Bad dn string <North American DN> in play message '

EventType='error'

Probable Cause: weekday value is out of range (1 - 7). There is an error either in the provisioning system or in the service supplying the runtime value

Corrective Action: Correct the provisioning error or the runtime call as appropriate.

32801 URL033

Message = 'processCurrency: unknown currency <currency> in play message'

EventType='error'

Probable Cause: Invalid string passed in to play currency method, either through invalid provisioning software or through a play request to the runtime system.

Corrective Action: Correct the provisioning error or the runtime call as appropriate.

32802 URL034

Message='processText: unsupported type in play message '

EventType='error'

Probable Cause: Call to play a variable of type "Text".

Corrective Action: Correct the provisioning error or the runtime call as appropriate.

32803 URL035

Message = 'getDateInfo: Bad date string <date string> in play message'

EventType='error'

Probable Cause: Invalid value passed in for a date variable, either through an error in the provisioning system or through a play request to the runtime system.

Corrective Action: Correct the provisioning error or the runtime call as appropriate.

32804 URL036

Message = 'getTimeInfo: Bad time string <time string> in play message'

EventType='error'

Probable Cause: Invalid value passed in for a time variable, either through an error in the provisioning system or through a play request to the runtime system.

Corrective Action: Correct the provisioning error or the runtime call as appropriate.

32805 URL037

Message = 'resolve_multilang_var: unsupported language <language> in play message'

EventType='error'

Probable Cause: Invalid language identifier passed in for a variable, either through an error in the provisioning system or through a play request to the runtime system.

Corrective Action: Correct the provisioning error or the runtime call as appropriate.

32806 URL038

Message = 'No audio for language <language> in play message '

EventType='error'

Probable Cause: Attempt to play a supported language, but no audio exists.

Corrective Action: If the audio has been added to the system database, make sure the UAS has been updated with the latest audio. If the audio has not been provisioned, use the ASAM provisioning tool to add audio to the system for the target language.

32807 URL039

Message='Corrupt language version tree: language <language> in play message '

EventType='error'

Probable Cause: Software error in the provisioning system on the database server or a problem in the runtime code on the UAS.

Corrective Action: Contact Nortel support.

32808 URL040

Message = 'processVar: Missing multilang audio (dir <vfs directory number>), (index <index>) '

EventType='error'

Probable Cause: A specific file needed to announce a multilanguage variable is missing. The file has probably not been provisioned or the latest updates have not been sent to the UAS.

Corrective Action: Make sure the missing audio has been provisioned and that the audio update has been sent to the UAS.

32809 URL041

Message = 'processSet: exceeded max nesting for segment %d (dir %d), (index %d)'

EventType='error'

Probable Cause: Software error in the provisioning system on the database server has allowed a set to form a cycle or otherwise exceed the number of levels (15) supported by the runtime software.

Corrective Action: The segment should be verified through the provisioning system to make sure that it is valid in regard to the number of layers and to make sure that there are no cycles within the set.

Hardware Logs - unassociated

32818 HW_SOFTW_FAILURE

Message = 'Unknown failure - <failure description>'

EventType='error'

Probable Cause: An unexpected software error has occurred in the hardware interface software.

Corrective Action: If the problem persists, contact the next level of support.

32819 HW_NO_TIMESLOTS

Message = 'No timeslots available on board <board identifier>'

EventType='error'

Probable Cause: The system is loaded above supported levels or there is a resource leak.

Corrective Action: If the problem persists during low traffic times, contact the next level of support.

32820 HW_NMS_ERROR

Message = 'Bad return code <return code> for function <function name> with object <hardware object name>'

EventType='error'

Probable Cause: There is a problem with an NMS board. This could be due to transitive reasons, such as call load, or persistent reasons, such as a hardware problem.

Corrective Action: If enough of these problems occur in one session of callp, the board will be taken out of service until callp is restarted. If the problem persists, contact the next level of support.

32821 HW_NMS_KEYWORD_CONFIG_ERROR

Message = 'NMS oam error for keyword <keyword>.'

EventType='error'

Probable Cause: There is a problem with an NMS configuration file.

Corrective Action: If the problem persists, contact the next level of support.

32822 CG6K_ETHERNET_HALF_DUPLEX

Message = 'Interface %d on CG6000C in slot %d is in HALF-DUPLEX mode. For optimal performance, it should be in FULL-DUPLEX mode. Please check network configuration.'

EventType='error'

Probable Cause: An ethernet port on the CG6000C is connected to either a hub or to a switch port configured for half-duplex operation.

Corrective Action: Plug the CG6000C into a full-duplex switch port.

32823_CG6K_ETHERNET_10BT

Message = 'Interface %d on CG6000C in slot %d is in 10-baseT mode. This will limit capacity. For optimal performance, it should be in 100-baseT mode. Please check network configuration.'

EventType='error'

Probable Cause: An ethernet port on the CG6000C is connected to a 10-baseT port on a switch or hub.

Corrective Action: Reconfigure the port on the switch for 100baseT operation.

Vocabulary File System logs - unassociated

This section contains Vocabulary File System (VFS) logs. The VFS unassociated logs are logs that are not associated with a managed object. The system generates VFS logs from the Call Processing application and the vfs daemon (vfsapp). When the logs are generated from the call processing application, the component name is "AudioAccessVFS." When the logs are generated from the vfsapp, the component name is "AudioManagementVFS."

32868 URL100

Message = 'VFSBuilder::VFSBuilder: Warning: no VFS directory <directory name>'

EventType='error'

Probable Cause: The Global Server software has not been installed on the system, or the "VFSDIR" environment variable has been unset or set to an invalid value.

Corrective Action: Make sure the Global Server software has been installed correctly and that the VFSDIR variable is set to the correct directory.

32869 URL101

Message = 'VFSBuilder::VFSBuilder: unable to build the mmap for address <memory address> and buffer <buffer>'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32870 URL102

Message = 'VFSBuilder::read_rules: unable to read digit rule file <filename>'

EventType='error'

Probable Cause: This should never be seen, because digit rules are not used on the UAS.

Corrective Action: Issue an SR for UAS design investigation.

32871 URL103

Message = 'VFSBuilder::get_rough_sizes: Control: Unknown tag <tag id> for <filename>'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32872 URL104

Message = 'VFSBuilder::read_control: unable to open <filename> '

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32873 URL105

Message = 'VFSBuilder::read_control: Error! application index <index> exists as <filename>'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32874 URL106

Message = 'VFSBuilder::read_control: Error! No application for vocab id <index> '

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32875 URL107

Message = 'VFSBuilder::vfs_init: missing vocabulary directories'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32876 URL108

Message = 'VFSBuilder::vfs_init: Error allocating directories'

EentType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32877 URL109

Message = 'VFSBuilder::vfs_init: Error reading control information!'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32878 URL110

Message = 'VFSBuilder::vfs_init: Error reading directories! '

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32879 URL111

Message = 'VFSBuilder::vfs_init: Error reading vocab segments!'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32880 URL112

Message = 'VFSBuilder::reinit_dir: Cannot Open <filename>'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32881 URL113

Message = 'VFSBuilder::reinit_dir: Can't read file <filename>'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32882 URL114

Message = 'VFSBuilder::reinit_dir: Can't load lookup <filename> '

EventType='error'

Probable Cause: This should not occur, because the UAS does not use lookups in the VFS system.

Corrective Action: Issue an SR for UAS design investigation.

32883 URL115

Message = 'VFSBuilder::load_vocabs: Warning: Concode is neither RAM nor DISK'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32884 URL116

Message = 'VFSBuilder::load_vocabs: Can't read DATA file <filename>'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32885 URL117

Message = 'VFSBuilder::load_vocabs: Error opening DATA file <filename>'

EventType='error'

Probable Cause: File permission problem.

Corrective Action: Make sure file permissions allow access.

32886 URL118

Message = 'vfs_main::daemon_main: Daemon process is already running (pid <process id>)'

EventType='error'

Probable Cause: Another vfsapp process is already running.

Corrective Action: Make sure that the last shutdown of the Program Manager worked correctly (ie, all processes exited cleanly).

32887 URL119

Message = 'vfs_main::daemon_main: No segment loaded'

EventType='information'

Probable Cause: The system is starting fresh with no existing memory maps.

Corrective Action: None needed

32888 URL120

Message = 'vfs_main::daemon_main: BUILD FAILED'

EventType='error'

Probable Cause: The system has reached the maximum amount of audio that can be loaded in the current memory configuration, or there is a problem with some particular audio update.

Corrective Action: The most likely problem is exceeding the available memory. On the provisioning system, turn off the caching of as much audio as possible so that the audio is read from disk instead of from memory. This helps reduce the memory consumption on the UAS.

32889 URL121

Message = 'vfs_main::daemon_main: Starting daemon process'

EventType='information'

Probable Cause: This log is always generated when the vfsapp process starts.

Corrective Action: none

32890 URL122

Message = 'vfs_main::daemon_main: unable to allocate a socket!'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32891 URL123

Message = 'vfs_main::daemon_main: unable to set socket linger to OFF'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32892 URL124

Message = 'vfs_main::daemon_main: unable to set REUSEADDR'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32893 URL125

Message = 'vfs_main::daemon_main: unable to bind to port <port number>'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32894 URL126

Message = 'vfs_main::daemon_main: unable to get socket name '

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32895 URL127

Message = 'vfs_main::daemon_main: unable to set listen queue depth'

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32896 URL128

Message = 'vfs_main::daemon_main: Accepted a connection from <ip address of telnet connection>'

EventType='information'

Probable Cause:

Corrective Action: none - this is an informational log

32897 URL129

Message = 'VFS_API::handleVFSswitchover: vailMaint.unmapFile for %d (0x%x) return <return code>'

EventType='information'

Probable Cause:

Corrective Action: no action needed

32898 URL130

Message = 'VFS_API::handleVFSswitchover: vailMaint.mapFile for %d (0x%x) return <return code>'

EventType='information'

Probable Cause:

Corrective Action: no action needed

32899 URL131

Message = 'VFS_API::reinit: Error opening file <filename> '

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32900 URL132

Message = 'VFS_API::reinit: File <filename> does not seem to be a VFS file '

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32901 URL133

Message = 'VFS_API::reinit: mmap Error %d mapping the file <filename> '

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32902 URL134

Message = 'VFS_API::reinit: Attached segment 0x%08x for file <filename> in bad state %d '

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32903 URL135

Message = 'MMAP_Builder::MMAP_Builder: Failed to create %s '

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32904 URL136

Message = 'MMAP_Builder::MMAP_Builder: Error on file <filename> attach '

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32905 URL137

Message = 'MMAP_Builder::allocate: Error re-attaching file as part of grow operation '

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32906 URL138

Message = 'VFS_API::handleVFSswitchover: VAILmaintMgr is not running, no mmap attachment to VAIL '

EventType='error'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32907 URL139

Message = 'VFS_langver::getDefault: No default for node <node id> Selector Value <selector value>'

EventType='error'

Probable Cause: This should not occur. If at least one language version exists for the system, there should be a default.

Corrective Action: This is a software error in the provisioning system. The multilanguage audio should never be added to the audio server without a default language version.

32908 URL140

Message = 'VFSBuilder::vfs_init: Error reading language version file (langver.dat)'

EventType='information'

Probable Cause: unknown software error

Corrective Action: Issue an SR for UAS design investigation.

32909 URL141

Message = 'VFSBuilder::load_langver_file: langver.dat does not exist - possible error '

EventType='warning'

Probable Cause: The UAS has not been provisioned since the addition of multilanguage audio to the system database server.

Corrective Action: Check the system again after the next scheduled provisioning of the UAS from the system database server.

32910 URL142

Message = 'VFSBuilder::load_langver_file: could not allocate root node in memory'

EventType='error'

Probable Cause: Memory allocation error.

Corrective Action: Issue an SR for UAS design investigation.

32911 URL143

Message = 'VFSBuilder::load_langver_file: bad file format or contents for langver.dat '

EventType='error'

Probable Cause: The file used to locate the audio for a specific language version is corrupt.

Corrective Action: Issue an SR for UAS design investigation.

32912 URL144

Message = 'VFSBuilder::load_langver_file: could not create new langver file '

EventType='error'

Probable Cause: File permissions in the control directory or on the existing langver.dat file have been changed

Corrective Action: Make sure the control directory and langver.dat file permissions allow updates.

32913 URL145

Message = 'VFSUpdate::problem updating alias: <error description>"

EventType='error'

Probable Cause: This error occurs during audio provisioning from the APS. Problem connecting to the aliasServer process, or an error adding or removing an alias from the lookup structure.

Corrective Action: Make sure the aliasServer is running correctly inside program manager. Otherwise, issue an SR against UAS design. The audio can still be accessed by its segment ID. Also, if the audio is part of a language version, the alias does not get used on the UAS.

ManagedObjectLib logs - unassociated

Possible sources of these logs are as follows: 1) **StateMgrThread** - the state manager thread runs as part of the callp application; 2) **StateStore** - the component responsible for persisting managed object states.

33068 BAD_SC_MESSAGE

Message = 'received bad state change message'

EventType='error'

Probable Cause: The state manager thread has received a bad state change message. This indicates an internal software defect.

Corrective Action: n/a The log should be reported to the support group.

33069 UNKNOWN_MESSAGE_TYPE

Message = 'received message of an unknown type'

EventType='error'

Probable Cause: The state manager thread has received a bad message. This indicates an internal software defect.

Corrective Action: n/a The log should be reported to the support group.

33070 RECEIVE_ERROR

Message = 'receive error, code=<errorCode>'

EventType='error'

Probable Cause: The state manager thread has encountered a communications error.

Corrective Action: n/a The log should be reported to the support group.

33071 CORRUPT_MESSAGE

Message = 'message received is corrupt, length=<length>'

EventType='error'

Probable Cause: The state manager thread has encountered a communications error.

Corrective Action: n/a The log should be reported to the support group.

33072 SOCKET_INIT_ERROR

Message = 'failed to init socket, delay then try again ...'

EventType='error'

Probable Cause: The state manager thread is attempting to initialize its communications mechanism, but is encountering a problem. This is probably because another instance of the program (callp) is running.

Corrective Action: Ensure that only one callp process is running.

33079 MO_SELECT_SOCKET_ERROR

Message = 'Socket error on select statement, code=<error-code>.'

EventType='error'

Probable Cause: The state manager thread has encountered a communications error.

Corrective Action: The log should be reported to the support group.

33080 MO_SELECT_ERROR

Message = 'Unexpected result on select statement, result=<error-code>'

EventType='error'

Probable Cause: The state manager thread has encountered a communications error.

Corrective Action: The log should be reported to the support group.

33081 MO_BAD_STATE_TYPE

Message = 'Encountered bad state type code, code=<state-type-code>'

EventType='error'

Probable Cause: There was an internal program error.

Corrective Action: The log should be reported to the support group.

33082 MO_PERSIST_WRITE_ERROR

Message = 'Error writing to managed object state persistence file, key=<key>'

EventType='error'

Probable Cause: There was an internal program error.

Corrective Action: The log should be reported to the support group.

33083 MO_FILE_CREATE_ERROR

Message = 'Error creating file <filename>'

EventType='error'

Probable Cause: The application does not have permission to write to the file or the disk is full.

Corrective Action: Check permissions on the file and check available disk space.

33084 MO_PERSIST_BAD_STATE

Message = 'Client attempted to persist bad state, key=<key> state=<statecode>'

EventType='error'

Probable Cause: There was an internal program error.

Corrective Action: The log should be reported to the support group.

CoLib and UGWbase logs - unassociated

UGWBase logs

These logs are generated from the UGWbase software, which is used to implement the abstraction of provisionable entities for both UAS or PRI gateway applications. Entities represented in UGWbase are the system cards, carriers on carrier cards, carrier DS0s, and generalized trunk groups, along with the UGWnode entity that manages these UGWbase entities.

CoLib logs

These logs are generated by various components in the ConfigObjectLib library:

- **Config Object Change Group** - The system generates the logs in this section when the network administrator modifies a configuration parameter through the management station.

- **General Config Group** - The system generates the logs listed below when the user accesses configuration parameters in the config file, c:\uas\etc\uas.conf. The following is a list of failures for the logs:

  — The config file does not exist.

  — The config file is not readable or writable.

  — The required configuration parameter is not in the file or is misspelled.

- **uas.conf Validation Group** - The system generates the logs in this section when the user validates the c:\uas\etc\uas.conf file. The logs report either the absence of a required configuration parameter or

an invalid configuration parameter value. The configuration should be corrected in response to these logs.

33118 UGWNODE_MEMALLOC_FAILURE

Message = 'UGWNODE_MEMALLOC_FAILURE: <message>'

EventType='warning'

Probable Cause: Insufficient memory resources.

Corrective Action: Restart application. Report log to support team.

Source: UGWbase.UGWnode

33119 UGWNODE_CONFOBJACC_FAILURE

Message = 'UGWNODE_CONFOBJACC_FAILURE: <message>'

EventType='warning'

Probable Cause: Failure to access configuration card object.

Corrective Action: Check that the uas.conf file is valid using the configuration manager. Restart application. Report log to support team.

Source: UGWbase.UGWnode

33120 UGWNODE_SLOTALLOC_FAILURE

Message = 'UGWNODE_SLOTALLOC_FAILURE: <message>'

EventType='warning'

Probable Cause: Failure to allocate a slot in the chassis.

Corrective Action: Check that the uas.conf file is valid with respect to physical slots specified (range and duplicates) using configuration manager. Restart the application if necessary.

Source: UGWbase.UGWnode

33121 UGWNODE_CARDLSTLOC_FAILURE

Message = 'UGWNODE_CARDLSTLOC_FAILURE: <message>'

EventType='warning'

Probable Cause: Card cannot be located in card list.

Corrective Action: Check that ugw.conf and uas.conf are consistent using the configuration manager. Restart application. Report log to support team.

Source: UGWbase.UGWnode

33122 UGWNODE_PERSISTADMST_FAILURE

Message = 'UGWNODE_PERSISTADMST_FAILURE: <message>'

EventType='warning'

Probable Cause: Failure to persist the UAS node administrative state.

Corrective Action: Check that the ugwStates.conf file exists and that there is sufficient disk space. Report log to support team.

Source: UGWbase.UGWnode

33123 UGWNODE_DS0LSTLOC_FAILURE

Message = 'UGWNODE_DS0LSTLOC_FAILURE: <message>'

EventType='warning'

Probable Cause: DS0 cannot be located in DS0 object list.

Corrective Action: Check that ugw.conf and uas.conf are consistent using the configuration manager. Restart application. Report log to support team.

Source: UGWbase.UGWnode

33124 UGWNODE_BADLISTTYPE_FAILURE

Message = 'UGWNODE_BADLISTTYPE_FAILURE: <message>'

EventType='warning'

Probable Cause: An unknown ugwState.conf file managed object type has been detected by UGWnode during purge of UGWnode object persisted states.

Corrective Action: Use element manager to correct the administative states of UGWnode objects. Delete the ugwState.conf file and restart application if necessary. Report log to support team.

Source: UGWbase.UGWnode

33128 UGWCNFG_FAILURE

Message = 'UGWCNFG_FAILURE: <message>.'

EventType='warning'

Probable Cause: Problem with the ugw.conf file format or parameters.

Corrective Action: Correct the ugw.conf file inconsistencies and restart application.

Component: UGWcnfgService

33129 UGWCNFG_INIT_SUCCESS

Message = 'UGWCNFG_INIT_SUCCESS'

EventType='information'

Probable Cause: Successful parse of ugw.conf file. Validated GW provisioning data exists in the system.

Corrective Action: n/a

Component: CoLib

33130+ GENERIC_ERROR_LOG

Message = 'CoLib error: Error reading config file'

EventType='error'

Probable Cause: see group description

Corrective Action: see group description

Component: CoLib

33130+ GENERIC_ERROR_LOG

Message = 'CoLib error: error writing to config file, config parameter is: <parameterName>'

EventType='error'

Probable Cause: see group description

Corrective Action: see group description

Component: CoLib

33130+ GENERIC_ERROR_LOG

Message = 'MoLib error: error looking up config parameter <parameterName>'

EventType='error'

Probable Cause: see group description

Corrective Action: see group description

Component: CoLib

33130+ GENERIC_ERROR_LOG

Message = 'MoLib error: could not update config file (interface table row addition)'

EventType='error'

Probable Cause: see group description

Corrective Action: see group description

Component: CoLib

33130+ GENERIC_ERROR_LOG

Message = 'MoLib error: Subagent: could not update config file (interface table row removal)'

EventType='error'

Probable Cause: see group description

Corrective Action: see group description

Component: CoLib

33130+ GENERIC_ERROR_LOG

Message = 'MoLib error: Subagent: could not update config file (interface table row modification)'

EventType='error'

Probable Cause: see group description

Corrective Action: see group description

Component: CoLib

33130+ GENERIC_ERROR_LOG

Message = 'MoLib error: Subagent: could not update number of bearer cards after row add or delete'

EventType='error'

Probable Cause: see group description

Corrective Action: see group description

Component: CoLib

33130+ GENERIC_ERROR_LOG

Message = 'MoLib error: A required key was not found in configuration file <filename>. The key name is <parameterName>'

EventType='error'

Probable Cause: see group description

Corrective Action: see group description

Component: CoLib

33130+ GENERIC_ERROR_LOG

Message = 'MoLib error: Bad value in configuration file, key: <key> value: <value>'

EventType='error'

Probable Cause: An invalid value was found for the specified key in a configuration file

Corrective Action: Look the key up in the configuration documentation and use the UAS EM to change the value of the key.

Component: CoLib

33130+ GENERIC_ERROR_LOG

Message = 'MoLib error: bad number of AG cards: <number>'

EventType='error'

Probable Cause: An error was encountered while detecting the number of AG cards in the system. There must be 1 or 2 AG cards in the system.

Corrective Action: see group description

Component: CoLib

33130+ GENERIC_ERROR_LOG

Message = 'MoLib error: invalid nms card configuration, number of AG cards is <number>, number of bearer cards is <number>"

EventType='error'

Probable Cause: Only certain combinations of AG and bearer cards are valid. The number of AG cards detected in the system and the number of bearer cards specified in the uas.conf file is not a supported combination.

Corrective Action: see group description

Component: CoLib

33130+ GENERIC_ERROR_LOG

Message = 'MoLib error: Bad interface table entry: <rowContent>'

EventType='error'

Probable Cause: see group description

Corrective Action: see group description

Component: CoLib

33131+ GENERIC_WARNING_LOG

Message = 'T.38 codec is configured in a non-BCT UAS system'

EventType='warning'

Probable Cause: The T.38 codec is currently configured, but will not be used in a non-BCT UAS system.

Corrective Action: To remove the warning, do not configure T.38 in an all-BCT system.

Component: CoLib

33131+ GENERIC_WARNING_LOG

Message = 'Voice codecs are configured in an all-BCT system'

EventType='warning'

Probable Cause: Voice codecs are currently configured, but voice codecs are not used in an all-BCT system.

Corrective Action: To remove the warning, do not configure any codecs in an all-BCT system.

Component: CoLib

33132 CONFIG_OBJECT_SET

Message = 'Configuration object <parameter> was changed from <oldValue> to <newValue>'

EventType='information'

Probable Cause: see group description

Corrective Action: n/a

Component: CoLib

33133 CONFIG_ROW_ADD

Message = 'A row was added to the <nameOfTable> table. The new row is: <rowContent>'

EventType='information'

Probable Cause: see group description

Corrective Action: n/a

Component: CoLib

33134 CONFIG_ROW_DELETE

Message = 'A row was deleted from the <nameOfTable> table. The deleted row was: <rowContent>'

EventType='information'

Probable Cause: see group description

Corrective Action: n/a

Component: CoLib

33135 CONFIG_ROW_MODIFY

Message = 'A row was modified in the <nameOfTable> table. The old row was: <rowContent> The new row is: <rowContent>'

EventType='information'

Probable Cause: see group description

Corrective Action: n/a

Component: CoLib

33136 MAINSA_OBJECT_SET

Message = 'Configuration object <parameter> was changed from <oldValue> to <newValue>'

EventType='information'

Probable Cause: see group description

Corrective Action: n/a

Group: config object change group

Component: CoLib

33138 CARD_PROVDUP_FAILURE

Message = 'CARD_PROVDUP_FAILURE: <message>'

EventType='warning'

Probable Cause: Duplicate carrier card in uas.conf or ugw.conf file.

Corrective Action: Check that ugw.conf and uas.conf are consistent using the configuration manager. Restart application.

Source: UGWbase.IfCard

33139 CARD_INSTALLDUP_FAILURE

Message = 'CARD_INSTALLDUP_FAILURE: <message>'

EventType='warning'

Probable Cause: Attempting to mark installed card as installed.

Corrective Action: Check that ugw.conf and uas.conf are consistent using the configuration manager.

Source: UGWbase.IfCard

33140 CARD_MEMALLOC_FAILURE

Message = 'CARD_MEMALLOC_FAILURE: <message>'

EventType='warning'

Probable Cause: Insufficient memory resources.

Corrective Action: Restart application. Report log to support team.

Source: UGWbase.IfCard

33141 CARD_NUMCARRRANGE_FAILURE

Message = 'CARD_NUMCARRRANGE_FAILURE: <message>'

EventType='warning'

Probable Cause: Number of carriers on card out of range.

Corrective Action: Check that the ugw.conf file is valid and restart application. Report log to support team.

Source: UGWbase.IfCard

33142 CARD_BADCARRTYPE_FAILURE

Message = 'CARD_BADCARRTYPE_FAILURE: <message>'

EventType='warning'

Probable Cause: Unknown carrier type specified for card carrier.

Corrective Action: Check that the ugw.conf file is valid and restart application. Report log to support team.

Source: UGWbase.IfCard

33143 CARD_UNKNMGMTLVL_FAILURE

Message = 'CARD_UNKNMGMTLVL_FAILURE: <message>'

EventType='warning'

Probable Cause: Unknown managed object level originating card administrative state change.

Corrective Action: Restart application. Report log to support team.

Source: UGWbase.IfCard

33148 CARR_BADCARRTYPE_FAILURE

Message = 'CARR_BADCARRTYPE_FAILURE: <message>'

EventType='warning'

Probable Cause: Unknown carrier type specified for carrier.

Corrective Action: Check that the ugw.conf file is valid and restart application. Report log to support team.

Source: UGWbase.genCarrier

33149 CARR_MEMALLOC_FAILURE

Message = 'CARR_MEMALLOC_FAILURE: <message>'

EventType='warning'

Probable Cause: Insufficient memory resources.

Corrective Action: Restart application. Report log to support team.

Source: UGWbase.genCarrier

33150 CARR_PERSISTADMST_FAILURE

Message = 'CARR_PERSISTADMST_FAILURE: <message>'

EventType='warning'

Probable Cause: Failure to persist the UAS carrier administrative state.

Corrective Action: Check that the ugwStates.conf file exists and that there is sufficient disk space. Report log to support team.

Source: UGWbase.genCarrier

33152 DS0_PERSISTADMST_FAILURE

Message = 'DS0_PERSISTADMST_FAILURE: <message>'

EventType='warning'

Probable Cause: Failure to persist the UAS DS0 administrative state.

Corrective Action: Check that the ugwStates.conf file exists and that there is sufficient disk space. Report log to support team.

Source: UGWbase.Ds0

33158 TG_BADTGID_FAILURE

Message = 'TG_BADTGID_FAILURE: <message>'

EventType='warning'

Probable Cause: Trunk Group ID is out of range.

Corrective Action: Check that the ugw.conf file is valid and restart application. Report log to support team.

Source: UGWbase.generalTrunkGroup

33159 TG_UNKNTGTYPE_FAILURE

Message = 'TG_UNKNTGTYPE_FAILURE: <message>'

EventType='warning'

Probable Cause: Unknown trunk group type.

Corrective Action: Check that the ugw.conf file is valid and restart application. Report log to support team.

Source: UGWbase.generalTrunkGroup

33160 TG_PERSISTADMST_FAILURE

Message = 'TG_PERSISTADMST_FAILURE: <message>'

EventType='warning'

Probable Cause: Failure to persist the UAS trunk group administrative state.

Corrective Action: Check that the ugwStates.conf file exists and that there is sufficient disk space. Report log to support team.

Source: UGWbase.generalTrunkGroup

Data Sync Framework logs - unassociated

Data Sync logs are generated by the DataSync Manager thread and threads that utilize the SyncClient objects, which run as part of the callp and Main Subagent applications.

33168 SYNC_THREADS_FAILURE

EventType='warning'

Message='SYNCMANAGER : The DataSync framework's threads failed to start. Reason the system is not configured in HA mode.'

Probable Cause: The system is not configured in an HA configuration.

Corrective Action: Ensure that the system is configured in an HA configuration if the Data Sync is to be utilized.

33169 SYNC_MEMORY_EXHAUSTION

EventType='error'

Message='SYNCMANAGER : Unable to allocate memory inside <method name> method.'

Probable Cause: Memory Exhaustion.

Corrective Action: Free up system resources.

33170 SYNC_CLIENT_REG_SUCCESS

EventType='information'

Message='SYNCMANAGER : Sync Client <client name> has successfully registered with the SyncManager.'

Probable Cause: Sync Client Registration during process initialization.

Corrective Action: N/A.

33171+ SYNC_CLIENT_REG_FAILURE

EventType='error'

Message='SYNCMANAGER : Sync Client <client name> failed to register with the SyncManager. Reason another client had registered with the same name.'

Probable Cause: A sync client does not register it self with a unique.

Corrective Action: Ensure that the specified client registers with a unique name.

33171+ SYNC_CLIENT_REG_FAILURE

EventType='error'

Message='SYNCMANAGER : Sync Client <client name> failed to register with the SyncManager. Reason the SyncManager instance is NULL.'

Probable Cause: A client attempts to register itself with the Sync Manager before the Sync Manager is constructed. Most probable cause is initialization order is not correct.

Corrective Action: Ensure proper initialization order.

33172 SYNC_BULK_REQ_FAILURE

EventType='error'

Message='SYNCMANAGER : Can't request BulkSync. Only <number of registered clients> sync client have registered out of <number of expected clients to register>.'

Probable Cause: One or more Sync Clients failed to register with the Sync Manager.

Corrective Action: Ensure that all expected clients register with the Sync Manager.

33173 SYNC_CLIENT_EXCEPTION

EventType='error'

Message='SYNCMANAGER : Unhandled exception by Client <client's name> in their <method name> method.'

Probable Cause: Sync client exception. check for other err logs. Issue SR

Corrective Action: None needed. Self correcting.

Callpmain logs - unassociated

These logs are generated by the main component of the callp process.

33268 CALLP_ALREADY_RUNNING

EventType='error'

Message='Another instance of callp is already running.'

Probable Cause: An attempt was made to involke the callp process, but a callp process was already running.

Corrective Action: n/a

Component: CallpCommand

HA Monitor logs - unassociated

HA Monitor logs are generated by the HA Monitor thread, which runs as part of the callp and Main Subagent applications.

33368 URL600

EventType='warning'

Message='WARNING : Unable to Register <Notification Agent name> entity with HA Monitor for NGS tag '<Nortel GlobalServer tag>'.'

Probable Cause: The HA Monitor was unable to register the entity's NoticationAgent, for notification of this particular Nortel GlobalServer(NGS) tag.

Corrective Action: Ensure that the NGS Event Distributer ED.exe is up and running. Also ensure that the HA Monitor thread has been started successfully within the process.

33369 URL601

EventType='warning'

Message='WARNING : Unable to Register the HA Monitor with the NGS Event Distributer for tag '<Nortel GlobalServer tag>'.'

Probable Cause: The NGS Event Distributer(E.D.) is not been started or in a non-functional state.

Corrective Action: Ensure that the NGS Event Distributer ED.exe is running successfully, before the HA Monitor tries to register with it for all interested tags.

33370 URL602

EventType='error'

Message='ERROR : The < HA Monitor thread name> was unable to successfully initialize the NGS Event Distributer socket.'

Probable Cause: Lack of system resources or an overloaded system could result in the unsuccessful initialization of the NGS Event Distributer socket.

Corrective Action: Free up system resources and restart the application.

33371 URL603

EventType='error'

Message='ERROR : The <HA Monitor object name> detected a listening failure on NGS Event Distributer socket.'

Probable Cause:

Corrective Action:

33372 URL604

EventType='error'

Message='ERROR : Unable to create the instance of the HA Monitor within the <process name> process.'

Probable Cause: Memory exhaustion

Corrective Action: Free up system resources.

33373 URL605

EventType='warning'

Message='WARNING : HA Monitor received a UNKNOWN external request.'

Probable Cause: The HA Monitor received a unhandled request. The HA Monitor only recognizes certain requests.

Corrective Action: None

Card Maintenance logs - unassociated

Card Maintenance logs are generated by the Card Maintenance thread, which runs as part of the callp application.

33378 URL610/CARDMTC_GENERAL_LOG

EventType='Information'

Message = 'CardMtc: %s'

Probable Cause: Information related to the card maintenance system, not implemented at this time

Corrective Action: None

33379 URL611/CARDMTC_STARTUP_LOG

EventType='Information'

Message = 'CardMtc: The CardMtc process has started'

Probable Cause: Card Maintenance has been initialized

Corrective Action: None

33380 URL612/CARDMTC_SHUTDOWN_LOG

EventType='Information'

Message = 'CardMtc: The CardMtc process has terminated'

Probable Cause: Card Maintenance has been terminated

Corrective Action: None

33381 URL613/CARDMTC_CARD_STARTUP_LOG

EventType='Information'

Message = 'CardMtc: Card %d has started '

Probable Cause: Card Maintenance has a new card and has started using it

Corrective Action: None

33382 URL614/CARDMTC_CARD_SHUTDOWN_LOG

EventType='Information'

Message = 'CardMtc: Card %d has been removed from service : Reason : %s'

Probable Cause: Card Maintenance has stopped using a card, this would be a good place to look to find out why

Corrective Action: None

33383 URL615/CARDMTC_CARD_GENERAL_LOG

EventType='Information'

Message = 'CardMtc: %s'

Probable Cause: General report for a card event that has occurred.

Corrective Action: None

33384 URL616/CARDMTC_EVENT_LOG

EventType='warning'

Message = 'Unexpected event occurred: %s'

Probable Cause: An unexpected event was sent to the card maintenance system

Corrective Action: Note the event if printed and notify the development team of this event.

33385 URL617/CARDMTC_OBSERVER_LOG

EventType='warning'

Message ='CardMtc: Unexpected Observer Event Occurred %s'

Probable Cause:An observer has done something unexpected or unsupported in the system

Corrective Action: Forward this log to development team.

33386 URL618/CARDMTC_ERROR_LOG

EventType='Error'

Message = 'CardMtc: Unexpected Error Occurred %s'

Probable Cause: General report for a card error that has occurred.

Corrective Action: Note the event and take the corrective action included in the string message.

Backup program logs - unassociated

These logs are generated by the backup program, which is run periodically to back up UAS configuration files.

33429 BACKUP_MOUNT_ERROR

Message = 'BackupNodeData: <message>'

EventType='Error'

Probable Cause: An attempt to mount the backup file system failed.

Corrective Action: Ensure that the backup file system is configured properly on the UAS. Determine if the backup file system is operational and configured properly.

33430 BACKUP_UMOUNT_ERROR

Message = 'BackupNodeData: <message>'

EventType='Error'

Probable Cause: An attempt to unmount the backup file system failed.

Corrective Action: Ensure that the backup file system is configured properly on the UAS. Determine if the backup file system is operational and configured properly.

33431 BACKUP_SUCCESS_INFO

Message = 'BackupNodeData: <message>'

EventType='information'

Probable Cause: The backup operation was successful.

Corrective Action: None

ATM service logs

This section contains asynchronous transfer mode (ATM) logs.

34818 ATM_INIT_LOG

Message = 'The ATM service has initialized successfully'

EventType='information'

Probable Cause: The ATM component on the Universal Audio Server completed initialization

Corrective Action: none.

34819 GATEWAY_DEL_FAILED

Message = 'The ATM delete Gateway <Gateway Description> request has failed - cause ID: <Cause ID>'

EventType='error'

Probable Cause: There are probably active calls associated with that gateway, and until those calls are not active, the gateway may not be deleted.

Corrective Action: Lock the port to drop all calls and repeat the action.

34820 GATEWAY_CHG_FAILED

Message = 'The ATM change Gateway <Gateway Description> request has failed - cause ID: <Cause ID>'

EventType='error'

Probable Cause: There are probably active calls associated with that gateway, and until those calls are not active, the gateway may not be changed. Alternatively, the ATM address assigned may be associated with another gateway.

Corrective Action: Lock the port to drop active calls, or if it is an ATM address issue, a different address not currently associated with another gateway should be selected.

34821 ATM_PORT_LOCK_FAIL

Message = 'ATM port <port number> in slot <slot number> has failed to lock - cannot recover unlock state'

EventType='information'

Probable Cause: Hardware is not responding to the requested command.

Corrective Action: Restart the system if repeating the lock attempt is unsuccessful. Call Tier 1 support if the problem returns after a restart - this command should not fail.

34822 ATM_PORT_LOCK_REC_STATE_FAIL

Message = 'ATM port <port number> in slot <slot number> lock failed - can't recover unlock state'

EventType='information'

Probable Cause: Hardware is not responding to the requested command. However, in this case, the state was updated one time to a temporary state and then it froze up.

Corrective Action: Try to repeat the action. If that fails, restart the system. Call Tier 1 support if the problem returns after a restart - this command should not fail.

34823 ATM_VC_AIS

Message = 'ATM VC <vpi>/<vci> on port <port number> in slot <slot number> has experienced an AIS alarm'

EventType='error'

Probable Cause: The ATM port received an F5 AIS alarm on the specified VC.

Corrective Action: None. If the alarm persists the call will be dropped and the VC if it is switched i.e.:SVC will be released.

34824 ATM_VC_RDI

Message = 'ATM VC <vpi>/<vci> on port <port number> in slot <slot number> has experienced an RDI alarm'

EventType='error'

Probable Cause: The ATM port received an F5 RDI alarm on the specified VC.

Corrective Action: None. If the alarm persists the call will be dropped and the VC if it is switched i.e.:SVC will be released.

34826 ATM_VC_AIS_CLEAR

Message = 'ATM VC <vpi>/<vci> on port <port number> in slot <slot number> cleared AIS alarm'

EventType='information'

Probable Cause: The ATM port stopped receiving F5 AIS alarms on the specified VC.

Corrective Action: None.

34827 ATM_VC_RDI_CLEAR

Message = 'ATM VC <vpi>/<vci> on port <port number> in slot <slot number> cleared RDI alarm'

EventType='information'

Probable Cause: The ATM port stopped receiving F5 RDI alarms on the specified VC.

Corrective Action: None.

34829 ATM_WRONG_UNI_VER

Message = 'ATM port <port number> in slot <slot number> has is not configured with UNI 4.0'

EventType='error'

Probable Cause: It is not using the appropriate UNI version.

Corrective Action: Ensure your UNI stack is at the right version

34830 ATM_ILMI_FAILURE

Message = 'ILMI failure on ATM port <port number> in slot <slot number>'

EventType='error'

Probable Cause: ILMI not configured or installed properly.

Corrective Action: Configure ILMI correctly.

34831 ATM_UNI_FAILURE

Message = 'UNI failure on ATM port <port number> in slot <slot number>'

EventType='error'

Probable Cause: UNI not configured or installed properly.

Corrective Action: Configure UNI correctly.

34832 ATM_ILMI_READY

Message = 'ILMI is now ready on ATM port <port number> in slot <slot number>'

EventType='information'

Probable Cause: ILMI is configured correctly and enabled.

Corrective Action: None.

34833 ATM_UNI_READY

Message = 'UNI is now ready on ATM port <port number> in slot <slot number>'

EventType='information'

Probable Cause: UNI is configured correctly

Corrective Action: None.

34834 ATM_INVALID_SDP_PARM

Message = 'Invalid SDP received parm name: <parameter name> recd value: <received value> expected value: <expected value>'

EventType='error'

Probable Cause: Gateway Controller sent an invalid SDP

Corrective Action: call first tier support

34835 AAL2_INVALID_SVC_VCCI_RECEIVED

Message = 'The VCCI=%d received in the incoming SVC setup msg is invalid.'

EventType='error'

Probable Cause: The remote AAL2 gateway is selecting VCCIs from an invalid range.

Corrective Action: Check the remote gateway.

34836 ATM_SW_ERROR

Message = 'The following ATM software error was reported: <software error string>'

EventType='error'

Probable Cause: The ATM card has a software error

Corrective Action: Call first tier support

34837 ATM_ACQUIRE_CHANNEL_FAIL

Message = 'ATM Failed to acquire channel bearer=<endpoint name> destination=<NSAP address>'

EventType='error'

Probable Cause: Possibly no route available or no additional card resources

Corrective Action: Restart call processing

34916 ATM_S200_SW_ERROR

Message = 'The following error was reported by the NMS PA200 API on card in slot <card number>: <software error string>'

EventType='error'

Probable Cause: The ATM card has a software error

Corrective Action: Call first tier support

34917 ATM_S200_FIRMWARE_VERSION

Message = 'The NMS PA200 card is slot <slot number> has the following firmware: <version>'

EventType='information'

Probable Cause: The PA200 is being initialized. The firmware version is automatically queried and this log is generated.

Corrective Action: None

ATM Audit Logs

35016 ATM_AUDI_MISMATCH_RSC

Message = 'The ATM AUDIT has found the following unmatched resources: <resource description>'

EventType='warning'

Probable Cause: A call was not properly cleared and a resource leaked.

Corrective Action: None (audit should properly dispose of/clean the resource)

35017 ATM_AUDIT_RSC_NOT_CLEANED

Message = 'The ATM AUDIT could not dispose of the following unmatched resource: <resource description>'

EventType='error'

Probable Cause: A call was not properly cleared and ATM audit failed to clean the leaked resource.

Corrective Action: If the error persists, call first tier support.

35018 ATM_AUDIT_RSC_DISPOSED

Message = 'The ATM ATUID successfully disposed of the following unmatched resource: <resource description>'

EventType='information'

Probable Cause: A call was not properly cleared and ATM audit successfully cleaned the leaked resource.

Corrective Action: None

ATM port logs

38913 ATM_PORT_INIT_LOG

Message = 'ATM port <port number> in slot <slot number> has initialized successfully'

EventType='information'

Probable Cause: The ATM port on the ATM adapter completed initialization.

Corrective Action: none.

Clock Manager logs

90113 CLOCK_EVENT

Message = '<name-of-clock-source> on slot <slot> now driving <local-or-h110> clock'

EventType='information'

Probable Cause: This message is displayed on initialization or on a failover to a different clock source. <name-of-clock-source> is either: TRUNK_1, TRUNK_2, TRUNK_3, TRUNK_4, OSCILLATOR, H.110 A clock or H.110 A clock. <local-or-h110> is either "local" or "H.110".

Corrective Action: none.

90114 CLOCK_SWERR

Message = 'Unexpected error <error-code> from <function-name> at <source-file-name>:<line-number>'

EventType='error'

Probable Cause: An error occurred on a call to a board level function.

Corrective Action: If the problem persists contact the next level of support.

BCT Service logs

92161 BCT_SOFTW_FAILURE

Message = 'Unknown failure - <failure description>'

EventType='error'

Probable Cause: An unexpected software error has occurred in the BCT hardware software.

Corrective Action: If the problem persists, contact the next level of support.

Test Trunk Service Logs

94208 TT_INVALID_INPUT_PARM

Message = 'Missing required input parameter: - <input parameter>'

EventType='error'

Probable Cause: The gateway controller has not specified the value for a required parameters, such as direction or test type.

Corrective Action: Issue a problem report against the gateway controller.

94209 TT_SOFTW_FAILURE

Message = 'Unknown failure: - <problem description>'

EventType='error'

Probable Cause: An unexpected software error has occurred in the test trunk srf software.

Corrective Action: If the problem persists, contact the next level of support.

94211 TT_MISSING_RETURN_PARM

Message = 'Missing required return parameter: - <parameter>'

EventType='error'

Probable Cause: One of the required return parameters for the particular test type (T100, T102, or T105) is missing.

Corrective Action: If the problem persists, contact the next level of support.

94212 TT_ORIGINATING_SUCCESS

Message = 'Test type <test type> completed successfully: full text: <return text>'

EventType='information'

Probable Cause: The originating test trunk ran successfully, with the results printed in the return text.

Corrective Action: None

94213 TT_ORIGINATING_FAILURE

Message = 'Test type <test type> failed: full text <return text>'

EventType='error'

Probable Cause: The originating test trunk test failed, with the results printed in the return text.

Corrective Action: If the problem persists, contact the next level of support.

APS logs

APS logs are similar to alarms in that they inform system administrators about fault conditions. Specifically, the APS logs are used for notifying an operator about error conditions that cannot be cleared, for providing additional information about an existing alarm condition, for developing a system operation history, and for providing information to be used in troubleshooting.

Provisioner logs

The provisioner log contains log messages that provide a starting point for troubleshooting provisioner problems. Each time a provisioner process runs, an entry is appended to the log for the related APS server, in the format:

PROVISIONER START on <hostname> at <date> [PID: <pid>] <single provision or full provision information>

Since log entries are intermixed, the pid included in the entry identifies the operating system process ID of the particular provisioning process for which the log entry was created.

Each time a provisioner process exits, an entry is also appended to the log for the related APS server, in the format:

PROVISIONER END on <hostname> at <date> [PID: <pid>] <single provision or full provision information>

If a provisioner process exits abnormally, an entry is appended to the log for the related APS server, in the format:

PROVISIONER STOP on <hostname> at <date> because <fault information> [PID: <pid>] <single provision or full provision information>

During normal operation, progress messages are entered in the provisioner logs. For example, when a provisioner creates transaction files for a node, the following entries are made in the related provisioner log:

Attempting to provision node <node name> from host <hostname> at
<date>. [PID: <pid>]

Attempting to transfer files for node <node name> from <hostname>

at <date>. [PID: <pid>]

Last prov date updated for node <node name> on host <hostname> at

<date>. [PID: <pid>]

Any errors that the provisioner encounters are also logged.

The provisioner logs are located in the "/PROV_data" directory. The provisioner logs must be periodically deleted to prevent them from consuming too much space in the file system and preventing the provisioner from running. A script, "provLog_cleanup.sh," located in the "nightly_cleanup.sh" script, runs automatically every night to ensure that only three days worth of provisioner logs are retained. Logs that would normally be deleted by this automatic process can be stored in a different file if they are to be used later for troubleshooting.

The provisioner logs are shown below.

Log code: 03

Exit code=2

Dynamic text message="The specified node ($NODE_ID) is not a configured node on $(hostname)."

Log code: 03

Exit code=3

Dynamic text message="The specified node ($NODE_ID) either does not have provisioning enabled or else does not have a provision set assigned to it on $(hostname)."

Log code: 03

Exit code=n/a

Dynamic text message="Problems on $(hostname) transferring files for node $NODE."

Log code: 03

Exit code=5

Dynamic text message="The last prov date for the node $NODE cannot be updated on $(hostname) because the database is not accessible."

Log code: 02

Exit code=3

Dynamic text message="A full provisioner process cannot be run when another full provision is already in progress on $(hostname)"

Log code: 03

Exit code=3

Dynamic text message="A full provisioner process has timed out waiting for a node-specific provisioner process to complete on $(hostname)."

Log code: 02

Exit code=3

Dynamic text message="A node-specific provisioner process cannot be run on $(hostname) because a full provision is already in progress."

Log code: 02

Exit code=3

Dynamic text message="A node-specific provisioner process cannot be run on $(hostname) because another provision process is already running for that node."

Log code: 02

Exit code=6

Dynamic text message="The provisioner cannot run on $(hostname) because the file system ($IpsProvPath) is full."

Log code: 03

Exit code=n/a

Dynamic text message="The $IpsProvPath file system on $(hostname) is almost full. The provisioner will not be able to run if corrective action isn't taken."

Log code: 02

Exit code=5

Dynamic text message="The provisioner cannot run on $(hostname) because the database is inaccessible."

APS system logs

An APS system log consists of a five-character log identifier, comprised of a three-character log ID that identifies the software component that generated the log followed by a two-digit log number, and the log text. Three types of logs are issued:

- error, which indicates that a software error has occurred
- warning, which indicates that an abnormal situation has occurred that could lead to an error condition
- information

For a procedure used to view APS system logs, see Procedure .

Servlet Request logs

This section contains Servlet Request logs.

45058 SESSION_TIMER_EXPIRED

EventType="information"

Message="Session timer expired: %s"

45059 DB_SW_EXCEPTION

EventType="error"

Message="Software exception: %s"

45060 DB_RMI_EXCEPTION

EventType="error"

Message="RMI exception: %s"

45061 DB_DB_ERR

EventType="error"

Message="Error while accessing the DB."

45062 INVLD_OPCODE

EventType="information"

Message="Invalid OpCode: %s"

Audio Management logs

This section contains Audio Management logs.

28673 AM_SW_EXCEPTION

EventType="error"

Message="Software exception: %s""

28674 AM_SQL_EXCEPTION

EventType="error"

Message="SQL exception: %s"

28675 AM_DB_ERROR

EventType="error"

Message="Error while accessing the DB."

28676 USER_BEGIN_SESSION

EventType="information"

Message="User: %s, Group: %s - is beginning a session at: %s"

28677 USER_END_SESSION

EventType="information"

Message="User: %s, Group: %s - is ending a session"

28678 USER_NOT_ACTIVE

EventType="warning"

Message="User: %s, Group: %s - status is not active"

28679 USER_UPLOAD_FILE

EventType="information"

Message="User: %s, is uploading files."

28680 READ_ERROR

EventType="error"

Message="Error while reading from: %s"

28681 WRITE_ERROR

EventType="error"

Message="Error while writing to file: %s"

28682 DELETE_ERROR

EventType="error"

Message="Error while deleting: %s"

28683 INVLD_FILE_OR_DIR

EventType="error"

Message="Invalid file or directory: %s"

28684 DIR_CREATED

EventType="information"

Message="Directory created: %s"

28685 SEG_ID_GENERATED

EventType="information"

Message="New generated seg id: %s"

28686 SEG_ID_RELEASED

EventType="information"

Message="Seg id released: %s"

28687 PKG_ID_GENERATED

EventType="information"

Message="New generated package id: %s"

28688 PKG_ID_RELEASED

EventType="information"

Message="Package id released: %s"

28689 MAX_VER_REACHED

EventType="information"

Message="Max number of versions reached for physseg id: %s"

28690 MAX_VER_NUMBER_EXCEEDED

EventType="warning"

Message="Max version number exceeded for physseg id: %s"

28691 PKG_MAX_VER_REACHED

EventType="information"

Message="Max number of versions reached for pkg id: %s"

28692 PKG_MAX_VER_NUMBER_EXCEEDED

EventType="warning"

Message="Max version number reached for pkg id: %s"

28693 MAX_SET_DEPTH_REACHED

EventType="warning"

Message="Max set depth reached for set id: %s"

28694 MAX_SEQ_DEPTH_REACHED

EventType="warning"

Message="Max sequence depth reached for seq id: %s"

28695 NO_SEG_IN_DB

EventType="information"

Message="No segments in DB"

28696 AM_INVLD_SEG_ID

EventType="warning"

Message="Invalid segment id: %s"

28697 INVLD_PHYS_SEG_ID

EventType="warning"

Message="Invalid phys segment id: %s, ver: %s"

28698 AM_INVLD_PKG_ID

EventType="warning"

Message="Invalid package id: %s, ver: %s"

28699 AM_INVLD_PE_TYPE

EventType="warning"

Message="Invalid PE Type: %s"

28700 AM_INVLD_PROG_GRP

EventType="warning"

Message="Invalid program group: %s"

28701 AM_INVLD_SELECTOR_TYPE

EventType="warning"

Message="Invalid selector type: %s"

28702 AM_INVLD_SELECTOR_VAL

EventType="warning"

Message="Invalid selector value: %s"

28703 AM_ZIP_ARCHIVE_EXTRACTED

EventType="information"

Message="Zip archive extracted: %s"

28704 SET_INFINITE_LOOP

EventType="warning"

Message="Infinite loop in set id: %s"

28705 SEQ_INFINITE_LOOP

EventType="warning"

Message="Infinite loop in sequence id: %s"

28706 SEGID_NOT_UNIQUE

EventType="information"

Message="Seg id: %s is not unique"

28707 ALIAS_NOT_UNIQUE

EventType="information"

Message="Alias: %s is not unique"

28708 SELECTOR_VALUE_NOT_UNIQUE

EventType="information"

Message="Selector value: %s is not unique"

28709 SEGID_AND_ALIAS_NOT_UNIQUE

EventType="information"

Message="Seg id %s and alias %s are not unique"

28710 NO_PERM_TO_CACHE

EventType="information"

Message="No permission to set cache for user: %s"

28711 NO_PERM_TO_LOCK

EventType="information"

Message="No permission to change lock status for user: %s"

28712 INVLD_LOCK_STATUS

EventType="information"

Message="Seg id: %s cannot be added to locked package: %s"

28713 INVLD_PKG_FORMAT

EventType="warning"

Message="Invalid package format, segment id: %s cannot be added to package: %s"

Administration Configuration management function logs

This section contains Administration Configuration management logs.

47203 FTL99 SEGMENT NOT PROVISIONED

EventType="error"

Message="A segment was not able to be provisioned. (severity = CRITICAL)%s"

47105 FTL01 LANG_VER_PROV_PROBLEM

EventType="error"

Message="The langver.dat file was not able to be provisioned. (severity = MAJOR)%s"

47106 FTL02 IPS_PROVISIONER_TERMINATION

EventType="error"

Message="The provisioner experienced early termination. (severity = CRITICAL)%s"

47106 FTL02 IPS_PROVISIONER_TERMINATION / APS DATA BASE IS DOWN

EventType="error"

Message="The provisioner experienced early termination. (severity = CRITICAL)%s" ERROR: <date> <time> APS Data Base Instance <instance name> is down!

47107 FLT03 NODE_NOT_PROVISIONED

EventType="error"

Message="A specified node was not provisioned. (severity = MAJOR)%s"

47135 FTL31 FILE_ACCESS_FAILURE

EventType="error"

Message="A file cannot be accessed. Probable causes: incorrect file permissions or full filesystem. (severity = CRITICAL)%s"

File Upload logs

This section contains File Upload logs.

43009 FT_SW_EXCEPTION

EventType="error"

Message="Software exception: %s"

43010 FT_SQL_EXCEPTION

EventType="error"

Message="SQL exception: %s"

43011 FT_IO_FILE_ERR

EventType="error"

Message="IO file error: %s"

43012 FTP_CONNECT

EventType="information"

Message="Connected to host IP: %s"

43013 FTP_CONNECT_ERROR

EventType="error"

Message="Could not connect to host IP: %s"

43014 FTP_CDW_FAILED

EventType="warning"

Message="Could not change directory to: %s"

43015 FTP_FILE_FAILED

EventType="warning"

Message="File %s could be not transferred."

43016 FT_ZIP_ARCHIVE_EXTRACTED

EventType="information"

Message="ZIP archive extracted: %s"

Administration logs

This section contains Administration logs.

26625 CM_SW_EXCEPTION

EventType="error"

Message="Software exception: %s"

26626 CM_SQL_EXCEPTION

EventType="error"

Message="SQL exception: %s"

26627 CM_DB_ERR

EventType="error"

Message="Error while accessing the DB."

26628 NULL_VALUE

EventType="warning"

Message="Null value for: %s"

26629 CREATE_USER_ERR

EventType="error"

Message="Error creating user: %s"

26630 CREATE_DIR_ERR

EventType="error"

Message="Error creating directory: %s"

26631 CREATE_NODE_ERR

EventType="error"

Message="Error creating node: %s"

26632 REMOVE_NODE_ERR

EventType="error"

Message="Error removing node: %s"

26633 HOSTF_UPDATE_ERR

EventType="error"

Message="Error updating host file: %s"

26634 NODE_NOT_ENABLED

EventType="information"

Message="Node not enabled: %s"

26635 CM_INVLD_PROG_GRP

EventType="warning"

Message="Invalid program group: %s"

26636 CM_INVLD_SEG_ID

EventType="warning"

Message="Invalid segment id: %s"

26637 CM_INVLD_PKG_ID

EventType="warning"

Message="Invalid package id: %s"

26638 CM_INVLD_PE_TYPE

EventType="warning"

Message="Invalid PE Type: %s"

26639 CM_INVLD_SELECTOR_TYPE

EventType="warning"

Message="Invalid selector type: %s"

26640 CM_INVLD_SELECTOR_VAL

EventType="warning"

Message="Invalid selector value: %s"

26641 INVLD_PROV_SET

EventType="warning"

Message="Invalid provisionable set: %s"

26642 INVLD_NODE_ID

EventType="warning"

Message="Invalid node id: %s"

26643 INVLD_USER_ID

EventType="warning"

Message="Invalid user id: %s"

26644 INVLD_SYS_PARM_VALUE

EventType="warning"

Message="Invalid sys parm value: %s"

26645 INVLD_ENTITY

EventType="warning"

Message="Invalid entity: %s of entity type: %s"

26646 INVLD_OLD_PSWD

EventType="information"

Message="Invalid old password for user: s%"

26647 CALLP_SEL_VALUE_NOT_UNIQUE

EventType="information"

Message="Callp Selector value: %s is not unique"

26648 PRG_GRP_NOT_UNIQUE

EventType="information"

Message="Program group: %s is not unique"

26649 PROV_SET_NOT_UNIQUE

EventType="information"

Message="Provision set: %s is not unique"

26650 SELTYPE_DISPVAL_NOT_UNIQUE

EventType="information"

Message="Selector type display value: %s is not unique"

26651 USER_NO_ACCESS

EventType="information"

Message="User: %s has no access to program group: %s"

26652 SELECTOR_TYPE_EXISTS

EventType="information"

Message="Selector type: %s already exists"

26653 SELECTOR_VALUE_EXISTS

EventType="information"

Message="Selector value: %s already exists"

26654 ASSOCIATION_EXISTS

EventType="warning"

Message="Association already exists between %s and %s"

26655 CHG_PERM_EXIT_CODE

EventType="information"

Message="Exit code: % while changing permission on: %s"

26656 REM_NODE_EXIT_CODE

EventType="information"

Message="Exit code: % while removing node: % from %s"

26657 REM_DIR_EXIT_CODE

EventType="information"

Message="Exit code: % while removing userdir for user: %s"

26658 INCONSISTENT_ARRY_SIZE

EventType="warning"

Message="Inconsistent array sizes between %s and %s"

26659 CALLP_VAL_NOT_UNIQUE

EventType="information"

Message="CallP value: %s is not unique"

26660 SELVAL_NOT_UNIQUE

EventType="information"

Message="Selector value: %s is not unique"

26661 DISPVAL_NOT_UNIQUE

EventType="information"

Message="Selector type display value: %s is not unique"

26662 CM_INVLD_AE_TYPE

EventType="warning"

Message="Invalid AE Type: %s"

Viewing UAS logs through the Universal Audio Server Manager in a telnet session

This procedure enables you to view UAS logs through the Universal Audio Server Manager, in a telnet session.

Viewing UAS logs through the Universal Audio Server Manager in a telnet session

At a management station

1 Create a telnet session with the Universal Audio Server Manager.

2 Enter the following commands to display the content of the ptmlog file:

```
cd /var/log

less -i ptmlog
```

The content of the ptmlog file displays.

3 Search for the hostname of the network element for which you want a log display. The following commands will enable you to search the file:

```
/ <hostname> (provides a forward search)

? <hostname> (provides a backward search)
```

The following procedures will enable you to maneuver through the file's content:

- to page forward, press the space bar
- to page backward, enter ctrl-b
- to go to the top of the file, press the escape key (Esc), then press the Shift key and >
- to go the bottom of the file, press Esc, then press the Shift key and <

4 To view additional detail about the logs and to determine the corrective action required, refer to the log listing in <u>UAS logs on page 55</u>.

5 You have completed this procedure.

Viewing UAS logs through Windows Event Viewer

This procedure enables you to view UAS logs through the Windows Event Viewer tool.

Viewing UAS logs through Windows Event Viewer

At the Windows desktop interface

1   Select **Start -> Programs -> Administrative Tools -> Event Viewer**.

The Event Viewer window displays.

2   In the Tree panel located on the left side of the window, select either Application Log, Security Log, or Event Log.

3   In the resulting Log display on the right side of the Event Viewer window, double-click on a log.

The system displays details related to the log, including the log text, in an Event Properties window.

If	Do
you want to configure the amount of disk space allowed for the log display	step 4
you want to set the event filters	step 5

4   In the Tree panel of the Event Viewer window, select either Application Log, Security Log, or Event Log.

   a   Select "Properties" in the pull-down menu under Action.

     A Log Properties window displays.

   b   In the General tab of the Log Properties window, select a Maximum Log Size, according to the table below, and then select the "Overwrite events as needed" radio button.

   c   To save the changes you have made, click Apply and, when instructed, click Clear Log; to Cancel the changes you have made, click Cancel.

d To dismiss the screen, click OK.

Windows Event Log Settings

Log	Maximum Log Size (kbyte)	Event Log Wrapping
System	1024	Overwrite events as needed
Application	4096	Overwrite events as needed
Security	1024	Overwrite events as needed

e Go to step 6.

5 In the Tree panel of the Event Viewer window, select either Application Log, Security Log, or Event Log.

a Select "Properties" in the pull-down menu under Action.

A Log Properties window displays.

b In the Log Properties window, select the Filter tab. Make your selections in the Filter tab.

c To apply the changes you have made, click Apply; to Cancel the changes you have made, click Cancel.

d To dismiss the screen, click OK.

6 You have completed this procedure.

Viewing UAS events through the dumpel tool

This procedure enables you to view events from Windows system, security, and application event logs through the Windows dumpel tool. Audio Server events (logs and alarms) are stored in the Windows "application" event log.

Viewing UAS events through the dumpel tool

At the Windows desktop interface

1   Open a command interface by performing the following steps:

     a   select **Start -> Run**

     b   type **cmd** in the window that displays

     c   click OK or press Enter

2   Enter the following command to display the content of the "application" file:

     `dumpel -l application | more`

     The content of the Windows "application" event log file displays. Piping the command through the "more" command enables you to view one screen of information at a time.

3   If you wish, instead, to create a file containing the content of the application file, enter the following command:

     `dumpel -f <file name.txt> -l application`

     where *<file name.txt>* is the name you give the file

     Note: Other input options available for the Dumpel command can be viewed by entering "dumpel -h" at the command line.

     The "more" program can be used to search the file for a particular string. The following commands will enable you to search the file using "more":

     `more <file name.txt>`

     `/ <string> (provides a forward search)`

     `? <string> (provides a backward search)`

     The following procedures will enable you to maneuver through the file's content:

     •   to page forward, press the space bar

     •   to page backward, enter ctrl-b

- to go to the top of the file, press the escape key (Esc), then press the Shift key and >

- to go to the bottom of the file, press Esc, then press the Shift key and <

    Note: A text editor program like "Notepad" can also be used to examine the file contents.

To view additional detail about the logs and alarms and to determine the corrective action required, refer to the log listing in UAS logs on page 55 and to the alarm listing in UAS alarms on page 6.

4   You have completed this procedure.

Viewing Component states

The UAS Manager enables you to display a list of component (managed object instance) states. The following states are maintained for the UAS software and hardware components:

- alarm state
- administrative state
- operational state
- availability
- usage

The possible alarm states include:

- cleared
- critical
- major
- minor
- warning

All alarms in the UAS are associated with software or hardware components. The alarm state of a component is dependent upon the active alarms, if any, that are associated with the component. If there are no active alarms, then the alarm state of a component is "cleared". If there are active alarms, then the alarm state of the component depends upon the severity-level of its most severe, active alarm.

The possible administrative states include:

- unlocked
- locked
- shutting down

The administrative state is not applicable to every component. If the administrative state is not maintained for a component, the default administrative state value "unlocked" is displayed.

The possible operational states include:

- enabled
- disabled

The operational state is not applicable to every component. If the operational state is not maintained for a component, the default value "enabled" is displayed.

Availability status is displayed for every component. The possible status values, and the rules governing the status values displayed are shown in the following list:

- "notInstalled" or "normal", for fans

- "notInstalled", "powerOff", or "normal", for power supplies

- "offline", "powerOff", or "notInstalled", for card base- and service-levels (described below), carrier, and host ethernet interface

- "normal", for all other components

The possible usage states include:

- idle

- active

- busy

If the usage state is not maintained for a component, the default value "idle" is displayed.

Each card component has a set of "base-level" states, that provide information about low-level functionality of the card. The base-level card states are found in the component, "Card_<slot>". Thus, a card for which the base-level states are provided, is identified by the slot number in which the card resides.

Each IO card, in addition, has a set of "service-level" states, that provide information about high-level functionality of the card. Service-level states apply only to the AG4000 and CG6000 cards. The service-level states information for these cards is found in the entries, "AG4000_<slot>" and "CG6000_<slot>".

The following procedure enables you to view all of the UAS component states.

Viewing Component states

At the Network Element Status panel of the Universal Audio Server Manager

1   In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

2   In the pull-down list in the box labeled, "Please select," select Maintenance.

3   In the Maintenance Tree pane, select "Node".

4   Click the "View Components States" button located at the bottom of the Node States pane.

The View Component States Dialog window displays. The component states display includes a separate row of information for each component. For a description of the state information as it applies to each component, consult the "Component states" table below. The information in the table is arranged in alphabetical order, by component name. To view complete information about an alarm condition shown in the display, consult your solution's Fault Management document for the appropriate procedure. Specific information about an alarm can be found in .

The display is a snapshot. If you wish to view an updated version of the display, click Refresh.

5   You have completed this procedure.

The following table contains state information about the components represented in the rows in the display.

Component states

Display category	Value
Activity_Manager_0	
Products	all
Category	software
Description	Represents the states of the Activity Manager process (AM.exe). This process is part of the Nortel Networks Global Server base software upon which the UAS software is built.
Administration State	Changes are not supported. Will always have a value of "unlocked".
Operational State	Not maintained. Will always have a value of "enabled".
Availability Status	Not maintained. Will always have a value of "normal".
Usage Status	Not maintained. Will always have a value of "idle".
AG4000_<slot>	

Component states

Display category	Value
Products	UAS_ATM
Category	hardware (card)
Description	Represents the service-level states of an AG4000 DSP card.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	The operational state of an AG4000 card will be "enabled" unless one or more of the following conditions are true: 1) initialization of the card is not complete 2) the application software is experiencing an excessive amount of errors when attempting to use the card 3) the base-level operational state is "disabled" (because of a card extraction)
Availability status	The availability status of the AG4000_<slot> component is always the same as the availability status of the associated Card_<slot> component. See the description of the "Card_<slot>" component for possible availability status values.
Usage state	For cards not configured for test trunks, the usage state is always "idle". For a card configured for test trunks, the usage state of the card is dependent upon the usage states of the carriers on that card. The rules used to determine usage state of an AG4000 card are listed under the "CG6000_<slot>" component.
AtmPort_<n>	
Products	UAS-ATM
Category	hardware
Description	Represents the states of an ATM port, where <n> is a unique identifier derived from the physical slot number and atm port number, as follows: slot*10 + port.
Administrative state	Lock force is supported.

Component states

Display category	Value
Operational state	The operational state of an ATM port will be "enabled" unless the ATM communications link is down.
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Nor maintained. Will always have a value of "idle".

Atm_Service_0	
Products	UAS-ATM
Category	software
Description	Represents the states of the ATM service component in an ATM-based UAS.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability state	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".

Audio_Access_0	
Products	UAS-ATM and UAS-IP
Category	software
Description	Represents the states of the audio access component, which is responsible for accessing audio on the local disk.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".

BCT_Service_0	

Component states

Display category	Value
Products	UAS-ATM and UAS-IP, with BCT support enabled
Category	software
Description	Represents the states of the BCT service component.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	In a UAS-ATM system, the operational state of the BCT service will be "enabled" unless one or more of the following conditions are true: 1) the BCT service subsystem did not initialize 2) the ATM service is disabled In a UAS-IP system, the operational state of the BCT service will be "enabled" unless one or more of the following conditions are true: 1) the BCT service subsystem did not initialize 2) no BCT card resources are available
Availability state	Not maintained. Will always have a value of "normal".
Usage state	For UAS-ATM, not maintained. Will always have a value of "idle". For UAS-IP, possible values are: "idle" - if no BCT channels are in use "active" - if one or more, but not all, BCT channels are in use "busy" - if all BCT channels are in use
Call_Agent_Connection_0	
Products	all
Category	software
Description	Represents the states of the connection to the call agent.

Component states

Display category	Value
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
Call_Engine_0	
Products	all
Category	software
Description	Represents the states of the main call engine component.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
Callp_Subagent_0	
Products	all
Category	software
Description	Represents the states of the SNMP subagent component that runs inside the main call processing application.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
Card_<slot>	

Component states

Display category	Value
Products	all
Category	hardware (card)
Description	Represents the base-level states of an AG4000 or CG6000 card, where <slot> is the physical slot number, 1-6 in domain A (left side) or 11-16 in domain B (right side).
Administrative state	Changes are not supported in UAS-ATM systems. Will always have a value of "unlocked". Lock force and lock graceful are supported in UAS-IP. The possible base-level administration states include: "unlocked" - the firmware load has been successfully loaded into the card "locked" - the card is not available for use. A card's base-level administrative state can move into a "locked" state under these conditions: 1) the card was extracted from the chassis 2) the card was locked at the base level, through the EM 3) the card failed to initialize The card service-level state must be "locked" before a card can be locked at the base level.
Operational state	The operational state of a card will be "enabled" unless one or more of the following conditions are true: 1) for AG4000 or CG6000, there was a failure in loading firmware into the card 2) the card was extracted 3) for a CG6000, there is a base-level administrative lock from the EM

Component states

Display category	Value
Availability status	The possible abnormal card availability status values are: "offline" - power to the slot is on, but no card is present in the slot "powerOff" - power to the slot is turned off "notInstalled" - there is no card in the slot
Usage state	Not maintained. Will always have a value of "idle".
CarrierMtc_0	
Products	UAS with test trunks
Category	software
Description	Represents the states of the carrier maintenance subsystem, which is responsible for maintaining the states of the carriers.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
Carrier_<n>	
Products	UAS with test trunks
Category	hardware
Description	Represents the states of carrier <n>, where <n> is the index of the carrier in the entPhysicalTable of the Entity MIB (RFC2737).
Administrative state	Changes are not supported. Will always have a value of "unlocked".

Component states

Display category	Value
Operational state	The operational state of the carrier will be "enabled" unless one or more of the following conditions are true: 1) initialization of the carrier is not complete 2) a carrier alarm is raised 3) the card is out of service
Availability status	The possible abnormal availability status values are: "degraded" - the carrier operational state is still "enabled" but the service is degraded. At lease one of the carrier performance parameters has exceeded the pre-defined threshold value. This is called "Threshold Crossing Alert (TCA)." "dependency" - the carrier operational state is "disabled" because of one of these conditions: 1) a carrier alarm is raised 2) the card is out of service "notInstalled" - the card on which the carrier resides is not installed
Usage state	The carrier usage state is dependent on the usage states of all the channels on that carrier, according to these rules: - if all bearer channels are "idle", then the usage state of the carrier is "idle" - if all bearer channels are busy, then the usage state of the carrier is "busy" - some bearer channels are idle and some bearer channels are busy, then the usage state of the carrier is "active" The usage state of a DS0 (CAS-channel) is either "idle" or "busy".
Carrier Channel	
Products	UAS with test trunks
Category	hardware

Component states

Display category	Value
Description	Represents the states of a carrier channel (DS0). *Note:* The UAS EM does not display channel states.
Administrative state	In a UAS with test trunks, changes are not supported. Will always have a value of "unlocked".
Operational state	The operational state of a channel will be "enabled" unless one or more of the following conditions are true: 1) initialization of the channel is not complete 2) the carrier is "disabled" or locked 3) a failure of the channel is detected
Availability status	The possible abnormal carrier channel availability status values are: "dependency" - the carrier is "disabled" or locked "failed" - a failure of the channel is detected "notInstalled" - the channel is not part of a trunk group
Usage state	The possible usage state values for a CAS test channel are: "idle" - not being used on a call "busy" - being used on a call The possible usage state values for a PRI D-channel are: "idle" - not in use "active" - in use
CG6000_<slot	
Products	IP-based UAS
Category	hardware (card)
Description	Represents the service -level states of a CG6000C voice over IP card.

Component states

Display category	Value
Administrative state	In a UAS-IP system, a lock force and lock graceful are supported. A CG6000 card cannot be unlocked at the service level unless the base-level state of the card is "unlocked".
Operational state	The operational state of a CG6000 card will be "enabled" unless one or more of the following conditions are true: 1) initialization of the card is not complete 2) both ethernet interfaces on the card have failed 3) the application software is experiencing an excessive amount of errors when attempting to use the card 4) the base-level operational state is "disabled" (because of a base-level card lock or because of a card extraction)
Availability status	The availability status of the CG6000_<slot> component is always the same as the availability status of the associated Card_<slot> component. See the description of the "Card_<slot>" component for possible availability status values.
Usage state	For cards configured for IVR, BCT, or conferencing, the usage state is always "idle". For cards configured for trunking (test trunks or PRI), the usage state of the card is dependent on the usage states of the carriers on that card, according to the following rules: - if all carrier ports on a card are "idle", then the card usage state is "idle" - if all carrier ports are busy (all channels on all ports are in use), then the card usage state is "busy" - if there is a mix of idle, active, and busy carrier ports, the card usage state is "active"
ChassisEventManager_0	
Products	all
Category	software

Component states

Display category	Value
Description	Represents the states of the chassis event manager process (CEM.exe). This process is part of the Nortel Networks Global Server base software upon which the UAS software is built. The chassis event manager is responsible for maintaining and monitoring fans, power supplies, slots, and base-level states of cards.
Administrative state	Changes are not support. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
Conferencing_Service_0	
Products	IP-based UAS, only if conferencing is enabled
Category	software
Description	Represents the states of the conferencing service component.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	The operational state of the conferencing service will be "enabled" unless one or more of the following conditions are true: 1) the conferencing service subsystem did not initialize 2) no card resources are available
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Possible values are: "idle" - if no conferencing channels are in use "active" - if one or more, but not all, conferencing channels are in use "busy" - if all conferencing channels are in use

Component states

Display category	Value
Cooling_System_0	
Products	all
Category	hardware
Description	Represents the state of the overall cooling system, as determined by temperature sensors in the chassis. The alarm status will normally be "cleared," but will change if a chassis temperature threshold is exceeded.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
EthernetInterface_0	
Products	all
Category	hardware
Description	Represents the state of the host network adapter, which is used for messaging related to call control and device management. This host network adapter has two physical interfaces. The adapter is run in Adapter Fault Tolerance (AFT) mode, which provides automatic redundancy. If the primary adapter fails, the secondary takes over. The alarm status will normally be "cleared." If a link goes down, the alarm status will change to critical and the availability status will be set to "degraded."
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "unlocked".
Availability status	The possible abnormal value is: - degraded; one of the ethernet interface links is down
Usage state	Not maintained. Will always have a value of "idle".

Copyright © 2005, Nortel Networks

Component states

Display category	Value
Fan_<n>	
Products	Domain A (left-hand CPU) systems only (all configurations)
Category	hardware
Description	Represents the states of fan <n>, where <n> is 1, 2, 0r 3.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	The operational state of a fan will be "enabled" unless one or more of the following conditions are true: 1) the sled is extracted 2) there is a problem with the fan
Availability status	Possible values are: "notInstalled" - there is no fan unit in the sled. A fan unit needs to be put in the sled, or perhaps the sled needs to be reseated "normal" - the fan unit is present in the sled
Usage state	Not maintained. Will always have a value of "idle".
Hard_Disk_<n>	
Products	Domain A (left-hand CPU) systems only (all configurations)
Category	hardware
Description	Represents the states of the hard disk, where <n> is 1 or 2. Hard disk 1 is the hard disk for domain A and hard disk 2 is the hard disk for domain B. Currently, states for hard disk 2 can only be monitored by domain A software. Therefore, there will be two hard disk components listed under domain A, Hard_Disk_1 and Hard_Disk_2, but none listed under domain B. If you want to view the hard disk states for domain B, then you must view the components dialog for domain A.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".

Component states

Display category	Value
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
IVR_Service_0	
Products	UAS with IVR support enabled
Category	software
Description	Represents the states of the IVR service component.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	In a UAS-ATM system, the operational state of the IVR service will be "enabled", unless one or more of the following conditions are true: 1) the BCT service subsystem did not initialize 2) the ATM service is "disabled" In a UAS-IP system, the operational state of the IVR service will be "enabled", unless one or more of the following conditions are true: 1) the IVR service subsystem did not initialize 2) no card resources are available
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Possible values are: "idle" - if no IVR channels are in use "active" - if one or more IVR channels are in use
LocalResourceManager_0	
Products	all
Category	software

Component states

Display category	Value
Description	Represents the states of the local resource manager process (LRM.exe). This process is part of the Nortel Network Global Server base software upon which the UAS software is built. The local resource manager process is responsible for monitoring CPU usage, memory usage, and disk space usage.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
Main_Subagent_0	
Products	all
Category	software
Description	Represents the states of the main subagent application, which is responsible for maintaining the active alarm table, maintaining fan, power supply, and hard disk states, and forwarding logs and alarms to the element manager through SNMP traps.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
NodeMtc_0	
Products	all
Category	software
Description	Represents the states of the node maintenance subsystem, which is responsible for maintaining the states of the network element.

Component states

Display category	Value
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
Power_Supply_<n>	
Products	Domain A (left-hand CPU) systems only (all configurations)
Category	hardware
Description	Represents the states of power supply <n>, where <n> is 1, 2, or 3.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	The operational state of a power supply will be "enabled", unless one or more of the following conditions are true: 1) the sled is extracted 2) there is a problem with the power supply
Availability status	Possible values are: "notInstalled" - there is no power supply unit in the sled. Perhaps the sled needs to be reseated. "powerOff" - the power supply is not supplying power "normal" - power is on for that power supply unit in the sled, and/or the power supply unit is present in the sled
Usage state	Not maintained. Will always have a value of "idle".
ProgramManager_<n>	
Products	all
Category	software

Component states

Display category	Value
Description	Represents the states of the program manager processes (pmgr.exe). The program manager is part of the Nortel Networks Global Server base software upon which the UAS software is built. The program manager processes are responsible for starting, stopping, and monitoring application processes. The program manager processes are controlled by a Windows service called pmgrdaemon. Every UAS-based product has one program manager process associated with the component name, "ProgramManager_0".
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
Resource_Manager_0	
Products	all
Category	software
Description	Represents the states of the resource manager component, which is responsible for maintaining pools of endpoints.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
SCSI_Controller_<slot>	
Products	all
Category	hardware (card)

Component states

Display category	Value
Description	Represents the base-level states of the SCSI controller card, where <slot> is 8 in domain A, or 10 in domain B. A separate SCSI controller card is found only in systems with the CPV5350 processor card.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
ShelfController_<slot>	
Products	all
Category	hardware (card)
Description	Represents the base-level states of the shelf controller card (CPV5350 or CPV5370 processor card), where <slot> is 7 in domain A or 9 in domain B.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	Not maintained. Will always have a value of "enabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Not maintained. Will always have a value of "idle".
System_0	
Products	all
Category	software
Description	Represents the states of the network element, that is, the node. In the UAS EM (UAS Manager) and PRI EM, these states are displayed when "Node" is selected in the navigation tree in the maintenance screen.
Administrative state	Lock force and lock graceful are supported in all configurations, UAS-ATM and UAS-IP.

Component states

Display category	Value
Operational state	For UAS, the operational state of the node is dependent on the operational state of the underlying "node services". Node services include the IVR service, conferencing service, BCT service, and test trunk service. If one or more node services are "enabled", then the node operational state is "enabled". If all node services are "disabled", then the node operational state is "disabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	For UAS-ATM and UAS-IP, system usage state is dependent on the usage state of the underlying node services: "idle" - all node services are "idle" "active" - one or more node services are active or busy *Note:* In ATM systems, usage state on the BCT service is not maintained and is always "idle". Therefore, the BCT service usage state does not factor into the determination of ATM system usage state. That means that a BCT-only system will always have a system usage state of "idle".
TrunkTest_Service_0	
Products	UAS-ATM or UAS-IP, with test trunk support enabled
Category	software
Description	Represents the states of the test trunk service component.
Administrative state	Changes are not supported. Will always have a value of "unlocked".
Operational state	In a UAS-ATM system, the operational state will be "enabled" unless one or more of the following conditions are true: 1) the trunk test service subsystem did not initialize 2) the ATM service is "disabled" In a UAS-IP system, set to "disabled" at the beginning of Test Trunk service initialization. Set to "enabled" if the trunk test service initializes successfully.
Availability status	Not maintained. Will always have a value of "normal".

Component states

Display category	Value
Usage state	Usage state will be: "idle" - if no test trunk channels are in use "active" - if one or more test trunk channels are in use "busy" - if all test trunk channels are in use
Trunk_Group_<n>	
Products	UAS with test trunks
Category	software
Description	Represents the states of a trunk group, where <n> is a unique trunk group identifier.
Administrative state	Lock force and lock graceful are not supported in the UAS.
Operational state	The operational state of a CAS trunk group is dependent on the number of channels that are in service. If one or more channels are in service. then the operational state of the trunk group is "enabled". If no channels are in service, then the operational state of the trunk group is "disabled".
Availability status	Not maintained. Will always have a value of "normal".
Usage state	Usage state will be: "idle" - if no channels are in use "active" - if one or more channels are in use "busy" - if all channels in the trunk group are in use

Checking system visual indicators

The visual indicators described below provide you with the means of determining quickly the operational status of the UAS hardware.

Chassis alarm panel

The alarm panel located at the top of the CPX8216T chassis contains LEDs arranged in three groups: System Status indicators; Telco alarm indicators; and card slot status indicators. The System Status indicators and the card slot status indicators are not operational. The Telco alarm indicators, located in the upper-right corner of the alarm panel, are operational. These LEDs are activated in response to Critical, Major, and Minor system alarms raised in both domains of the chassis. If a system alarm is raised either in a single domain, or in both domains, of a chassis, the appropriate Telco alarm indicator on the panel is activated. The color scheme for the Telco alarm indicators is shown in the following table.

Telco Alarm Indicators

LED	Color
Minor	Yellow
Major	Red
Critical	Red

Although the UAS can be deployed in pairs of systems (domains) on a single chassis, some situations may require that only one system be deployed on a chassis. In that event, the single system must be configured in the left-hand domain of the chassis (when viewed from the front of the chassis), or "A" domain. This ensures that the system alarms can activate the appropriate Telco alarm LEDs on the CX8216T chassis alarm panel.

The UAS can be configured in either a dc or an ac cabinet. In a dc configuration, the CPX8216T chassis alarm panel is cabled to the breaker interface panel located at the top of the cabinet. This enables the alarm indicators on the breaker interface panel to be activated when alarms are activated on the alarm panel of any of the CPX8216T chassis provisioned in the cabinet. The ac configuration does not have cabinet LEDs.

AG4000C CompactPCI

The faceplate of the main (front) AG4000C module, shown in the Figure labeled , has the following indicator LEDs:

- Trunk LEDs

- Hot Swap LED

The trunk LEDs show trunk interface status information. Three LEDs per trunk display the status about each of four T1 or E1 trunks, as described in the following table.

AG4000C trunk LEDs

LED	Status indicated
Green	Indicates proper frame sync to the trunk: all required framing alignment has been found. This LED is extinguished if one or more of the following conditions exist: - all ones alarm (AIS) - loss of frame - loss of signaling multiframe - CRC errors (when the board is configured for Extended Super Frame (ESF))
Yellow	Indicates remote loss of frame, or remote loss of signaling multiframe for the respective trunk
Red	Indicates loss of frame, loss of signal, or bit error rate for the respective trunk

The blue Hot Swap LED, when illuminated, indicates that it is safe to remove the module from the system.

AG4000C front module faceplate

Frame SYNC Indicator (green)
Remote Fault Alarm (yellow)
Line Fault Alarm (red)

1 — Trunk 1
2 — Trunk 2
3 — Trunk 3
4 — Trunk 4

Hot Swap
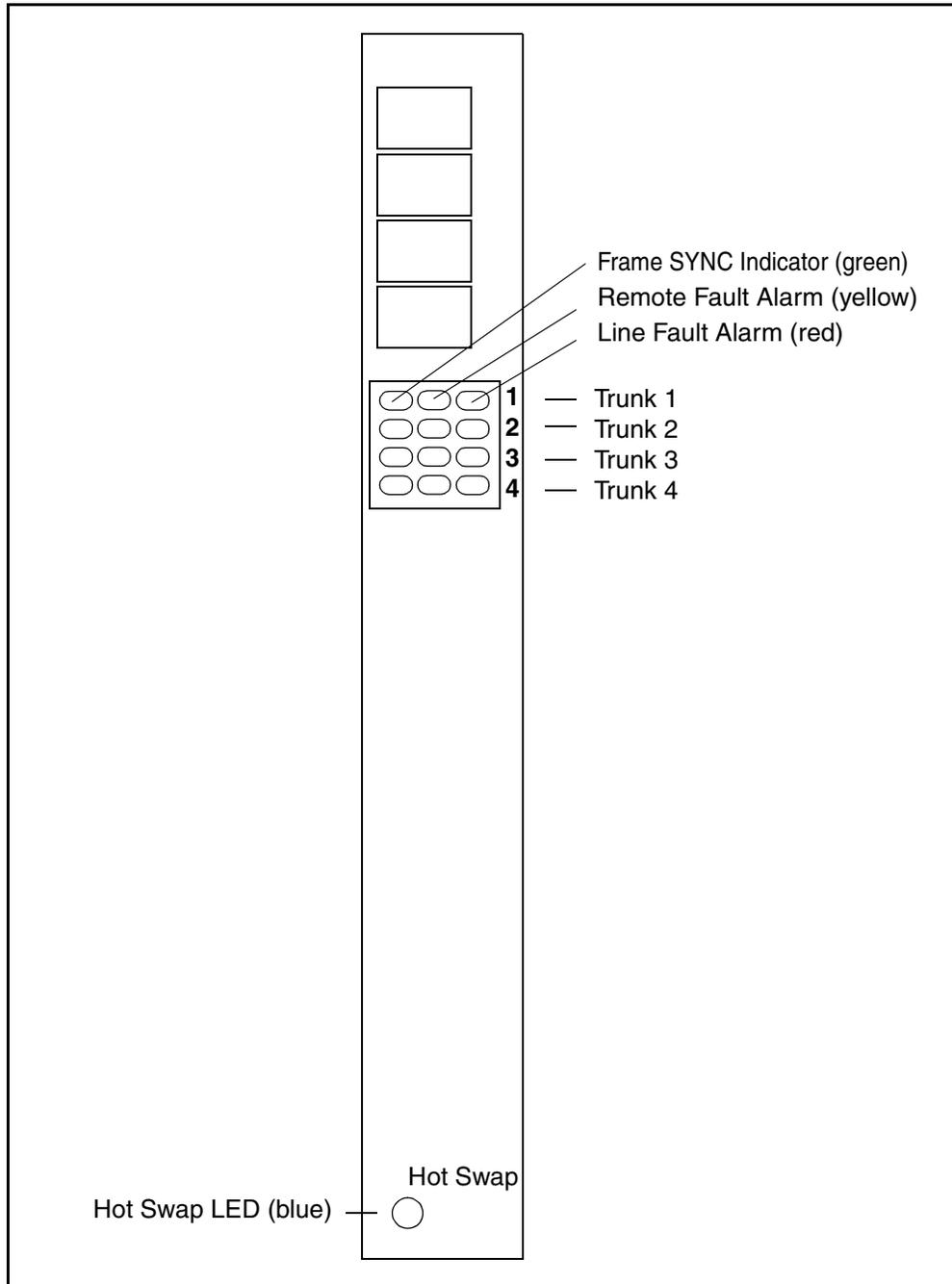
Hot Swap LED (blue)

CG6000C

The faceplate of the main (front) CG6000C module, shown in the Figure labeled [CG6000C front module faceplate on page 215](#), has the following indicator LEDs:

- Ethernet LEDs

- Trunk LEDs

- Hot Swap LED

The Ethernet LEDs provide information about the Ethernet links, as described in the following table:

CG6000C Ethernet LEDs

LED	Status indicated
LINK	Indicates the status of the Ethernet link. If the LED is illuminated, the respective Ethernet link is reliable, that is, the connection has been established.
100Mb	Indicates the data rate of the respective Ethernet link. When the LED is illuminated, the data rate is 100 Mbps. When the LED is extinguished, the data rate is 10 Mbps. This LED is used only when a reliable Ethernet connection has been established, that is, the LINK LED is illuminated.
ACTIVITY	Indicates the transmitting/receiving activity on the respective Ethernet link. When activity is present on the Ethernet link, the LED will flicker.

The trunk LEDs show trunk interface status information. Three LEDs per trunk display the status about each of four T1 or E1 trunks. The use and meaning of the trunk LEDs are only defined for the PRI Trunk Gateway configuration.

The blue Hot Swap LED, when illuminated, indicates that it is safe to remove the module from the system. The LED is illuminated in response to one of the following conditions:

- If the module is fully inserted when the backplane is powered up, the blue LED flashes momentarily. This is a normal part of the initialization process.

- After opening the lock latches (during the extraction process), the LED illuminates, indicating that it is safe to remove the module.

- If the LED remains illuminated after insertion of the module and after you have closed the lock latches, the module failed to successfully perform its primary hardware initialization. Although it is safe to remove the module, this condition indicates a problem.

CG6000C front module faceplate

LINK
100Mb
ACTIVITY

1 —— Ethernet 1(green)
2 —— Ethernet 2 (green)

Frame SYNC Indicator (green)
Remote Fault Alarm (yellow)
Line Fault Alarm (red)

1 —— Trunk 1
2 —— Trunk 2
3 —— Trunk 3
4 —— Trunk 4

Hot Swap

Hot Swap LED (blue) —— ◯
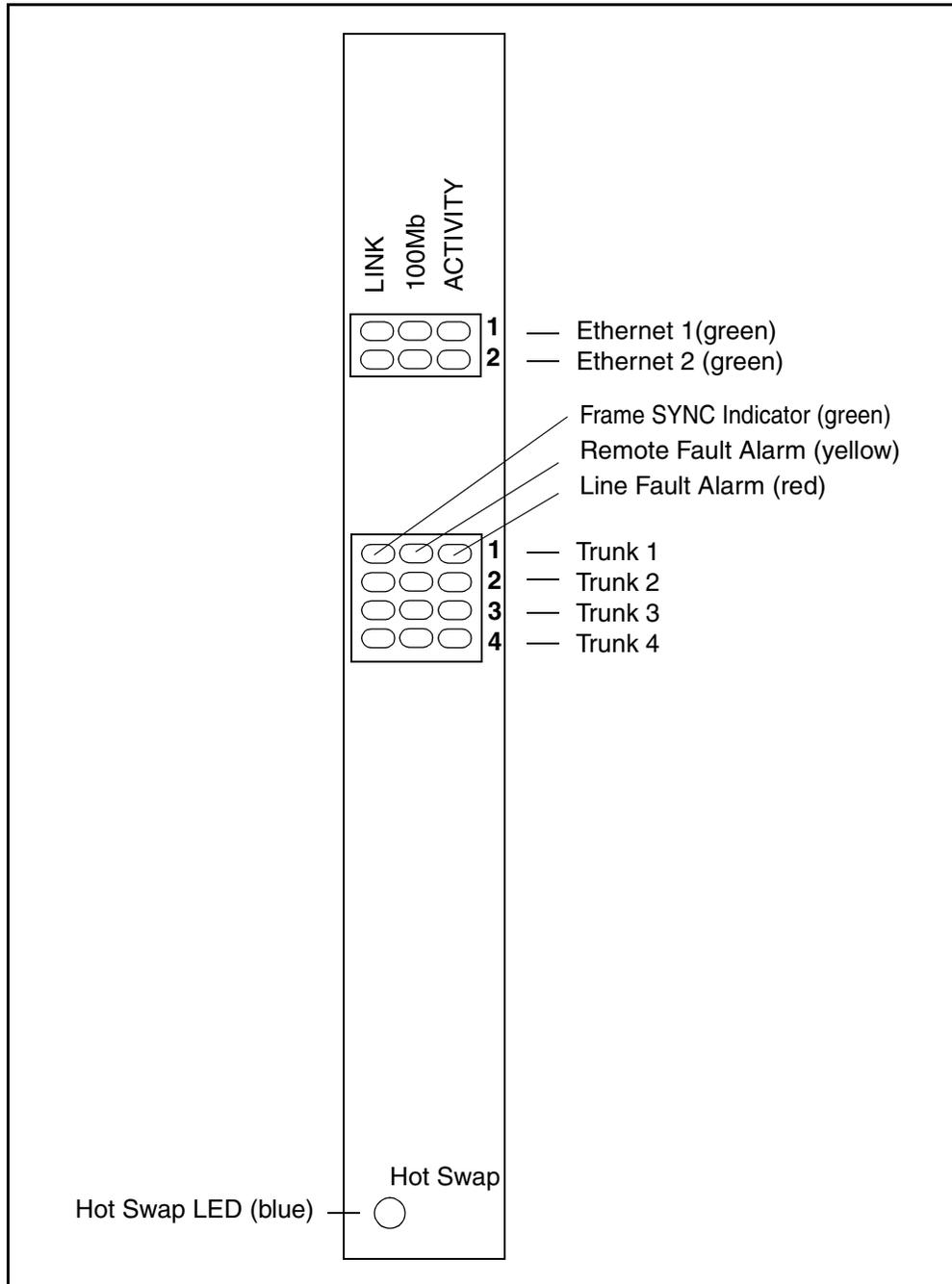
Configuring the log distribution profile

Network element software collects logs from various sources in the network element server. The Main Subagent component sends the logs to the management station through an SNMP trap. Log event sources include:

- the Win2K system event log

- the Win2K security event log

- the Win2K application event log

- network element applications

Events from the Win2K system event log, the Win2K application event log and network element applications can be either information, warning, or error events. Events from the Win2K security event log can be either audit-succeed or audit-fail.

The Main Subagent can be configured to send either all logs from all sources, or only certain types of logs for each source, to the Universal Audio Server Manager station. For the Win2K system event log, the Win2K application event log and audio server applications the Main Subagent can be configured to send:

- all logs for that source

- only warning and error logs for that source (default)

- only error logs for that source

- no logs for that source

For the Win2K security event log, the Main Subagent can be configured to send:

- all security logs

- only audit-fail logs (default)

- no logs for that source

Configuring the log distribution profile

At the Network Element Status panel of the Universal Audio Server Manager

1   In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

2   In the System Identification pane, pull down the "Please select" menu and select Configuration.

3   In the Network Element Tree pane, select "Node".

Tabs display in the "Details of selected tree node" pane. Each tab selects a separate screen used for data filling.

4   Select the "Log Levels" tab.

5   In the "Log Levels" tab window, verify and/or select new information for the following fields:

- **System Log Level**

  System logs are information, warning, or error events. This field specifies that the Main Subagent is to send either all logs for that source, only warning and error logs for that source, only error logs for that source, or no logs for that source to the element management station.

- **UAS Log Level**

  Audio Server logs include information, warning, or error events. This field specifies that the Main Subagent is to send either all logs for that source, only warning and error logs for that source, only error logs for that source, or no logs for that source to the element management station.

- **Application Log Level**

  Application logs include information, warning, or error events. This field specifies that the Main Subagent is to send either all logs for that source, only warning and error logs for that source, only error logs for that source, or no logs for that source to the element management station.

- **Security Log Level**

  Logs are either audit-succeed or audit-fail. This field specifies that the Main Subagent is to send either all security logs, only audit-fail logs, or no logs for that source to the element management station.

6   Click Save.

7   You have completed this procedure.

Rebooting a UAS through the Universal Audio Server Manager

This procedure enables you to reboot the UAS through the Universal Audio Server Manager.

Rebooting a UAS through the Universal Audio Server Manager

At the Network Element Status panel of the Universal Audio Server Manager

1 In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

2 In the pull-down list in the box labeled, "Please select," select Maintenance.

3 In the Maintenance Tree pane, select "Node".

4 Click the node entry that displays in the table shown in the Node States pane.

5 Lock the node by clicking the "Lock Graceful" button located at the bottom of the Node States pane.

6 Reboot the UAS node by clicking the "Reboot" button located at the bottom of the Node States pane.

7 Click OK in the Reboot Gateway Warning window.

8 Click OK in the Warning window.

9 You have completed this procedure.

Rebooting an audio server remotely through a telnet session

This procedure enables you to reboot a UAS using a command line interface, through a telnet session. The procedure should be performed only when the Universal Audio Server Manager is down due to a hardware or network problem.

Rebooting an audio server remotely through a telnet session

⚠ **CAUTION**
This procedure disrupts service. The first step in this procedure stops the call processing (callp) application.

In a telnet connection to the UAS

1   Stop Universal Audio Server applications by typing the following command:

   net stop pmgrdaemon

2   Enter the following command:

   `shutdown/l/r`

   Note: /l specifies a local shutdown; /r specifies that a reboot is to occur after shutdown has been completed.

3   You have completed this procedure.

Rebooting an audio server through a Windows interface

This procedure enables you to reboot a UAS through a Windows interface. The procedure should be performed only when the Universal Audio Server Manager is down due to a hardware or network problem.

Rebooting an audio server through a Windows interface

> ⚠ **CAUTION**
> **This procedure disrupts service. The first step in this procedure stops the call processing (callp) application.**

At the Windows desktop interface

1   Stop any applications that may be running.

    a   Access the "Services" window as follows:

        select **Start -> Programs -> Administrative Tools -> Services**

    b   Right-click **PMGRdaemon service** and select Stop. Wait for notification that the applications have stopped.

2   Re-boot the system by performing the following steps:

    a   select **Start -> Shutdown**

    b   select "restart the computer" in the Shutdown Windows screen.

3   You have completed this procedure.

Restarting a UAS through the Universal Audio Server Manager

This procedure enables you to restart UAS applications through the UAS Manager.

Restarting a UAS through the Universal Audio Server Manager

At the Network Element Status panel of the Universal Audio Server Manager

1   In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

2   In the pull-down list in the box labeled, "Please select," select Maintenance.

3   In the Maintenance Tree pane, select "Node".

4   Click the node entry that displays in the table shown in the Node States pane.

5   Lock the node by clicking the "Lock Graceful" button located at the bottom of the Node States pane.

6   Restart the node by clicking the "Restart Application" button located at the bottom of the Node States pane.

7   Click OK in the Restart Application Warning window.

8   Click OK in the Warning window.

9   You have completed this procedure.

Stopping and Restarting Universal Audio Server applications through the command line interface

This procedure enables you to stop and start Universal Audio Server applications through the command line interface in order to perform configuration and maintenance activities.

Note: Universal Audio Server applications can also be stopped and started through the Windows desktop interface; see the procedure .

Stopping and Restarting Universal Audio Server applications through the command line interface

```
┌─────────────────────────────────────────────────────────────┐
│   ⚠      CAUTION                                              │
│          This procedure disrupts service. The first step in  │
│          this procedure stops the call processing (callp)    │
│          application.                                        │
└─────────────────────────────────────────────────────────────┘
```

At the Windows desktop interface

1   Stop the UAS applications by performing the following steps:

    a   select **Start -> Run**

    b   type **cmd** in the window that displays

    c   press Enter

    d   type **net stop pmgrdaemon** in the window that displays

    e   press Enter

2   Start the UAS applications by performing the following steps:

    a   select **Start -> Run**

    b   type **cmd** in the window that displays

    c   press Enter

    d   type **net start pmgrdaemon** in the window that displays

    e   press Enter

3   View a list of active services by performing the following steps:

    a   select **Start -> Run**

    b   type **cmd** in the window that displays

c press Enter

d type **net start** in the window that displays

e press Enter

4 You have completed this procedure.

Stopping and Restarting Universal Audio Server applications through the Windows interface

This procedure enables you to stop and start Universal Audio Server applications through the Windows desktop interface in order to perform configuration and maintenance activities.

Note: Universal Audio Server applications can also be stopped and started through the command line; see the procedure <u>Stopping and Restarting Universal Audio Server applications through the command line interface on page 222</u>.

Stopping and Restarting Universal Audio Server applications through the Windows interface

> **CAUTION**
> **This procedure disrupts service. The first step in this procedure stops the call processing (callp) application.**

At the Windows desktop interface

1 Stop any UAS applications that are running.

   a Access the "Services" window as follows:

   select **Start -> Programs -> Administrative Tools -> Services**

   b Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

2 Start the UAS applications.

   a Access the "Services" window as follows:

   select **Start -> Programs -> Administrative Tools -> Services**

   b Right-click PMGRdaemon service and select Start.

3 You have completed this procedure.

Resetting a processor on the mate UAS domain

This procedure causes a reset (reboot) of a mate UAS domain processor contained in the UAS chassis, when access to the processor to be reset cannot be gained through the Universal Audio Server Manager.

Note: Since this procedure is performed <u>remotely</u>, you must first identify the inaccessible UAS domain and then record the IP address of its <u>mate</u> UAS domain, before you perform the procedure. You will then telnet to this mate UAS domain and, from it, enter the command to reset the inaccessible processor.

Resetting a processor on the mate UAS domain

At the Windows desktop interface

1 Open a command interface by performing the following steps:

    a select **Start -> Run**

    b type **cmd** in the window that displays

    c press Enter

2 On the command line, telnet to the mate UAS domain, from which the reset command is to be issued. For more information, see the Note above.

3 Enter the following command to cause the reset of the inaccessible mate UAS processor:

`domainreset`

    Note: The mate UAS domain must have Global Server software installed on it in order for this command to be used.

4 You have completed this procedure.

Changing the Admin state

Using the Universal Audio Server Manager, you can change the administrative state of the UAS node either to unlocked (in service) or locked (out of service).

Although the network element unit is locked, its applications continue to run, but it does not receive any new requests.

Changing the Admin state

At the Network Element Status panel of the Universal Audio Server Manager

1   In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

2   In the pull-down list in the box labeled, "Please select," select Maintenance.

3   In the Maintenance Tree pane, select "Node".

4   Click the node entry that displays in the table shown in the Node States pane.

5   Determine whether you are locking or unlocking the node.

If	Do
you are locking the node	Step 6
you are unlocking the node	Step 9

6   Lock the node by clicking either the "Lock Graceful" button or the "Lock (Force)" button located at the bottom of the Node States pane. A graceful lock of the node allows existing calls to complete before the node is removed from service. A forced lock of the node terminates immediately any existing calls and then removes the node from service.

7   If you force locked the node ("Lock (Force)"), click OK in the Lock Force Warning window.

8   Go to step 10.

9   Unlock the node by clicking the "Unlock" button located at the bottom of the Node States pane.

10   You have completed this procedure.

Adding a CG6000 to a UAS node

This procedure enables you to add a new CG6000 card set to a UAS node.

Adding a CG6000 to a UAS node

> **WARNING**
> **Static electricity damage**
> While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

> **CAUTION**
> **Possible equipment damage**
> Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

At the Network Element Status panel of the Universal Audio Server Manager

1 In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

2 In the pull-down list in the box labeled, "Please select," select Maintenance.

3 In the Maintenance Tree pane, select "Node".

4 Click the node entry that displays in the table shown in the Node States pane.

5 Lock the node by clicking the "Lock Graceful" button located at the bottom of the Node States pane.

At the Windows desktop interface

6   Stop any applications that may be running.

   a   Access the "Services" window as follows:

   select **Start -> Programs -> Administrative Tools -> Services**

   b   Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

Note: You may wish to leave the Services window open, for use later in this procedure.

At the shelf of the UAS node being serviced

7   Insert the new rear module in the appropriate card slot:

   a   With a Phillips head screwdriver, loosen the screws that secure the faceplate over the slot into which the rear module will be inserted and remove the filler faceplate.

   b   Insert the rear module in the slot, lock the lock latches on the module, and tighten the screws that secure the module in the slot.

8   Insert the new front module in the appropriate card slot:

   a   With a Phillips head screwdriver, loosen the screws that secure the faceplate over the slot into which the front module will be inserted and remove the filler faceplate.

   b   Insert the front module in the slot, lock the lock latches on the module, and tighten the screws that secure the module in the slot.

   c   Perform any required cabling.

At the Windows desktop interface

9   Update the uas.conf file to reflect the card configuration in the UAS node.

    a Launch the Local Configuration Interface GUI by performing the following steps:

      i open a command window by selecting **Start -> Run**

      ii type **lci** in the window that displays

        Note: The first letter in the lci command is an "l", as in "local."

      iii click OK or press Enter

        Because you have added a card set to the shelf, the Save Card Type Difference screen displays, indicating that the uas.conf file has been automatically updated to reflect the changed card configuration on the shelf.

    b Click OK in the Save Card Type Difference screen and then click OK in the subsequent "Card type is saved" confirmation window that displays. Finally, click the "Cards folder", located in the Network element Tree pane.

      The "Details of selected tree node" card screen displays.

    c Review the card list that displays. An entry for the card that you just installed will appear in the card list. Double click the "Cards Folder", located in the Network element Tree pane and, from the list of cards that displays below the "Cards Folder", click the bullet associated with the card that has been added.

      A card detail screen displays.

    d Enter information in the following fields in the screen:

- IP address associated with the CG6000C card
- network mask associated with the CG6000C card
- default router associated with the CG6000C card
- Bearer Channel Tandeming (BCT) support capability for the CG6000C card, either Enabled or Disabled.
- Test Trunk Support; select either Enabled or Disabled
- Test Trunk Config Size; select the appropriate size (small - 50k trunks; medium - 100k trunks; large - 200k trunks),

when Test Trunk Support is Enabled. This determines the number of channels available for tests.

- Sage Box 1 IP (address); enter when Test Trunk Support is Enabled. One Sage test box is use for small and medium test trunk configurations.

- Sage Box 2 IP (address); enter if a second Sage test box is required, when Test Trunk Support is Enabled. Two Sage test boxes are used for large configurations.

   Note: The Card Type field cannot be changed.

   e Click Validate.

   f Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select "Save". Click OK when the confirmation screens display.

   g Close the Local Configuration Interface GUI screens by pulling down the menu under File and selecting "Exit", and then close the command window.

10   Restart the UAS by performing the following steps:

   a If the "Services" window is not already open, access the "Services" window as follows:

     select **Start -> Programs -> Administrative Tools -> Services**

   b Right-click PMGRdaemon service and select Start. Wait for approximately 2 or 3 minutes before performing the next step, to ensure that the UAS has restarted.

At the Network Element Status panel of the Universal Audio Server Manager

11   In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

12   In the pull-down list in the box labeled, "Please select," select Maintenance.

13   In the Maintenance Tree pane, select "Node".

14   Click the node entry that displays in the table shown in the Node States pane.

15   Unlock the node by clicking the "Unlock" button located at the bottom of the Node States pane.

16   You have completed this procedure.

Removing a CG6000 from a UAS node

This procedure enables you to remove a CG6000 card set from a UAS.

Removing a CG6000 from a UAS node

<table>
<tr>
<td>⚡</td>
<td>

WARNING
Static electricity damage
While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

</td>
</tr>
</table>

<table>
<tr>
<td>⚠</td>
<td>

CAUTION
Possible equipment damage
Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

</td>
</tr>
</table>

At the Network Elements pane of the Universal Audio Server Manager main screen

1   In the Network Elements pane, select the UAS node containing the CG6000 card set to be operated on.

Information about the node displays in the System Identification pane.

2   In the pull-down list in the box labeled, "Please select," select Maintenance.

3   In the Maintenance Tree pane, select "Node".

4   Click the node entry that displays in the table shown in the Node States pane.

5   Lock the node by clicking the "Lock Graceful" button located at the bottom of the Node States pane.

At the Windows desktop interface

6   Stop any applications that may be running.

    a   Access the "Services" window as follows:

        select **Start -> Programs -> Administrative Tools -> Services**

    b   Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

    Note: You may wish to leave the Services window open, for use later in this procedure.

At the shelf of the UAS node being serviced

7   Remove the front module by performing the following steps:

    a   With a Phillips head screwdriver, loosen the screws that secure the module in the slot.

    b   Unlock the lower lock latch on the module.

    c   Unlock the upper lock latch on the module and remove the module from the slot.

        Note: The blue light located at the bottom of the card may light momentarily as the card is being extracted.

    d   Install a filler faceplate over the slot from which the front module was removed and tighten the screws that secure the faceplate in position.

8   Remove the rear module by performing the following steps:

    a   Perform any required cable removal.

    b   With a Phillips head screwdriver, loosen the screws that secure the module in the slot.

    c   Unlock the lock latches on the module.

    d   Remove the module from the slot.

    e   Install a filler faceplate over the slot from which the rear module was removed and tighten the screws that secure the faceplate in position.

At the Windows desktop interface

9   Update the uas.conf file to reflect the card configuration in the UAS node.

      a   Launch the Local Configuration Interface GUI by performing the following steps:

          i   open a command window by selecting **Start -> Run**

          ii   type **lci** in the window that displays

               Note: The first letter in the lci command is an "l", as in "local."

          iii   click OK or press Enter

               Because you have removed a card set from the shelf, the Save Card Type Difference screen displays, indicating that the uas.conf file has been automatically updated to reflect the changed card configuration on the shelf.

      b   Click OK in the Save Card Type Difference pop-up and then click OK in the subsequent "Card type is saved" confirmation pop-up that displays. Finally, click the "Cards folder", located in the Network element Tree pane.

         The "Details of selected tree node" cards screen displays.

      c   Review the card list that displays. The card you removed should not appear on the list.

      d   Close the Local Configuration Interface GUI screens by pulling down the menu under File and selecting "Exit", and then close the command window.

10   To effect the card configuration change you have made, restart the UAS by performing the following steps:

      a   If the "Services" window is not already open, access the "Services" window as follows:

         select **Start -> Programs -> Administrative Tools -> Services**

      b   Right-click PMGRdaemon service and select Start. Wait for approximately 2 or 3 minutes before performing the next step, to ensure that the UAS has restarted.

At the Network Elements pane of the Universal Audio Server Manager main screen

11   In the Network Elements pane, select the UAS node containing the CG6000 card set that was operated on.

Information about the node displays in the System Identification pane.

12   In the pull-down list in the box labeled, "Please select," select Maintenance.

13   In the Maintenance Tree pane, Select "Node".

14   Click the node entry that displays in the table shown in the Node States pane.

15   Unlock the node by clicking the "Unlock" button located at the bottom of the Node States pane.

16   You have completed this procedure.

Replacing CG6000 cards

This procedure enables you to replace faulty CG6000 cards in a UAS node.

Replacing CG6000 cards

⚠	**WARNING** **Static electricity damage** While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

⚠	**CAUTION** **Possible equipment damage** Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

At the Network Elements pane of the Universal Audio Server Manager main screen

1   In the Network Elements pane, select the UAS node containing the CG6000 card set to be operated on.

     Information about the node displays in the System Identification pane.

2   In the pull-down list in the box labeled, "Please select," select Maintenance.

3   In the Maintenance Tree pane, select "Cards Folder".

4   In the table of cards that displays in the Contents of Cards Folder pane, click the entry for the card to be operated on.

5   Perform a graceful lock on the card by clicking the "Lock Graceful" button located at the bottom of the Contents of Cards Folder pane.

6   Perform a base-level lock on the card by clicking the "Base Level Lock" button located at the bottom of the Contents of Cards Folder pane.

> *Note:* The red "out of service" light located above the card on the alarm panel will light when the card has been successfully locked.

7   Determine the steps to follow based on the card configuration action you are performing.

If	Do
you are replacing only a front module	step 8
you are replacing only a rear module	step 11
you are replacing both a front module and a rear module	step 16

At the shelf of the UAS node being serviced

8   Remove the front module by performing the following steps:

    a   With a Phillips head screwdriver, loosen the screws that secure the module in the slot.

b Unlock the lower lock latch on the module. When you unlock the lower lock latch, the blue light located at the bottom of the module faceplate will light.

Note: It is possible, on rare occasions, that a card failure may affect the hot swap circuitry and prevent the blue light, which indicates that it is safe to remove the card, from illuminating. **If this occurs, the card cannot be removed safely without first shutting down the processor - premature removal of a peripheral card (no blue light illuminated) can cause the operating system to crash, resulting in loss of service.** It is recommended to leave the card locked and wait until a maintenance interval during which the processor can be rebooted safely by performing the procedure, <u>Rebooting a UAS through the Universal Audio Server Manager on page 218</u>. After the reboot, the card can be removed and replaced by continuing from this step, in this procedure.

c Unlock the upper lock latch on the module and remove the module from the slot.

Note: <u>Both the blue light on the module faceplate and the red "out of service" light, located above the module on the alarm panel, must be lit before you can remove the module</u>.

9 Insert the new front module, lock the lock latches on the card and tighten the screws that secure the card in the slot.

10 Go to step <u>20</u>.

11   Remove the front module by performing the following steps:

    a With a Phillips head screwdriver, loosen the screws that secure the module in the slot.

    b Unlock the lower lock latch on the module. When you unlock the lower lock latch, the blue light located at the bottom of the module faceplate will light.

        Note: It is possible, on rare occasions, that a card failure may affect the hot swap circuitry and prevent the blue light, which indicates that it is safe to remove the card, from illuminating. **If this occurs, the card cannot be removed safely without first shutting down the processor - premature removal of a peripheral card (no blue light illuminated) can cause the operating system to crash, resulting in loss of service.** It is recommended to leave the card locked and wait until a maintenance interval during which the processor can be rebooted safely by performing the procedure, Rebooting a UAS through the Universal Audio Server Manager on page 218. After the reboot, the card can be removed and replaced by continuing from this step, in this procedure.

    c Unlock the upper lock latch on the module and remove the module from the slot.

        Note: Both the blue light on the module faceplate and the red "out of service" light, located above the module on the alarm panel, must be lit before you can remove the module.

12   Remove the rear module by performing the following steps:

    a   With a Phillips head screwdriver, loosen the screws that secure the module in the slot.

    b   Unlock the lock latches on the module.

    c   Remove the module from the card slot.

13   Insert the new rear module, lock the lock latches, and tighten the screws that secure the module in the slot.

14   Insert the front module that you removed in step 11. Lock the lock latches on the card and tighten the screws that secure the card in the slot.

15   Go to step 20.

16   Remove the front module by performing the following steps:

    a   With a Phillips head screwdriver, loosen the screws that secure the module in the slot.

    b   Unlock the lower lock latch on the module. When you unlock the lower lock latch, the blue light located at the bottom of the module faceplate will light.

        Note: It is possible, on rare occasions, that a card failure may affect the hot swap circuitry and prevent the blue light, which indicates that it is safe to remove the card, from illuminating. **If this occurs, the card cannot be removed safely without first shutting down the processor - premature removal of a peripheral card (no blue light illuminated) can cause the operating system to crash, resulting in loss of service.** It is recommended to leave the card locked and wait until a maintenance interval during which the processor can be rebooted safely by performing the procedure, Rebooting a UAS through the Universal Audio Server Manager on page 218. After the reboot, the card can be removed and replaced by continuing from this step, in this procedure.

    c   Unlock the upper lock latch on the module and remove the module from the slot.

        Note: Both the blue light on the module faceplate and the red "out of service" light, located above the module on the alarm panel, must be lit before you can remove the module.

17   Remove the rear module by performing the following steps:

    a   With a Phillips head screwdriver, loosen the screws that secure the module in the slot.

    b   Unlock the lock latches on the module.

    c   Remove the module from the slot.

18   Insert the new rear module, lock the lock latches, and tighten the screws that secure the module in the slot.

19   Insert the new front module. Lock the lock latches on the module and tighten the screws that secure the module in the slot.

At the Network Elements pane of the Universal Audio Server Manager main screen

20   In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

21   In the pull-down list in the box labeled, "Please select," select Maintenance.

22   In the Maintenance Tree pane, select "Cards Folder".

23   In the table of cards that displays in the Content of Cards Folder pane, select the entry for the card that you have been operating on.

24   Perform a base-level unlock on the card by clicking the "Base Level Unlock" button located at the bottom of the Node States pane.

25   Complete unlocking the card by clicking the "Unlock" button located at the bottom of the Contents of Cards Folder pane.

26   You have completed this procedure.

Adding an AG4000 card to a UAS node

This procedure enables you to add an AG4000 card to a UAS node.

Adding an AG4000 card to a UAS node

⚠	**WARNING** **Static electricity damage** While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

⚠	**CAUTION** **Possible equipment damage** Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

At the Network Element Status panel of the Universal Audio Server Manager

1   In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

2   In the pull-down list in the box labeled, "Please select," select Maintenance.

3   In the Maintenance Tree pane, select "Node".

4   Click the node entry that displays in the table shown in the Node States pane, to activate the buttons located at the bottom of the Node States pane.

5   Lock the node by clicking the "Lock Graceful" button located at the bottom of the Node States pane.

At the Windows desktop interface

6   Stop any applications that are running.

    a   Access the "Services" window as follows:

        select **Start -> Programs -> Administrative Tools -> Services**

    b   Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

    Note: You may wish to leave the Services window open, for use later in this procedure.

At the shelf of the UAS node being serviced

7   Add the AG4000 by performing the following steps:

    Note: Ensure that the variant of the card you are adding (that is, E1 or T1) is the same as the variant of any cards already installed on the shelf.

    a   Determine whether the AG4000 will be used for trunk testing.

        Note: Only cards of variant type, T1 can be used for trunk testing.

If	Do
the AG4000 will be used for trunk testing	step **b**
the AG4000 will not be used for trunk testing	step **d**

    b   With a Phillips head screwdriver, loosen the screws that secure the faceplate over the slot into which the rear AG4000 module will be inserted and remove the filler plate.

    c   Insert the new module into the slot, lock the lock latches, and tighten the screws that secure the module in the slot.

    d   With a Phillips head screwdriver, loosen the screws that secure the faceplate over the slot into which the front AG4000 module will be inserted and remove the filler plate.

    e   Insert the new module into the slot, lock the lock latches, and tighten the screws that secure the module in the slot.

    f   Perform any required cabling.

8   Determine whether the uas.conf file needs to be updated.

If	Do
the AG4000 will be used for trunk testing, the uas.conf file will need to be updated	step 9
the AG4000 will not be used for trunk testing, the uas.conf file will not need to be updated	step 12

At the Windows desktop interface

9   Update the uas.conf file to reflect the new card configuration in the UAS node.

   a   Launch the Local Configuration Interface GUI by performing the following steps:

   i   open a command window by selecting **Start -> Run**

   ii   type **lci** in the window that displays

   Note: The first letter in the lci command is an "l", as in "local."

   iii   click OK or press Enter

   iv   click "Node" in the Network Element Tree pane

10   The bearer type ATM-AAL2 configuration screen displays. Three tabs display in the "Details of selected tree node" window. Each tab selects a separate screen used for data filling.

   a   In the Network Element tree pane, double-click the "Cards Folder," which is located below the "Node" folder.

   A list of the AG4000s provisioned in the UAS node displays.

   b   In the list, click the bullet associated with the AG4000 that you have just installed.

   A card detail window displays in the "Details of selected tree node" screen.

   c   Enter information in the following fields in the card detail window:

   •   Test Trunk Support (Enabled)

   •   Test Trunk Config Size (select the appropriate size)

   •   Sage Box 1 IP (enter the appropriate IP address)

   •   Sage Box 2 IP (when a second box is required, enter the appropriate IP address)

    d Click Validate and then click OK in the message screen indicating that the configuration is valid.

    e Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select "Save". Click OK when the confirmation screen displays, and then click OK in the message screen indicating that the configuration data has been saved.

11   Close the Local Configuration Interface GUI by pulling down the menu under File and selecting "Exit", and then close the command window.

12   Restart the UAS by performing the following steps:

    a If the "Services" window is not already open, access the "Services" window as follows:

        select **Start -> Programs -> Administrative Tools -> Services**

    b Right-click PMGRdaemon service and select Start. Wait for approximately 2 or 3 minutes before performing the next step, to ensure that the UAS has restarted.

At the Network Element Status panel of the Universal Audio Server Manager

13   In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

14   In the pull-down list in the box labeled, "Please select," select Maintenance.

15   In the Maintenance Tree pane, select "Node".

16   Click the node entry that displays in the table shown in the Node States pane, to activate the buttons located at the bottom of the Node States pane.

17   Unlock the node by clicking the "Unlock" button located at the bottom of the Node States pane.

18   You have completed this procedure.

Removing an AG4000 from a UAS node

This procedure enables you to remove an AG4000 from a UAS node.

Removing an AG4000 from a UAS node

	WARNING **Static electricity damage** While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

	CAUTION **Possible equipment damage** Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

At the Network Element Status panel of the Universal Audio Server Manager

1   In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

2   In the pull-down list in the box labeled, "Please select," select Maintenance.

3   In the Maintenance Tree pane, select "Node".

4   Click the node entry that displays in the table shown in the Node States pane, to activate the buttons located at the bottom of the Node States pane.

5   Lock the node by clicking the "Lock Graceful" button located at the bottom of the Node States pane.

At the Windows desktop interface

6 Stop any applications that are running.

a Access the "Services" window as follows:

select **Start -> Programs -> Administrative Tools -> Services**

b Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

Note: You may wish to leave the "Services" window open, for use later in this procedure.

At the shelf of the UAS node being serviced

7 Remove the AG4000 by performing the following steps:

a Perform any required cable removal at the rear of the chassis.

b With a Phillips head screwdriver, loosen the screws that secure the front AG4000 module in the slot.

c Unlock the lower lock latch on the module. When you unlock the lower lock latch, the blue light located at the bottom of the module faceplate will light.

d Unlock the upper lock latch on the module and remove the module from the slot.

e Install a filler faceplate over the slot from which the front module was removed.

f Determine whether the AG4000 was used for trunk testing.

If	Do
the AG4000 was used for trunk testing	step g
the AG4000 was not used for trunk testing	step 8

g With a Phillips head screwdriver, loosen the screws that secure the rear AG4000 module in the slot.

h Unlock the latches on the module and remove the module from the slot.

i Install a filler faceplate over the slot from which the rear module was removed.

At the Windows desktop interface

8   Update the uas.conf file to reflect the new card configuration in the UAS node.

    a   Launch the Local Configuration Interface GUI by performing the following steps:

        i   Open a command window by selecting **Start -> Run**

        ii   Type **lci** in the window that displays

            Note: The first letter in the lci command is an "l", as in "local."

        iii   Click OK or press Enter

        iv   If the fabric type of your system is ATM-AAL2 and if the card you removed was used for trunk testing, the message, "System does not have enough card to set up Test Trunk" displays. Click OK.

        v   If the fabric type of your system is ATM-AAL2 and if the card you removed was used for trunk testing, the message, "Test Trunk has been disabled" displays. Click OK.

        vi   Click "Node" in the Network Element Tree pane

        The LCI GUI main screen displays.

9   The message, "Data is inconsistent with the bearer type ATM. It is modified to function with this bearer type" may display. Click OK.

10   The configuration screen associated with the "General" tab displays in the "Details of selected tree node" window, appropriate for the bearer fabric type of your system. Click the Validate button located at the bottom of the screen.

11   Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select "Save". Click OK when the confirmation screen displays.

12   Close the Local Configuration Interface GUI by pulling down the menu under File and selecting "Exit", and then close the command window.

13   Restart the UAS by performing the following steps:

    a   If the "Services" window is not already open, access the "Services" window as follows:

    select **Start -> Programs -> Administrative Tools -> Services**

b Right-click PMGRdaemon service and select Start. Wait for approximately 2 or 3 minutes before performing the next step, to ensure that the UAS has restarted.

At the Network Element Status panel of the Universal Audio Server Manager

14 In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

15 In the pull-down list in the box labeled, "Please select," select Maintenance.

16 In the Maintenance Tree pane, select "Node".

17 Click the node entry that displays in the table shown in the Node States pane, to activate the buttons located at the bottom of the Node States pane.

18 Unlock the node by clicking the "Unlock" button located at the bottom of the Node States pane.

19 You have completed this procedure.

Replacing AG4000 cards

This procedure enables you to replace an AG4000 card.

Replacing AG4000 cards

> **WARNING**
> **Static electricity damage**
> While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

> **CAUTION**
> **Possible equipment damage**
> Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

At the Network Element Status panel of the Universal Audio Server Manager

1   In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

2   In the pull-down list in the box labeled, "Please select," select Maintenance.

3   In the Maintenance Tree pane, select "Node".

4   Click the node entry that displays in the table shown in the Node States pane.

5   Lock the node by clicking the "Lock Graceful" button located at the bottom of the Node States pane.

At the Windows desktop interface

6   Stop any applications that are running.

       a   Access the "Services" window as follows:

            select   **Start -> Programs -> Administrative Tools -> Services**

       b   Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

    Note: You may wish to leave the "Services" window open, for use later in this procedure.

At the shelf of the UAS node being serviced

7   With a Phillips head screwdriver, loosen the screws that secure the front module in the slot.

8   Unlock the lower lock latch on the module. When you unlock the lower lock latch, the blue light located at the bottom of the module faceplate will light.

9   Determine the next action to perform:

If	Do
you are replacing only the rear module	step 10
you are replacing only the front module	step 18
you are replacing both the rear module and the front module	step 21

10   Unlock the upper lock latch on the front module and pull out the module in the slot only far enough to disengage it from the back plane.

11   Perform any required cable removal.

12   With a Phillips head screwdriver, loosen the screws that secure the rear module in the slot.

13   Unlock the latches on the rear module and remove the module from the slot.

14   Insert the new rear module into the slot, lock the lock latches, and tighten the screws that secure the module in the slot.

       Note: Ensure that the variant of the card you are inserting (that is, E1 or T1) is the same as the variant of the card you are replacing.

15   Perform any required cabling.

16   Push the front module back into the slot, lock the lock latches, and tighten the screws that secure the module in the slot.

17   Go to step 28.

18   Unlock the upper lock latch on the front module and remove the module from the slot.

19   Insert the new front module into the slot, lock the lock latches, and tighten the screws that secure the module in the slot.

> *Note:* Ensure that the variant of the card you are inserting (that is, E1 or T1) is the same as the variant of the card you are replacing.

20   Go to step 28.

21   Unlock the upper lock latch on the front module and remove the module from the slot.

22   Perform any required cable removal.

23   With a Phillips head screwdriver, loosen the screws that secure the rear module in the slot.

24   Unlock the latches on the rear module and remove the module from the slot.

25   Insert the new rear module into the slot, lock the lock latches, and tighten the screws that secure the module in the slot.

> *Note:* Ensure that the variant of the card you are inserting (that is, E1 or T1) is the same as the variant of the card you are replacing.

26   Perform any required cabling.

27   Insert the new front module into the slot, lock the lock latches, and tighten the screws that secure the module in the slot.

> *Note:* Ensure that the variant of the card you are inserting (that is, E1 or T1) is the same as the variant of the card you are replacing.

At the Windows desktop interface

28   Restart the network element by performing the following steps:

     a   If the "Services" window is not already open, access the "Services" window as follows:

       select **Start -> Programs -> Administrative Tools -> Services**

     b   Right-click PMGRdaemon service and select Start. Wait for approximately 2 or 3 minutes before performing the next step, to ensure that the UAS has restarted.

At the Network Element Status panel of the Universal Audio Server Manager

29   In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

30   In the pull-down list in the box labeled, "Please select," select Maintenance.

31   In the Maintenance Tree pane, select "Node".

32   Click the node entry that displays in the table shown in the Node States pane.

33   Unlock the node by clicking the "Unlock" button located at the bottom of the Node States pane.

34   You have completed this procedure.

Replacing a SCSI Controller (CPV8540) card

This procedure enables you to replace a SCSI Controller (CPV8540) card.

Replacing a SCSI Controller (CPV8540) card

	WARNING **Static electricity damage** While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

	CAUTION **Possible equipment damage** Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

At the Network Elements pane of the Universal Audio Server Manager main screen

1   Using the procedure Changing the Admin state on page 226, set the administrative state for this UAS unit being serviced to "lock graceful."

The selected UAS unit informs the gateway controller (GWC) that it is disabled. The GWC stops sending call requests to this UAS unit.

At the Windows desktop interface

2   Stop any applications that are running.

    a   Access the "Services" window as follows:

       select **Start -> Programs -> Administrative Tools -> Services**

    b   Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

3   Shut down the system:

    select **Start -> Shut Down**

    a   On the Shut Down Windows screen, select "Shut down this computer." When the shutdown is complete and the system displays the message indicating that it is safe to turn off the computer, do <u>not</u> turn off power to the computer.

4   Locate the CPV8540 card. If the UAS node is located on the left side of the shelf, the card will be in slot 6; if the node is located on the right side of the shelf, the card will be in slot 11.

    a   Determine whether you are replacing only the front module, replacing only the rear module, or replacing both the front and the rear modules.

If	Do
you are replacing only the front module	step <u>b</u>
you are replacing only the rear module	step <u>e</u>
you are replacing both the front and the rear module	step <u>k</u>

    b   Remove the front module. (The screws that secure the module in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the modules can be removed.)

    c   Insert the new front module, lock the lock latches on the module and tighten the screws that secure the module in the shelf.

    d   Go to step <u>p</u>.

    e   Disconnect the SCSI cable from the rear transition module.

    f   Remove both front and rear modules<u>, in that order</u>. (The screws that secure the modules in the slots must be loosened with a Phillips head screwdriver, and the lock

latches must be unlocked, before the modules can be removed.)

g Insert the new rear transition module, lock the lock latches, and tighten the screws that secure the module in the shelf.

h Insert the front module that you removed in step f. Lock the lock latches on the module and tighten the screws that secure the module in the shelf.

i Reconnect the SCSI cable to the rear transition module.

j Go to step p.

k Disconnect the SCSI cable from the rear transition module.

l Remove both front and rear modules, in that order. (The screws that secure the modules in the slots must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the modules can be removed.)

m Insert the new rear transition module, lock the lock latches, and tighten the screws that secure the module in the shelf.

n Insert the new front module. Lock the lock latches on the module and tighten the screws that secure the module in the shelf.

o Reconnect the SCSI cable to the rear transition module.

p To effect the changes you have made, reset the system.

If	Do
you have a peer domain within the chassis, that has Global Server software installed on it	step q
you do not have a peer domain within the chassis	step t

q From the local KVM interface (system console), toggle/switch to the UAS domain that is the peer to the domain containing the card that was just replaced, by either

• pressing the RED -/+ buttons on the KVM switch

or

• pressing and releasing the <Ctrl> key followed by <Esc>

to bring up a list of the UAS nodes/domains on the overlay, from which (by using the arrow keys and pressing <Enter>) the domain can be chosen.

r Perform the following step to cause the reset of the inaccessible mate UAS processor:

`Start -> Run`

In the Run Dialog window that displays, type **domainreset** and then click OK.

> *Note:* The peer UAS domain must have Global Server software installed on it in order for this command to be used.

s Go to step 5.

t Unseat the CPV5350 Processor card associated with the domain being serviced and reseat the card in its slot. The CPV5350 card is located in slot 7 for the left domain and in slot 9 for the right domain. (The screws that secure the card in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the card can be removed. After the card is reseated in the slot, lock the lock latches, and tighten the screws that secure the card in the shelf.)

At the Network Elements pane of the Universal Audio Server Manager main screen

5 After the system reboot has completed, applications will automatically restart in the system but the network element will come up in an administrative "locked" state. Using the procedure Changing the Admin state on page 226 set the administrative state for this UAS unit to "unlocked."

The UAS unit informs the gateway controller (GWC) that it is enabled. The GWC then starts sending call requests to the unit.

6 You have completed this procedure.

Replacing a CPV5350 Processor card

This procedure enables you to replace a CPV5350 Processor card.

Replacing a CPV5350 Processor card

	WARNING **Static electricity damage** While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

	CAUTION **Possible equipment damage** Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

At the Network Elements pane of the Universal Audio Server Manager main screen

1   Using the procedure <u>Changing the Admin state on page 226</u>, set the administrative state for this UAS unit being serviced to "lock graceful."

   The selected UAS unit informs the gateway controller (GWC) that it is disabled. <u>The GWC stops sending call requests to this UAS unit.</u>

At the Windows desktop interface

2   Stop any applications that are running.

    a   Access the "Services" window as follows:

       select **Start -> Programs -> Administrative Tools -> Services**

    b   Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

3   Shut down the system:

    select **Start -> Shut Down**

    a   On the Shut Down Windows screen, select "Shut down this computer." When the shutdown is complete and the system displays the message indicating that it is safe to turn off the computer, do <u>not</u> turn off power to the computer.

4   Locate the CPV5350 card. If the UAS node is located in the left domain, the card will be in slot 7; if the node is located on the right domain, the card will be in slot 9.

    a   Determine whether you are replacing only the front module, replacing only the rear module, or replacing both the front and the rear modules.

If	Do
you are replacing only the front module	step <u>b</u>
you are replacing only the rear module	step <u>e</u>
you are replacing both the front and the rear module	step <u>k</u>

    b   Remove the front module. (The screws that secure the module in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the cards can be removed.)

    c   Insert the new front module, lock the lock latches on the card and tighten the screws that secure the module in the shelf.

    d   Go to step <u>5</u>.

    e   Disconnect the network interface cables, KVM, and connections from the rear transition module.

    f   Remove both front and rear modules,<u> in that order</u>. (The screws that secure the modules in the slots must be loosened with a Phillips head screwdriver, and the lock

latches must be unlocked, before the modules can be removed.)

g Insert the new rear transition module, lock the lock latches, and tighten the screws that secure the module in the shelf.

h Insert the front module that you removed in step f. Lock the lock latches on the card and tighten the screws that secure the card in the shelf.

i Reconnect the cables disconnected in step e.

j Go to step 5.

k Disconnect the network interface cables, KVM, and connections from the rear transition module.

l Remove both front and rear modules, in that order. (The screws that secure the modules in the slots must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the modules can be removed.)

m Insert the new rear transition module, lock the lock latches, and tighten the screws that secure the module in the shelf.

n Insert the new front module. Lock the lock latches on the module and tighten the screws that secure the module in the shelf.

o Reconnect the cables disconnected in step k.

5 The node will reboot upon insertion of the modules into the shelf. During the boot process, break into the BIOS menu using function key (F2) and ensure that the BIOS settings match those in the table located in BIOS Settings for CPV5350 SCSI on page 260.

At the Network Elements pane of the Universal Audio Server Manager main screen

6 After the system reboot has completed, applications will automatically restart in the system but the network element will come up in an administrative "locked" state. Using the procedure Changing the Admin state on page 226 set the administrative state for this UAS unit to "unlocked."

The UAS unit informs the gateway controller (GWC) that it is enabled. The GWC then starts sending call requests to the unit.

7 You have completed this procedure.

BIOS Settings for CPV5350 SCSI

This table provides you with the CPV5350 BIOS settings, when you are performing the procedure to replace the CPV5350 card.

Menu	Field or sub-menu	Field or sub-menu	Field or sub-menu	Setting
Main	BIOS Version			CPV5350 v1.0RM01
	Board Version			board specific
	Board Serial Number			board specific
	CPU Type			system specific
	CPU Speed			system specific
	Cache RAM			system specific
	Total Memory			system specific
	System Time			system specific
	System Date			system specific
	Diskette A			3.5 inch 1.44MB
	Diskette B			DISABLED
	Primary Master			NONE
	Primary Slave			NONE
	Secondary Master			NONE
	Secondary Slave			NONE

Menu	Field or sub-menu	Field or sub-menu	Field or sub-menu	Setting
Advanced	Plug and Play OS			NO
	Reset Configuration Data			NO
	L2 Cache ECC			Enabled
	ECC Memory Config			Disabled
	Memory Bank 0			256MB RAM
	PCI Configuration	Default Primary Video Adapter		AGP
		On Board Ethernet	On-board Ethernet 1	ENABLED
			Ethernet 1 Connection	REAR
			Ethernet 1 Option ROM	DISABLED
			On-board Ethernet 2	ENABLED
			Ethernet 2 Connection	REAR
			Ethernet 2 Option ROM	DISABLED
		USB Connection		FRONT
		HA Config		ENABLED
		DOMAIN A (applies only if HA Config = ENABLED)		ENABLED if left side DISABLED if right side

Menu	Field or sub-menu	Field or sub-menu	Field or sub-menu	Setting
		DOMAIN B (applies only if HA Config = ENABLED)		ENABLED if right side DISABLED if left side
		PCI/PNP IRQ CONFIGURATION	IRQ 9	Available
			IRQ 11	Available
			PCI IRQ Line 1	10
			PCI IRQ Line 2	10
			PCI IRQ Line 3	10
			PCI IRQ Line 4	10
	I/O Device Configuration	Serial Port A		ENABLED
		Base I/O Address		3F8
		Interrupt		IRQ 4
		Serial Port B		ENABLED
		Base I/O Address		2F8
		Interrupt		IRQ 3
		Parallel Port		Enabled
		Mode		Bi-directional
		Base I/O Address		378
		Interrupt		IRQ 7
	Local Bus IDE Adapter			DISABLED
	Large Disk Access Mode			DOS

Menu	Field or sub-menu	Field or sub-menu	Field or sub-menu	Setting
	Smart Device Monitoring			DISABLED
		Legacy USB Support		DISABLED
	REMOTE CONSOLE	Com Port		DISABLED
		BAUD Rate		9600
		Console Type		PC ANSI
		Flow Control		None
		Scan Lines		24
		Active After Post		OFF
	EMBEDDED FLASH	Status		Select source and load
		BIOS Image Source		Diskette Drive
		Load BIOS Image		ENTER
		CLEAR CMOS		YES
		Program Flash		ENTER
Security	USER Password is:			CLEAR
	Supervisor Password is:			CLEAR
	Set User Password			ENTER
	Set Supervisor Password			ENTER
	Password on Boot			DISABLED
Status				

Menu	Field or sub-menu	Field or sub-menu	Field or sub-menu	Setting
Boot	Floppy Check			ENABLED
	Quick Boot Mode			ENABLED
	Summary Screen			DISABLED
	Setup Prompt			ENABLED
	Num Lock			AUTO
	Boot Device Priority	Removable Devices		
		8XX SCSI CD-ROM SYMBIOS		
		Hard Drive		
		Legacy Network Support		
		ATAPI CD-ROM Drive		

Replacing a CPV5370 Processor card

This procedure enables you to replace a CPV5370 Processor card.

Replacing a CPV5370 Processor card

	WARNING **Static electricity damage** While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

	CAUTION **Possible equipment damage** Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

At the Network Elements pane of the Universal Audio Server Manager main screen

1   Using the procedure Changing the Admin state on page 226, set the administrative state for this UAS unit being serviced to "lock graceful."

The selected UAS unit informs the gateway controller (GWC) that it is disabled. The GWC stops sending call requests to this UAS unit.

At the Windows desktop interface

2   Stop any applications that are running.

   a   Access the "Services" window as follows:

      select **Start -> Programs -> Administrative Tools -> Services**

   b   Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

3   Shut down the system:

   select **Start -> Shut Down**

   a   On the Shut Down Windows screen, select "Shut down this computer." When the shutdown is complete and the system displays the message indicating that it is safe to turn off the computer, do <u>not</u> turn off power to the computer.

4   Locate the CPV5370 card. If the UAS node is located in the left domain, the card will be in slot 7; if the node is located on the right domain, the card will be in slot 9.

   a   Determine whether you are replacing only the front module, replacing only the rear module, or replacing both the front and the rear modules.

If	Do
you are replacing only the front module	step <u>b</u>
you are replacing only the rear module	step <u>e</u>
you are replacing both the front and the rear module	step <u>k</u>

   b   Remove the front module. (The screws that secure the module in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the modules can be removed.)

   c   Insert the new front module, lock the lock latches on the module and tighten the screws that secure the module in the shelf.

   d   Go to step <u>5</u>.

   e   Disconnect the network interface cables, KVM, SCSI cable, and connections from the rear transition module.

   f   Remove both front and rear modules, <u>in that order</u>. (The screws that secure the modules in the slots must be

loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the modules can be removed.)

g Insert the new rear transition module, lock the lock latches, and tighten the screws that secure the module in the shelf.

h Insert the front module that you removed in step f. Lock the lock latches on the module and tighten the screws that secure the module in the shelf.

i Reconnect the cables disconnected in step e.

j Go to step 5.

k Disconnect the network interface cables, KVM, SCSI cable, and connections from the rear transition module.

l Remove both front and rear modules, in that order. (The screws that secure the modules in the slots must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the modules can be removed.)

m Insert the new rear transition module, lock the lock latches, and tighten the screws that secure the module in the shelf.

n Insert the new front module. Lock the lock latches on the module and tighten the screws that secure the module in the shelf.

o Reconnect the cables disconnected in step k.

5 The node will reboot upon insertion of the modules into the shelf. During the boot process, break into the BIOS menu using function key (F2) and ensure that the BIOS settings match those in the table located in BIOS Settings for CPV5370 SCSI on page 268.

At the Network Elements pane of the Universal Audio Server Manager main screen

6 After the system reboot has completed, applications will automatically restart in the system but the network element will come up in an administrative "locked" state. Using the procedure Changing the Admin state on page 226 set the administrative state for this UAS unit to "unlocked."

The UAS unit informs the gateway controller (GWC) that it is enabled. The GWC then starts sending call requests to the unit.

7 You have completed this procedure.

BIOS Settings for CPV5370 SCSI

This table provides you with the CPV5370 BIOS settings, when you are performing the procedure to replace the CPV5370 card.

Menu	Field or sub-menu	Field or sub-menu	Field or sub-menu	Setting
Main	BIOS Version			CPV5370 v1.0RM01
	Board Version			board specific
	Board Serial Number			board specific
	CPU Type			system specific
	CPU Speed			system specific
	Cache RAM			system specific
	Total Memory			system specific
	System Time			system specific
	System Date			system specific
Memory	Cache RAM			system specific
	Total Memory			system specific
	Memory Bank 0			system specific
	Memory Bank 1			system specific
	Memory Bank 2			system specific
	L2 Cache			ENABLED
	L2 Cache ECC Support			ENABLED
	ECC Memory Config			DISABLED
Advanced	Plug and Play OS			NO

Menu	Field or sub-menu	Field or sub-menu	Field or sub-menu	Setting
	Reset Configuration Data			NO
	Legacy USB Support			DISABLED
	Floppy Configuration	Floppy Controller		ENABLED
		Base I/O Address		PRIMARY
		Diskette A		1.44MB 3.5 inch
		Diskette B		DISABLED
		Floppy Check		ENABLED
	IDE Configuration	Local Bus IDE Adapter		DISABLED
		Large Disk Access Mode		DOS
		Smart Device Monitoring		DISABLED
		Primary Master		NONE
		Primary Slave		NONE
		Secondary Master		NONE
		Secondary Slave		NONE
	I/O Device Configuration	PS/2 Mouse		AUTO DETECT
		Serial Port A:		ENABLED
		Base I/O Address		3F8
		Interrupt		IRQ 4
		Serial Port B:		ENABLED

Menu	Field or sub-menu	Field or sub-menu	Field or sub-menu	Setting
		Base I/O Address		2F8
		Interrupt		IRQ 3
		Parallel Port:		ENABLED
		Mode		BI-DIRECTIONAL
		Base I/O Address		378
		Interrupt		IRQ 7
	PCI Configuration	Default Primary Video Adapter		AGP
		On-card Ethernet 1		ENABLED
		Ethernet 1 Connection		REAR
		Ethernet 1 Option ROM		DISABLED
		On-card Ethernet 2		ENABLED
		Ethernet 2 Connection		REAR
		Ethernet 2 Option ROM		DISABLED
		HA Configuration	HA Config	ENABLED
			DOMAIN A	ENABLED if left side DISABLED if right side
			DOMAIN B	ENABLED if right side DISABLED if left side
		PCI/PNP IRQ CONFIGURATION	IRQ 9	Available

Menu	Field or sub-menu	Field or sub-menu	Field or sub-menu	Setting
			IRQ 11	Available
			PCI IRQ Line 1	10
			PCI IRQ Line 2	10
			PCI IRQ Line 3	10
			PCI IRQ Line 4	10
	REMOTE CONSOLE	Com Port		DISABLED
		BAUD Rate		9600
		Console Type		PC ANSI
		Flow Control		None
		ScreenLines		24
		Active After Post		OFF
	EMBEDDED FLASH	Status		Select source and load
		Task		Save BIOS
		Device		Diskette Drive
		File		BIOS.ROM
		Execute		ENTER
Security	Supervisor Password is:			CLEAR
	USER Password is:			CLEAR
	Clear All Passwords			ENTER

Menu	Field or sub-menu	Field or sub-menu	Field or sub-menu	Setting
	Set Supervisor Password			ENTER
	Set User Password			ENTER
	Password on Boot			DISABLED
	Fixed Disk Boot Sector			NORMAL
	Diskette Access			SUPERVISOR
Boot	Quick Boot			ENABLED
	Summary Screen			DISABLED
	Setup Prompt			ENABLED
	Numlock			AUTO
	Boot Retry			DISABLED
	Jump To Flash			DISABLED
	Boot Device Priority	Removable Devices		
		8XX SCSI CD-ROM LSI LOGIC		
		Hard Drive		
		Legacy Network Boot		
		ATAPI CD-ROM Drive		

Replacing a Hot Swap Controller card

This procedure enables you to replace a Hot Swap Controller card.

Replacing a Hot Swap Controller card

⚠	**WARNING** **Static electricity damage** While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

⚠	**CAUTION** **Possible equipment damage** Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

At the Network Elements pane of the Universal Audio Server Manager main screen

1   Using the procedure Changing the Admin state on page 226, set the administrative state for this UAS unit being serviced to "lock graceful."

The selected UAS unit informs the gateway controller (GWC) that it is disabled. The GWC stops sending call requests to this UAS unit.

At the Windows desktop interface

2 Stop any applications that are running.

a Access the "Services" window as follows:

select **Start -> Programs -> Administrative Tools -> Services**

b Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

3 Shut down the system:

select **Start -> Shut Down**

a On the Shut Down Windows screen, select "Shut down this computer." When the shutdown is complete and the system displays the message indicating that it is safe to turn off the computer, do not turn off power to the computer.

4 Locate the Hot Swap Controller card. The Hot Swap Controller cards reside in the domain of the chassis opposite from the domain that they control. Thus, the Hot Swap Controller for the left domain resides in slot 10; the Hot Swap Controller for the right domain resides in slot 8.

a Remove the Hot Swap Controller card. (The screws that secure the card in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the card can be removed.)

Note: There is no rear transition module for this card.

b Insert the new Hot Swap Controller card. (After the new card has been inserted into the card slot, lock the lock latches, and tighten the screws that secure the card in the shelf.) The node will reboot automatically upon insertion of the new card.

At the Network Elements pane of the Universal Audio Server Manager main screen

5 After the system reboot has completed, applications will automatically restart in the system but the network element will come up in an administrative "locked" state. Using the procedure Changing the Admin state on page 226 set the administrative state for this UAS unit to "unlocked."

The UAS unit informs the gateway controller (GWC) that it is enabled. The GWC then starts sending call requests to the unit.

6 You have completed this procedure.

Replacing a BX4000c (S007) ATM interface card

This procedure enables you to replace a BX4000c (S007) ATM interface card.

Replacing a BX4000c (S007) ATM interface card

⚡	**WARNING** **Static electricity damage** While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

✋	**DANGER** **Laser radiation exposure** The exposed ends of fiber optic cables can emit harmful laser radiation. Do not look at the ends of fiber optic cables unless protector caps are in place. Disconnect all laser sources when personnel are working with fiber-optic cables.

⚠	**CAUTION** **Possible equipment damage** Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

At the Network Elements pane of the Universal Audio Server Manager main screen

1   Using the procedure <u>Changing the Admin state on page 226</u>, set the administrative state for this UAS unit being serviced to "lock graceful."

The selected UAS unit informs the gateway controller (GWC) that it is disabled. <u>The GWC stops sending call requests to this UAS unit.</u>

At the Windows desktop interface

2   Stop any applications that are running.

    a   Access the "Services" window as follows:

       select **Start -> Programs -> Administrative Tools -> Services**

    b   Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

3   Shut down the system:

    select **Start -> Shut Down**

    a   On the Shut Down Windows screen, select "Shut down this computer." When the shutdown is complete and the system displays the message indicating that it is safe to turn off the computer, do <u>not</u> turn off power to the computer.

4   Locate the BX4000c card. If the UAS node is located on the left side of the shelf, the card will be in slot 5; if the node is located on the right side of the shelf, the card will be in slot 12.

    a   Disconnect the OC3c interface cable from the BX4000c card. After the cable has been removed, cap the connectors on the card and on the fiber cable.

    b   Remove the BX4000c card. (The screws that secure the card in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the card can be removed.)

       Note: There is no rear transition module for this card.

    c   Insert the new BX4000c card. (After the new card has been inserted into the card slot, lock the lock latches, and tighten the screws that secure the card in the shelf.)

    d   Remove the protective caps from the connectors on the new card and on the fiber cable. Connect the OC3c interface cable to the BX4000c card.

e   To effect the changes you have made, reset the system.

If	Do
you have a peer domain within the chassis, that has Global Server software installed on it	step f
you do not have a peer domain within the chassis	step i

f   From the local KVM interface (system console), toggle/switch to the UAS domain that is the peer to the domain containing the card that was just replaced, by either

•   pressing the RED -/+ buttons on the KVM switch

or

•   pressing and releasing the <Ctrl> key followed by <Esc>

to bring up a list of the UAS nodes/domains on the overlay, from which (by using the arrow keys and pressing <Enter>) the domain can be chosen.

g   Perform the following step to cause the reset of the inaccessible mate UAS processor:

select **Start -> Run**

In the Run Dialog window that displays, type **domainreset** and then click OK.

> *Note:* The peer UAS domain must have Global Server software installed on it in order for this command to be used.

h   Go to step 5.

i   Unseat the CPV5350 Processor card associated with the domain being serviced and reseat the card in its slot. The CPV5350 card is located in slot 7 for the left domain and in slot 9 for the right domain. (The screws that secure the card in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the card can be removed. After the card is reseated in the slot, lock the lock latches, and tighten the screws that secure the card in the shelf.)

At the Network Elements pane of the Universal Audio Server Manager main screen

5   After the system reboot has completed, applications will automatically restart in the system but the network element will come up in an administrative "locked" state. Using the procedure

set the administrative state for this UAS unit to "unlocked."

The UAS unit informs the gateway controller (GWC) that it is enabled. The GWC then starts sending call requests to the unit.

6 You have completed this procedure.

Replacing a PA200 card

This procedure enables you to replace a PA200 ATM interface card.

Replacing a PA200 ATM interface card

⚠	**WARNING** **Static electricity damage** While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

✋	**DANGER** **Laser radiation exposure** The exposed ends of fiber optic cables can emit harmful laser radiation. Do not look at the ends of fiber optic cables unless protector caps are in place. Disconnect all laser sources when personnel are working with fiber-optic cables.

⚠	**CAUTION** **Possible equipment damage** Use care when inserting and removing cards from the SAM16 shelf. Ensure that the spiral gasket, located on the edge of the card faceplate, is not loose so that it can become caught on an adjacent card and be pulled off. A loose spiral gasket has the potential to make contact with the backplane inside the chassis, possibly causing damage or service outage due to electrical short circuit.

At the Network Elements pane of the Universal Audio Server Manager main screen

1   Using the procedure Changing the Admin state on page 226, set the administrative state for this UAS unit being serviced to "lock graceful."

The selected UAS unit informs the gateway controller (GWC) that it is disabled. The GWC stops sending call requests to this UAS unit.

At the Windows desktop interface

2   Stop any applications that are running.

   a   Access the "Services" window as follows:

      select **Start -> Programs -> Administrative Tools -> Services**

   b   Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

3   Shut down the system:

   select **Start -> Shut Down**

   a   On the Shut Down Windows screen, select "Shut down this computer." When the shutdown is complete and the system displays the message indicating that it is safe to turn off the computer, do not turn off power to the computer.

4   Locate the PA200 module. If the UAS node is located on the left side of the shelf, the module will be in slot 6; if the node is located on the right side of the shelf, the module will be in slot 11.

   a   Determine whether you are replacing only the front module, replacing only the rear module, or replacing both the front and the rear modules.

If	Do
you are replacing only the front module	step b
you are replacing only the rear module	step e
you are replacing both the front and the rear module	step k

   b   Remove the front module. (The screws that secure the module in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the module can be removed.)

c Insert the new front module, lock the lock latches on the module and tighten the screws that secure the module in the shelf.

d Go to step 5.

e Disconnect the OC3c interface cable from the rear module. After the cable has been removed, cap the connectors on the module and on the fiber cable.

f Remove both front and rear modules, in that order. (The screws that secure the modules in the slots must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the modules can be removed.)

g Insert the new rear transition module, lock the lock latches, and tighten the screws that secure the module in the shelf.

h Insert the front module that you removed in step f. Lock the lock latches on the module and tighten the screws that secure the module in the shelf.

i Remove the protective caps from the connectors on the new rear module and on the fiber cable. Connect the OC3c interface cable to the rear module.

j Go to step 5.

k Disconnect the OC3c interface cable from the rear module. After the cable has been removed, cap the connectors on the module and on the fiber cable.

l Remove both front and rear modules, in that order. (The screws that secure the modules in the slots must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the modules can be removed.)

m Insert the new rear transition module, lock the lock latches, and tighten the screws that secure the module in the shelf.

n Insert the new front module. Lock the lock latches on the module and tighten the screws that secure the module in the shelf.

o Remove the protective caps from the connectors on the new rear module and on the fiber cable. Connect the OC3c interface cable to the module.

5   To effect the changes you have made, reset the system.

If	Do
you have a peer domain within the chassis, that has Global Server software installed on it	step 6
you do not have a peer domain within the chassis	step 8

6   Perform the following step to reset the inaccessible mate UAS processor:

select **Start -> Run**

In the Run Dialog window that displays, type **domainreset** and then click OK.

>   *Note:* The peer UAS domain must have Global Server software installed on it in order for this command to be used.

7   Go to step 9.

8   Unseat the CPV5370 Processor card associated with the domain being serviced and reseat the card in its slot. The CPV5370 card is located in slot 7 for the left domain and in slot 9 for the right domain. (The screws that secure the card in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the card can be removed. After the card is reseated in the slot, lock the lock latches, and tighten the screws that secure the card in the shelf.)

At the Network Elements pane of the Universal Audio Server Manager main screen

9   After the system reboot has completed, applications will automatically restart in the system but the network element will come up in an administrative "locked" state. Using the procedure Changing the Admin state on page 226 set the administrative state for this UAS unit to "unlocked."

The UAS unit informs the gateway controller (GWC) that it is enabled. The GWC then starts sending call requests to the unit.

10   You have completed this procedure.

Replacing a UAS disk drive

This procedure enables you to replace a UAS system disk drive.

Replacing a UAS disk drive

	WARNING **Static electricity damage** While handling circuit cards or cables, wear a wrist strap connected to the wrist-strap grounding point on the frame. This protects the cards against damage caused by static electricity.

At the Network Elements pane of the Universal Audio Server Manager main screen

1   Using the procedure <u>Changing the Admin state on page 226</u>, set the administrative state for this UAS unit being serviced to "lock graceful."

The selected UAS unit informs the gateway controller (GWC) that it is disabled. <u>The GWC stops sending call requests to this UAS unit.</u>

At the Windows desktop interface

2   Stop any applications that are running.

    a   Access the "Services" window as follows:

        select **Start -> Programs -> Administrative Tools -> Services**

    b   Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

3   Shut down the system:

    select **Start -> Shut Down**

    a   On the Shut Down Windows screen, select "Shut down this computer." When the shutdown is complete and the system displays the message indicating that it is safe to turn off the computer, do <u>not</u> turn off power to the computer.

4   Replace the disk drive by performing the following steps:

    a   The key on the disk drive is spring-loaded. Press the key on the disk drive and, while the key is pressed in, turn the key

counter-clockwise to its stopping point (approximately one-quarter turn).

b   Remove the drive from the slot.

c   Insert the new drive into the slot.

Note: Ensure that the replacement disk drive is ready for operation, that is, it contains the latest software load.

d   Turn the key on the disk drive clockwise to its vertical position (approximately one-quarter turn). Ensure that the key has popped out into the locked position, that is, you can't turn the key.

5   To complete the installation of the new disk, reset the system.

If	Do
you have a peer domain within the chassis, that has Global Server software installed on it	step 6
you do not have a peer domain within the chassis	step 9

6   From the local KVM interface (system console), toggle/switch to the UAS domain that is the peer to the domain containing the card that was just replaced, by either

•   pressing the RED -/+ buttons on the KVM switch

or

•   pressing and releasing the <Ctrl> key followed by <Esc>

to bring up a list of the UAS nodes/domains on the overlay, from which (by using the arrow keys and pressing <Enter>) the domain can be chosen.

7   Perform the following step to cause the reset of the inaccessible mate UAS processor:

`Start -> Run`

In the Run Dialog window that displays, type **domainreset** and then click OK.

Note: The peer UAS domain must have Global Server software installed on it in order for this command to be used.

8   Go to step 10.

9   Unseat the CPV5370 or CPV5350 Processor card associated with the domain containing the disk being serviced and reseat the card in its slot. The CPV5370 or CPV5350 card is located in slot 7 for the left domain and in slot 9 for the right domain. (The

screws that secure the card in the slot must be loosened with a Phillips head screwdriver, and the lock latches must be unlocked, before the card can be removed. After the card is reseated in the slot, lock the lock latches, and tighten the screws that secure the card in the shelf.)

At the Network Elements pane of the Universal Audio Server Manager main screen

10 <u>After the network element has restarted (that is, the network element appears in the Network Elements pane)</u>, set the administrative state for this UAS unit to "unlocked" by performing the procedure Changing the Admin state on page 226.

The UAS unit informs the gateway controller (GWC) that it is enabled. The GWC then starts sending call requests to the unit.

11 You have completed this procedure.

Restoring UAS configuration files

At the time of installation, the UAS is configured to automatically back up configuration files each day at 2:00 am. If an APS node is configured in the network, all UAS nodes in the network can be backed up to the APS node. If an APS node is not configured in the network, the configuration files for UAS nodes in the network can be backed up, instead, to a remote UNIX server.

The backed-up files can be restored should a catastrophic system event, such as a hard disk drive failure, create the need for a re-installation. The files are restored by manually transferring the files from the APS node or remote UNIX server to the UAS node after the UAS software (and NGS software, if necessary) has been re-installed. The backed-up files are located in the directory, /opt/uas/uas_conf_backup and include:

- C:\UAS\etc\UAS.conf (all configurations)
- C:\UAS\etc\ugw.conf (for a PRI gateway only)
- C:\UAS\etc\atmconn.con (ATM only)
- C:\UAS\etc\mainsa.conf (all configurations)
- C:\UAS\etc\atmhard.con (ATM only)
- C:\etc\srconf\agt\snmpd.cnf (all configurations)
- C:\Winnt\system32\drivers\etc\hosts (all configurations)
- C:\UAS\etc\atmSvcProfile.con (ATM only)
- C:\UAS\etc\atmhardloop.con (ATM only)

This procedure enables you to restore backed-up UAS configuration files that are stored either on an APS node or on a remote UNIX server.

Restoring UAS configuration files

At the Network Element Status panel of the Universal Audio Server Manager

1   In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

2   In the pull-down list in the box labeled, "Please select," select Maintenance.

3   In the Maintenance Tree pane, select "Node".

4 Click the node entry that displays in the table shown in the Node States pane.

5 Lock the node by clicking the "Lock Graceful" button located at the bottom of the Node States pane.

At the Windows desktop interface

6 Log in as Administrator.

7 Stop any applications that are running.

a Access the "Services" window as follows:

select **Start -> Programs -> Administrative Tools -> Services**

b Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.

8 Perform the following steps:

a Enter the following command:

`cd \UAS\etc`

b Access the APS server directory containing the backed up configuration files by entering the following:

`mount * \\<APS IP address>\opt\uas\uas_conf_backup\<UAS node>\current` (all of this command is entered on one line)

where <APS IP address> is the address of the server containing the backed up configuration files, and <UAS node> is the <u>full directory path</u> that contains the name of the UAS node that you are restoring the backed up configuration files to.

c Execute the following command to confirm that the directory containing the backed-up configuration files is mounted:

`net use`

d Change directories to the location of the newly mounted configuration file backup directory by entering the following:

`cd <mounted drive letter>`

where <mounted drive letter> is the drive letter (for example, "F") displayed as the result of the previous command.

e List the contents of the configuration file backup directory by entering the following command in response to the prompt:

`ls -l`

The following backed up files should display:

- UAS.conf (for all configurations)
- ugw.conf (for a PRI gateway only)
- atmconn.con (for ATM only)
- mainsa.conf (for all configurations)
- atmhard.con (for ATM only)
- snmpd.cnf (for all configurations)
- hosts (for all configurations)
- atmSvcProfile.con (for ATM only)
- atmhardloop.con (for ATM only)

f Enter the following command to copy the contents of the mounted configuration file backup directory to the appropriate subdirectory on your UAS:

```
copy *.* c:\UAS\etc\
```

g Unmount the configuration file backup directory by entering the following command:

```
umount <drive letter>
```

where <drive letter> is the drive letter that you entered in step d.

h At the system console, perform the following steps:

```
mv snmpd.cnf \etc\srconf\agt\snmpd.cnf
```

```
mv hosts \Winnt\system32\drivers\etc\hosts
```

9 Restart the network element by performing the following steps:

a Access the "Services" window as follows:

select **Start -> Programs -> Administrative Tools -> Services**

b Right-click PMGRdaemon service and select Start.

At the Network Element Status panel of the Universal Audio Server Manager

10 In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

11 In the pull-down list in the box labeled, "Please select," select Maintenance.

12   In the Maintenance Tree pane, select "Node".

13   Click the node entry that displays in the table shown in the Node States pane.

14   Unlock the node by clicking the "Unlock" button located at the bottom of the Node States pane.

15   You have completed this procedure.

APS troubleshooting guide

The procedures that you perform to address operational issues pertaining to the APS are determined by system problem indicators that you encounter, such as an alarm or log, by the inability to perform a procedure, or audio being unavailable after it has been provisioned. The following table contains the most common indicators of system problems and the recommended troubleshooting procedure(s) to perform in response, in order to diagnose and solve the problems.

APS troubleshooting guide (Sheet 1 of 2)

Trouble Indicator	Procedure to perform
Cannot get audio to the UAS from the APS	Trouble-shooting the APS provisioner on page 292
Audio on the UAS sounds distorted.	The UAS only supports audio in G.711 a-law or mu-law format, sampled at 8Khz. Other formats, such as "wave" or "mp3," cannot be played on the UAS, although the APS does support provisioning of audio in these formats in the event that a gateway receiving exported audio from the APS does support the formats. The APS application does not examine audio files when they are uploaded and imported into the APS database. Therefore, ensure that the correct format has been selected in the audio file import dialog in the APS GUI (Procedure, "Importing Physical Segments", in the document NN10095-511, entitled "UAS Configuration Management"). Also ensure that the audio has the correct sampling rate.
APS system parameter changes have not been activated	To effect APS system parameter changes made through the APS Administration GUI, the following command must be entered at the system console after the changes have been made: /opt/uas/aps/scripts/killDbServer.sh

APS troubleshooting guide (Sheet 2 of 2)

Trouble Indicator	Procedure to perform
Cannot log in to the APS	<u>Troubleshooting APS login problems on page 298</u>
Cannot create a new APS Administration GUI user account	In a Telnet connection to the APS server, log in as the "root" user and perform the following commands: 1. cd /user_audio_files 2. ls -l 3. In the listing, look for the directory with the same name as the user ID being created. After you are sure that the directory exists, enter the following command to remove the directory: rmdir <user ID> 4. Log in to the APS Administration GUI and add the user again.

Trouble-shooting the APS provisioner

The following procedures enable you to trouble-shoot the APS provisioner that has stopped for some unknown reason.

Trouble-shooting the APS provisioner

In a telnet connection to the APS server

1 Open an xterm window and log in using the "maint" login and password.

2 Become the "root" user by entering:

```
su - root
```

3 Locate the provisioner log file in the /PROV_data directory by performing the following step:

```
ls -l -t | more
```

A list of files in the directory displays.

4 Display the contents of the _provisioner.log file by entering the following command:

```
view <hostname>_provisioner.log
```

The latest provisioning log data displays at the bottom of the file listing. Look in this data for references to the UAS node to which audio provisioning was attempted. If you discover one of the log messages shown in the list below, perform the error recovery steps that accompany the log message in this list:

Message: Provisioner stop on <hostname> at <time> because node <UASnode> is not provisionable.

Cause: The UAS may not have a provision set or provisioning of the UAS is not enabled.
Action:
- To create a provisioning set for the UAS, perform the procedure "Creating a Provisioning Set" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite.
- To enable provisioning on the UAS, perform the procedure "Enabling provisioning of a UAS node" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite.

Message: Provisioner stop on <hostname> at <time> because a full provisioner process is already running.

Cause: Two full provisioner processes cannot run simultaneously.
Action:
- Perform the procedure Removing provisioner lock files on page 296. You may then wish to see if your provisioning process is running by performing the procedure Checking for active audio provisioner processes on page 297. Note, however, that if the full provisioning process is running, any associated lock files will be removed only when the full provisioner completes. A full provisioner process starts automatically each hour.

Message: Provisioner stop on <hostname> at <time> because the /PROV_data file system is 100% full.

Action:
Remove un-needed files or user files from the /PROV_data directory. Contact your next level of support or your Nortel Networks service representative for assistance.

Message: Provisioner stop on <hostname> at <time> because the db is not accessible.

Cause: The Oracle database may be down.

Action:
Perform the procedure "Checking the APS Oracle database" in the document, NN10161-611, entitled "UAS Administration and Security," in your UAS document suite.

Message: Provisioner stop on <hostname> at <time> because node <UAS_node> is not provisionable.

Action:
Make the UAS node provisionable by associating a provisioning set with it and by then ensuring that provisioning on the node is enabled:
- To create a provisioning set for the UAS, perform the procedure "Creating a provision set" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite
- To enable provisioning on the UAS, perform the procedure "Enabling provisioning of a UAS node" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite

Message: Problems creating files for node <UAS_node) on host <hostname>

Cause: The APS had problems creating the transaction files in the /PROV_data/<UAS_node> directory.

Action:
In a telnet connection to the APS server, open an x-term window and ensure that the <UAS_node> directory exists in the /PROV_data directory:
  1. cd /PROV_data
  2. ls -l
- If the directory exists, ensure that the directory permissions allow writing to the directory.
- If the directory does not exist:
  1. delete the UAS node in question by performing the procedure "Deleting a UAS node" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite
  2. add the node back by performing the procedure "Creating a UAS node" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite
  3. add the provision set to the node by performing the procedure "Adding a provision set to a UAS node" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite
  4. enable provisioning on the node by performing the procedure "Enabling provisioning of a UAS node" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite
  5. provision the node by performing the procedure "Provisioning a UAS node" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite

Message: Problems transferring files for node <UASnode> from <hostname>

<u>Cause:</u> There are, generally, two causes for this condition: 1) call processing is not active on the UAS node; 2) the incorrect APS hostname and IP address are defined on the UAS.

<u>Action:</u>
- To restart call processing on a UAS node, perform the procedure <u>Restarting a UAS through the Universal Audio Server Manager on page 221</u>.
- To redefine the APS hostname and IP address on the UAS node, perform the procedure "Modifying configuration parameters through the Universal Audio Server Manager" or the procedure "Modifying configuration parameters through the Local Configuration Interface GUI", in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite.

5   You have completed this procedure.

Removing provisioner lock files

This procedure enables you to use the killProvJob.ksh tool to remove non-active provisioner lock files on the file system that prevent new provisioner processes from running.

Removing provisioner lock files

In a telnet connection to the APS server

1   Open an xterm window and log in using the "maint" login and password.

2   Become the "root" user by entering:

su - root

3   Enter the following command to remove any provisioner lock files that are preventing a new provisioner process from running:

killProvJob.ksh -cleanup

A status display informs you about the progress of the lock file removal.

4   Enter the following command to determine whether the hourly provisioner is scheduled to run:

killProvJob.ksh -autostatus

The system indicates whether the hourly provisioner is scheduled to run.

If	Do
the hourly provisioner is scheduled to run	step 5
the hourly provisioner is not scheduled to run	Contact your next level of support or your Nortel Networks service representative for assistance.

5   You have completed this procedure.

Checking for active audio provisioner processes

This procedure enables you to determine whether any audio provisioning processes are currently active.

Checking for active audio provisioner processes

In a telnet connection to the APS server

1   Open an xterm window and log in using the "maint" login and password.

2   Become the "root" user by entering:

`su - root`

3   Enter the following command to determine whether any provisioning processes are currently active:

`killProvJob.ksh -status`

The system indicates whether an audio provisioning process is currently running.

4   You have completed this procedure.

Troubleshooting APS login problems

This procedure enables you to identify and solve the following common problems that prevent you from logging in to the APS:

- URL in the browser address window is incorrect
- keyboard "Caps Lock" is on
- Oracle database is down
- web server is not running
- APS application software was removed or is not installed

Troubleshooting APS login problems

At your console

1   Verify that the URL in your browser address window is correct. The URL will be of the format: http://*<hostname or IP address of the APS>*:8080/aps/

If	Do
the URL is correct	step 3
the URL is incorrect	Correct the URL entry in the browser. Go to step 2

2   Try to log in to the APS.

If	Do
you are able to log in to the APS	step 28
you are unable to log in to the APS	step 3

3   Ensure that "Caps Lock" is not enabled on your keyboard.

If	Do
"Caps Lock" is enabled	Press the "Caps Lock" key on your keyboard. Go to step 4
"Caps Lock" is not enabled	step 5

4   Try to log in to the APS.

If	Do
you are able to log in to the APS	step 28
you are unable to log in to the APS	step 5

In a telnet connection to the APS server

5   Open an xterm window and log in using the "maint" login and password.

6   Become the "root" user by entering:

     `su - root`

7   Determine whether the APS login page is accessible.

If	Do
the APS login page is accessible	step 8
the APS login page is not accessible	step 19

8   Ensure that the Oracle database is online by entering the following command:

     `/opt/servman/bin/servman query -status -g DATABASE -v`

     The display will indicate that the Oracle processes, listed at the end of the display (that is, entries in the display that begin with "oracle <pid>"), are running.

If	Do
the displayed Oracle processes are not running	step 9
the displayed Oracle processes are running	step 13

9   Restart the Oracle database by entering the following command:

     `/opt/servman/bin/servstart DATABASE`

10   Kill the APS server process and let the server restart automatically, by entering the following command:

     `/opt/uas/aps/scripts/killDbServer.sh`

     A message eventually displays indicating that the server is restarting.

11   Enter the following command to check the status of the database:

     `/opt/servman/bin/servman query -status -g DATABASE -v`

The display will indicate that the Oracle processes, listed at the end of the display (that is, entries in the display that begin with "oracle <pid>"), are running.

If	Do
the displayed Oracle processes are running	step 12
the displayed Oracle processes are not running	step 27

12   Try to log in to the APS.

If	Do
you are able to log in to the APS	step 28
you are unable to log in to the APS	step 13

13   Ensure that you can connect to the Oracle database by entering the following command:

`sql`

An "sql" prompt will display.

If	Do
the sql prompt does not display	step 14
the sql prompt does display	step 26

14   Determine whether you already restarted the Oracle database once before during this procedure.

If	Do
you have already restarted the database once before	step 27
you have not already restarted the database once before	step 15

15   Restart the Oracle database by entering the following command:

`/opt/servman/bin/servstart DATABASE`

16   Kill the APS server process and let the server restart automatically, by entering the following command:

`/opt/uas/aps/scripts/killDbServer.sh`

A message eventually displays indicating that the server is restarting. This may take from 2 to 5 minutes.

17   Enter the following command to check the status of the database:

```
/opt/servman/bin/servman query -status -g
DATABASE -v
```

The display will indicate that the Oracle processes, listed at the end of the display (that is, entries in the display that begin with "oracle <pid>"), are running.

If	Do
the displayed Oracle processes are running	step 18
the displayed Oracle processes are not running	step 27

18   Try to log in to the APS.

If	Do
you are able to log in to the APS	step 28
you are unable to log in to the APS	step 27

19   If the correct IP address of the APS server is entered in the browser address window, but the login page is not accessible, an Application Launch Point page will display.

If	Do
the Application Launch Point page displays	step 21
the Application Launch Point page does not display	step 20

20   Enter the following command to start the Apache server:

```
/opt/servman/bin/servstart WEBSERVICES
```

Messages that indicate the Apache server has started display.

21   Verify that the APS software packages have been installed by entering the following command:

```
pkginfo | grep aps
```

If	Do
a list of the required APS software packages displays	step 22
a list of the required APS software packages does not display	You will need to install the required APS packages. Go to step 27.

22 Enter the following command to check the status of the database:

`/opt/servman/bin/servman query -status -g DATABASE -v`

The display will indicate that the Oracle processes, listed at the end of the display (that is, entries in the display that begin with "oracle <pid>"), are running.

If	Do
the displayed Oracle processes are running	step 26
the displayed Oracle processes are not running	step 23

23 Restart the Oracle database by entering the following command:

`/opt/servman/bin/servstart DATABASE`

24 Kill the APS server process and let the server restart automatically, by entering the following command:

`/opt/uas/aps/scripts/killDbServer.sh`

A message eventually displays indicating that the server is restarting. This may take from 2 to 5 minutes.

25 Enter the following command to check the status of the database:

`/opt/servman/bin/servman query -status -g DATABASE -v`

The display will indicate that the Oracle processes, listed at the end of the display (that is, entries in the display that begin with "oracle <pid>"), are running.

If	Do
the displayed Oracle processes are running	step 26
the displayed Oracle processes are not running	step 27

26 Try to log in to the APS.

If	Do
you are able to log in to the APS	step 28
you are unable to log in to the APS	It may be necessary to reboot the server. Go to step 27.

27   Contact your next level of support.

28   You have completed this procedure.

Starting the APS Oracle database

The Oracle database contains information about the APS audio and about the nodes to which the APS can provision audio. This procedure enables you to restart the Oracle database as part of APS system recovery.

Starting the APS Oracle database

In a telnet connection to the APS server

1   Open an xterm window and log in using the "maint" login and password.

2   Become the "root" user by entering:

`su - root`

3   Start the Oracle database by entering the following command:

`/opt/servman/bin/servstart DATABASE`

4   Kill the APS server process and let the server restart automatically, by entering the following command:

`/opt/uas/aps/scripts/killDbServer.sh`

A message eventually displays indicating that the server is restarting.

5   Enter the following command to check the status:

`/opt/servman/bin/servman query -status -g`
`DATABASE -v`

The display should indicate that the Oracle processes, listed at the end of the display (that is, entries in the display that begin with "oracle <pid>"), are running. If the processes are not running, contact your next level of support.

6   You have completed this procedure.

Restoring audio files to a UAS node

In the event that a re-installation of a UAS node is required due to an error condition, audio files must be restored to the unit when it becomes operational. This procedure allows you to enable audio provisioning to the node and to specify which audio files are to be restored to it.

Note: For more information about re-installation of a UAS node, contact your Nortel Networks service representative.

Restoring audio files to a UAS node

At your web browser interface

1   After the re-installation of the UAS node has been completed, determine whether you want to enable provisioning of the node occur during the next audio distribution cycle or immediately.

If	Do
you want to enable provisioning of the node to occur during the next audio distribution cycle	step 2
you want audio provisioning of the node to occur immediately	step 3

2   Perform the procedure "Enabling provisioning of a UAS node" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite.

Note: Provisioning of the node will begin during the next audio distribution cycle. The distribution cycle occurs once per hour.

a   Go to step 4.

3   Perform the procedure "Provisioning a UAS node" in the document, NN10095-511, entitled "UAS Configuration Management," in your UAS document suite.

Note: Provisioning of the node will begin immediately although as much as a five-minute delay may occur before actual provisioning activity begins.

4   You have completed this procedure.

Rebooting an APS

This procedure enables you to reboot an APS, as part of APS system recovery.

Rebooting an APS

In a telnet connection to the APS server

1   Open an xterm window and log in using the "maint" login and password.

2   Become the "root" user by entering:

`su - root`

3   Enter the following command to stop the Oracle database:

`db_stop.sh`

4   Enter the following command:

`shutdown -i 6 -y`

5   You have completed this procedure.