Carrier VoIP

Media Server 2000 Series Fault Management

NN10328-911

Document status: Standard
Document version: 05.02
Document date: 20 October 2006

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

Contents

New in this release

The following sections detail what's new in *Media Server 2000 Series Fault Management* (NN10328-911) for release (I)SN09U.

Feature changes

There are no feature changes in this release.

Other changes

See the following sections for information about changes that are not feature-related.

Additional alarm information and log reference added

Additional alarm information has been added to the "APS alarms" (page 21) section. A reference to the *Carrier Voice over IP Fault Management Logs Reference* Volume 3 (NN10275-909) has been added to the "APS logs" (page 24) and Media Server 2000 Series "Customer Logs" (page 11) sections.

IP-1610 cPCI Board and TP-6310 Board troubleshooting guides added

IP-1610 cPCI Board troubleshooting procedures have been added in the "IPM-1610 cPCI Board troubleshooting guide" (page 59) section. TP-6310 Board troubleshooting procedures have been added in the "TP-6310 Board troubleshooting guide" (page 63) section.

Fault management

Use the information in this section to learn about the Media Server 2000 Series fault management.

Media Server 2000 Series fault reporting

This NTP contains the fault management procedures used to maintain and monitor the Nortel Networks Media Server 2000 Series and the Audio Provisioning Server (APS).

Media Server 2000 Series fault reporting is based on Simple Network Management Protocol (SNMP). The Media Server 2000 Series carrier-grade alarm system provides a reliable alarm reporting mechanism that takes into account element manager outages, network outages, and an unreliable transport mechanism (SNMP over UDP). A carrier-grade alarm system is characterized by the following capabilities:

- a mechanism to allow an EM to determine which alarms are currently active in the NE. (The NE maintains an active alarm table.)
- a mechanism to allow an EM to detect lost alarm raise and clear notifications. [seq no in trap, current seq no mib object]
- a mechanism to allow an EM to recover lost alarm raise and clear notifications [keep a log history]
- the ability to send a cold start trap to indicate that it is starting. This allows the EM to synchronize its view of the NE's active alarms.
- clear alarms before shutting down if possible.

Both a listing of active alarms and a history of alarm are maintained on the Media Server 2000 Series servers using the standard NOTIFICATION-LOG-MIB and draft of the ALARM-MIB for the alarm history and active alarms.

The source for these traps is a proprietary enterprise SNMP MIB for the 2000 Series, called "AcBoard". Traps are generated off the Trunk Pack Modules (TPMs). Either TPM for the Media Server 2010 can generate traps. In the case of the Media Server 2020, there is only one TPM.

Alarms

The alarms (and trap names) listed in the following table are sent from the Media Server 2000 series. The traps are received and processed by the IEMS system in the network.

Note: The Media Server 2000 server must be added to IEMS for monitoring and management.

Media Server 2000 Series Alarms and Logs

Alarm/Trap	Description	Log
Active Alarm Table Overflow (acActiveAlarmTableOverflow)	During each development cycle, the size of the active alarm table that will hold all possible alarms that can be raised at any one time by the board This alarm will only be seen if there is an error in that calculation. The status stays major until reboot, because it denotes a possible loss of information until the next reboot. ***Note:*** If an alarm was raised when the table was full, it is possible that the alarm is active, but does not appear in the active alarm table.	AMS 309
Admin State Change (acgwAdminStateChange)	The administration state of the Media Server 2000 Series node changed either to "locked", "shutting down", or "unlocked". A Media Server 2000 Series node can be locked gracefully, allowing existing calls to complete, before administration (configuration and maintenance) is performed on the node. The Media Server 2000 Series also supports a forced lock which immediately takes down active calls. In both types of locks, the administrative state changes to critical for either a "shutting down" or "locked" state and clears when it transitions to an unlocked state.	AMS 501
ATM Port Alarm (acAtmPortAlarm)	This is applicable for the Media Server 2020 and indicates an ATM port error. The status stays critical until the problem is resolved and a reboot occurs.	AMS 310

Alarm/Trap	Description	Log
Audio Provisioning Alarm (acAudioProvisioningAlarm)	Audio provisioning alarm trap is sent when the Media Server times out waiting for audio provisioning from the audio provisioning server. A clear alarm trap is sent when a successful audio provisioning session occurs.	AMS 311
Board Call Resource Alarm (acBoardCallResourceAlarm)	This alarm is raised only in SIP/H.323- based gateway products as a major alarm.	AMS 305
Configuration Error (acBoardConfigurationError)	There is an error in the current configuration for the Media Server 2000 Series node. There is no corresponding clear SNMP trap. The status stays critical until a reboot.	AMS 302
Board Controller Failure Alarm (acBoardControllerFailureAlarm)	This alarm is raised only in SIP/H.323-based gateway products as a minor alarm.	AMS 306
Board Ethernet Link Alarm (acBoardEthernetLinkAlarm)	This alarm trap is received when there is a fault on one of the ethernet links which has an alarm status of "major". If there is a fault on both interfaces the alarm status is critical and the server is isolated. When both link interfaces are restored, an SNMP alarm clear trap is sent and the alarm is cleared.	AMS 307
Resetting Board (acBoardEvResettingBoard)	The IPM-1610 or TP-6310 board was reset. There is no corresponding clear SNMP trap. The status stays critical until a reboot and a board started trap occurs.	AMS 300

Alarm/Trap	Description	Log
Board Started (acBoardEvBoardStarted)	The IPM-1610 or TP-6310 board was restarted. There is no corresponding clear SNMP trap. This is not an alarm and does not go in the active alarm table. This trap is a signal to clear the entire active alarm table.	AMS 500
Fatal Error (acBoardFatalError)	The IPM-1610 or TP-6310 board has an unrecoverable runtime error. There is no corresponding clear SNMP trap. The status stays critical until a reboot.	AMS 301
Board Overload Alarm (acBoardOverloadAlarm)	This alarm is raised only in SIP/H.323- based gateway products as a major alarm.	AMS 308
Temperature Alarm (acBoardTemperatureAlarm)	The Media Server 2000 Series node has a higher than normal temperature condition. This alarm trap is sent from the server when the temperature is above 60 degrees C (140 degrees F). The status stays critical until a corresponding alarm clear is sent when the temperature falls below 55 degrees C (131 degrees F).	AMS 303
Feature Key Error (acFeatureKeyError)	The use of a service (such as conferencing, voice prompts) was attempted but a feature key allowing use of the service was not found.	AMS 304
Enhanced BIT Status (acEnhancedBITStatus)	Contains status of board hardware elements being tested. The board and status appear in the additional info fields.	AMS 600
NAT Traversal Alarm (acNATTraversalAlarm)	The NAT placed in front of a device has been identified as a symmetric NAT. This alarm clears when a non-symmetric NAT or no NAT replaces the symmetric NAT.	AMS 314

Alarm/Trap	Description	Log
Operational State Change (acOperationalStateChange)	Operational state is "disabled". When the state changes from enabled to disabled, an SNMP traps is sent with a "major" status. If the Media Server 2000 (ATM or IP) fails to initialize the operation state is disabled. A corresponding clear trap is sent when the state changes back to an "enabled" state. In ATM systems, the operational state of the node is also disabled if there are no ATM ports available for use. An ATM port is available for use if it is unlocked and enabled.	AMS 312
Performance Monitoring Threshold Crossing (acPerformanceMonitoring ThresholdCrossing)	Generates an information log every time the threshold of a performance monitored object is crossed. The *source* varibind in the trap indicates the object for which the threshold is crossed. The severity field is *warning* when the threshold is crossed, and *cleared* when it goes back below the threshold.	AMS 800

Customer Logs

The following table lists the Media Server 2000 Series logs. Refer to the Media Server 2000 Series alarms table above for a description of the alarms.

For additional information on Media Server Series logs including corrective Action and Probable Cause, refer to the *Carrier Voice over IP Fault Management Logs Reference* Volume 3 (NN10275-909).

> ***Note:*** The Media Server 2000 server must be added to IEMS for monitoring and management.

The table below also list the associated logs for the alarms. AMS numbers are added to the Media Server 2000 SNMP traps as they are processed by the management server and are visible in the IEMS user interface.

Media Server 2000 Series Logs

Log	Indication	Alarm/Trap
AMS 300	Resetting Board	acBoardEvResettingBoard
AMS 301	Fatal Error	acBoardFatalError

Log	Indication	Alarm/Trap
AMS 302	Configuration Error	acBoardConfigurationError
AMS 303	Temperature Alarm	acBoardTemperatureAlarm
AMS 304	Feature Key Error	acFeatureKeyError
AMS 305	Board Call Resource Alarm	acBoardCallResourceAlarm
AMS 306	Board Controller Failure Alarm	acBoardControllerFailureAlarm
AMS 307	Board Ethernet Link Alarm	acBoardEthernetLinkAlarm
AMS 308	Board Overload Alarm	acBoardOverloadAlarm
AMS 309	Active Alarm Table Overflow	acActiveAlarmTableOverflow
AMS 310	ATM Port Alarm	acAtmPortAlarm
AMS 311	Audio Provisioning Alarm	acAudioProvisioningAlarm
AMS 312	Operational State Change	acOperationalStateChange
AMS 314	NAT Traversal Alarm	acNATTraversalAlarm
AMS 500	Board Started	acBoardEvBoardStarted
AMS 501	Admin State Change	acgwAdminStateChange
AMS 600	Enhanced BIT Status	acEnhancedBITStatus
AMS 800	Performance Monitoring Threshold Crossing	acPerformanceMonitoring ThresholdCrossing
XPKT340	Packet Media Anchor Call failure. Potential announcement, conference, or BCT resource setup issue.	

BootP operation

A BootP server is configured on the SDM or CBM for the Media Server 2000 Series. The BootP server is needed, initially, for assigning an IP address for a Media Server 2000 Series node when it is installed. After installation is complete, the BootP server is used as a backup configuration repository for Media Server 2000 Series software loads (CMP file) and the basic configuration file (INI file).

A request to reload the CMP and INI files to a Media Server 2000 Series node from the BootP server is generated in response to the following:

- the Media Server 2000 Series node is power-cycled
- the Media Server 2000 series is reset

- a watchdog process running on the Media Server 2000 Series node determines that a fatal error has occurred in the IPM-1610 board

APS fault management

Since the APS resides on the CS 2000 Management Tool, the server that also hosts the CS 2000 Management Tools, APS fault management is primarily concerned with the audio provisioning function. A complete suite of procedures performed at a command line interface, in a telnet connection to the CS 2000 Management Tool enable you to correct these APS error conditions.

Media Server 2000 Series and APS fault management procedures

The following table lists Media Server 2000 Series fault management procedures.

Media Server 2000 Series fault management procedures

Procedure and page
"IPM-1610 fault management" (page 15)
"TP-6310 fault management" (page 16)

The following table lists Media Server 2000 Series fault management replacement procedures.

Media Server 2000 Series fault management replacement procedures

Procedure and page
"Replacing the Media Server 2010 Chassis" (page 69)
"Replacing the IPM-1610 board on a Media Server 2010" (page 78)
"Replacing the TP-6310 or SA-3 board on a Media Server 2020" (page 85)
"Replacing the TP-6310 RTM on a Media Server 2020" (page 91)
"Replacing the PEM on a Media Server 2020" (page 94)
"Replacing the Media Server 2020 power supply" (page 97)
"Replacing the Fan Tray Unit on a Media Server 2020" (page 100)
"Replacing the fan filter on a Media Server 2020" (page 102)

The following table lists APS alarm and log retrieval procedures, and APS fault management procedures.

APS alarm and log retrieval procedures and management procedures

Procedure and page
"APS alarms" (page 21)
"APS logs" (page 24)
"Viewing APS system alarms and logs" (page 41)
"APS troubleshooting guide" (page 42)
"Troubleshooting the APS provisioner" (page 44)
"Removing provisioner lock files" (page 46)
"Checking for active audio provisioner processes" (page 47)
"Troubleshooting APS login problems" (page 48)
"Starting the APS Oracle database" (page 54)
"Restoring audio files to a Media Server 2000 Series node" (page 66)
"Rebooting an APS" (page 68)

IPM-1610 fault management

The IPM-1610 cPCI Board is the main component of the Media Server 2010. The IPM-1610 is provisioned in a slot within the IPmedia 2000 chassis. On the front panel of the IPM-1610 board, LED indicators indicate the board's operational status. These LED indicators, which are labeled on the IPM-1610 front panel, are described in the tables below.

Board status LED indicators

Label	Color	Indication
FAIL	Off	Normal board operation
	Red	Fatal board failure
ACT	Green	Initialization OK; lights after download has completed successfully

Ethernet LED indicators

Label	Color	Indication
LINK	Green	The Ethernet link is active.
	Off	The Ethernet link is inactive.
ACT	Flashing Yellow	Normal Inservice - Packets are active on the Ethernet link (Receive or Transmit)
	Off	No packets are being transmitted/received on the Ethernet link.

Auxiliary LED indicators

Label	Color	Indication
PWR	Green	Power is supplied to the board.
	Off	Board power supply failure.
SWAP READY	Blue	The board can be removed or inserted.

TP-6310 fault management

The TP-6310 cPCI Board is the main component of the Media Server 2020, and is provisioned in a slot within the Media Server 2020 chassis. On the front panel of the TP-6310 board, LEDs indicate the board's operational status. These LED indicators, which are labeled on the TP-6310 front panel, are described in the tables below.

Board status LED indicators

Label	Color	Indication
FAIL	Off	Normal operation
	Red	Board failure
ACT	Off	Redundant board in standby mode
	Green	Working board

GbE (Ethernet) LED indicators

Label	Color	Indication
LINK 1	Off	No link
	Blinking Green	RX/TX OK
LINK 2	Off	No link
	Blinking Green	RX/TX OK

PSTN LED indicators

Label	Color	Indication
LINK 1A	Off	No Link
	Green	Working Link OK
	Yellow	Protection Link OK

Label	Color	Indication
ALARM 1A	Off	Normal operation
	Red	LOS - Loss of Signal
		RS-LOF (SDH) or LOF (SONET) - Loss of Frame
		MS-AIS (SDH) or AIS-L (SONET) - Alarm Indication Signal
		MS-RDI (SDH) or RDI-L (SONET) - Remote Defect Indication
LINK 1B	Off	No Link
	Green	Working Link OK
	Yellow	Protection Link OK
ALARM 1B	Off	Normal operation
	Red	LOS - Loss of Signal
		RS-LOF (SDH) or LOF (SONET) - Loss of Frame
		MS-AIS (SDH) or AIS-L (SONET) - Alarm Indication Signal
		MS-RDI (SDH) or RDI-L (SONET) - Remote Defect Indication

ATM LED indicators

Label	Color	Indication
Rx/Tx 1A	Off	No Link
	Blinking Green	Working Link OK; Rx/Tx OK
	Green	Working Link OK; No Rx/Tx
	Blinking Yellow	Protection Link OK; Rx/Tx OK
	Yellow	Protection Link OK; No Rx/Tx
ALARM 1A	Off	Normal operation
	Red	LOS - Loss of Signal
		RS-LOF (SDH) or LOF (SONET) - Loss of Frame
		MS-AIS (SDH) or AIS-L (SONET) - Alarm Indication Signal
		MS-RDI (SDH) or RDI-L (SONET) - Remote Defect Indication

Label	Color	Indication
Rx/Tx 2A	Off	No Link
	Blinking Green	Working Link OK; Rx/Tx OK
	Green	Working Link OK; No Rx/Tx
	Blinking Yellow	Protection Link OK; Rx/Tx OK
	Yellow	Protection Link OK; No Rx/Tx
ALARM 2A	Off	Normal operation
	Red	LOS - Loss of Signal
		RS-LOF (SDH) or LOF (SONET) - Loss of Frame
		MS-AIS (SDH) or AIS-L (SONET) - Alarm Indication Signal
		MS-RDI (SDH) or RDI-L (SONET) - Remote Defect Indication
Rx/Tx 3A	Off	No Link
	Blinking Green	Working Link OK; Rx/Tx OK
	Green	Working Link OK; No Rx/Tx
	Blinking Yellow	Protection Link OK; Rx/Tx OK
	Yellow	Protection Link OK; No Rx/Tx
ALARM 3A	Off	Normal operation
	Red	LOS - Loss of Signal
		RS-LOF (SDH) or LOF (SONET) - Loss of Frame
		MS-AIS (SDH) or AIS-L (SONET) - Alarm Indication Signal
		MS-RDI (SDH) or RDI-L (SONET) - Remote Defect Indication
Rx/Tx 1B	Off	No Link
	Blinking Green	Working Link OK; Rx/Tx OK
	Green	Working Link OK; No Rx/Tx
	Blinking Yellow	Protection Link OK; Rx/Tx OK
	Yellow	Protection Link OK; No Rx/Tx

Label	Color	Indication
ALARM 1B	Off	Normal operation
	Red	LOS - Loss of Signal
		RS-LOF (SDH) or LOF (SONET) - Loss of Frame
		MS-AIS (SDH) or AIS-L (SONET) - Alarm Indication Signal
		MS-RDI (SDH) or RDI-L (SONET) - Remote Defect Indication
Rx/Tx 2B	Off	No Link
	Blinking Green	Working Link OK; Rx/Tx OK
	Green	Working Link OK; No Rx/Tx
	Blinking Yellow	Protection Link OK; Rx/Tx OK
	Yellow	Protection Link OK; No Rx/Tx
ALARM 2B	Off	Normal operation
	Red	LOS - Loss of Signal
		RS-LOF (SDH) or LOF (SONET) - Loss of Frame
		MS-AIS (SDH) or AIS-L (SONET) - Alarm Indication Signal
		MS-RDI (SDH) or RDI-L (SONET) - Remote Defect Indication
Rx/Tx 3B	Off	No Link
	Blinking Green	Working Link OK; Rx/Tx OK
	Green	Working Link OK; No Rx/Tx
	Blinking Yellow	Protection Link OK; Rx/Tx OK
	Yellow	Protection Link OK; No Rx/Tx
ALARM 3B	Off	Normal operation
	Red	LOS - Loss of Signal
		RS-LOF (SDH) or LOF (SONET) - Loss of Frame
		MS-AIS (SDH) or AIS-L (SONET) - Alarm Indication Signal
		MS-RDI (SDH) or RDI-L (SONET) - Remote Defect Indication

Power and Swap Ready status LED indicators

Label	Color	Indication
PWR	Off	No power to board
	Green	Normal operation
SWAP READY	Off	No power to board
	Blue	cPCI can be removed, or has been inserted successfully

APS alarms

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

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
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)

Field	Description
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 alarms - connection errors

The cause of connection errors (CONNECT_ERR) can be that the database is down, the APS database account password is invalid and needs to be reset, or there are problems with the database (it may be corrupt) and a restore from a previous backup may be required.

APS Administration Alarms

This section contains APS Administration alarms. The APS administration software has detected that a connection to the database needed to read and write information cannot be made. The administration area of the APS sets up media server nodes, user accounts, provision sets, and program groups.

Refer to "Troubleshooting APS database connections" (page 55) for procedures on correcting faulty database connections.

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. The APS file upload software has detected that a connection to the database needed to read and write information cannot be made. The file upload area of the APS handles audio file uploads from a user's desktop machine to the APS database.

Refer to "Troubleshooting APS database connections" (page 55) for procedures on correcting faulty database connections.

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. The APS audio management software has detected that a connection to the database needed to read and write information cannot be made. Audio management of the APS handles importing audio into the APS and assigning audio ids, creating audio sets, sequences, variables, and languages.

Refer to "Troubleshooting APS database connections" (page 55) for procedures on correcting faulty database connections.

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"

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.

For additional information on APS logs including corrective Action and Probable Cause, refer to *Carrier Voice over IP Fault Management Logs Reference*Volume 1 (NN10275-909)

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 CS 2000 Management Tool, 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 CS 2000 Management Tool, 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 CS 2000 Management Tool, 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.

Note: For additional provisioner log information, including corrective Action and Probable Cause, refer to *Carrier Voice over IP Fault Management Logs Reference*Volume 1 (NN10275-909)

"The specified node ($NODE_ID) is not a configured node on $(hostname)."

"The specified node ($NODE_ID) either does not have provisioning enabled or else does not have a provision set assigned to it on $(hostname)."

"Problems on $(hostname) transferring files for node $NODE."

"The last prov date for the node $NODE cannot be updated on $(hostname) because the database is not accessible."

"A full provisioner process cannot be run when another full provision is already in progress on $(hostname)"

"A full provisioner process has timed out waiting for a node-specific provisioner process to complete on $(hostname)."

"A node-specific provisioner process cannot be run on $(hostname) because a full provision is already in progress."

"A node-specific provisioner process cannot be run on $(hostname) because another provision process is already running for that node."

"The provisioner cannot run on $(hostname) because the file system ($IpsProvPath) is full."

"The $IpsProvPath file system on $(hostname) is almost full. The provisioner will not be able to run if corrective action isn't taken."

"The provisioner cannot run on $(hostname) because the database is inaccessible."

The "adclient" (audio distributor client) runs the Media Server 2000 Series provisioning process. The dynamic text message that appears in a log when a problem with provisioning occurs is:

"the AMS (Media Server 2000 Series) provisioner (adclient) encountered errors while distributing audio files to one or more of the following AMS nodes:"

The proprietary protocol used for communication between the APS and the Media Server 2000 Series is "TPNCP". If an error in communication occurs between the APS and Media Server 2000 Series, the following message may appear:

"There was a TPNCP failure."

The "/PROV_data" directory, which contains the provisioner logs described above, can be viewed on the CS 2000 Management Tool at the following location:

/PROV_data/<*APS hostname*>_provisioner.log

Another provisioner log file, that contains additional detail about the provisioning logs, can be viewed on the CS 2000 Management Tool at the following location:

/opt/uas/aps/log/admanager <*date*>.log

This file should be accessed when the detail in the provisioner logs is not sufficient to determine the cause of the provisioning problem. The log messages in this "admanager.log" file can also help in determining a corrective action to perform in response to the problem.

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

Note: For additional APS system log information, including corrective Action and Probable Cause, refer to *Carrier Voice over IP Fault Management Logs Reference*Volume 1 (NN10275-909)

For a procedure used to view APS system logs, see Procedure "Viewing APS system alarms and logs" (page 41).

Servlet Request logs

This section contains Servlet Request logs.

45058 SESSION_TIMER_EXPIRED

EventType="information"

Message="Session timer expired: <n>"

45059 DB_SW_EXCEPTION

EventType="error"

Message="Software exception: <n>"

45060 DB_RMI_EXCEPTION

EventType="error"

Message="RMI exception: <n>"

45061 DB_DB_ERR

EventType="error"

Message="Error while accessing the DB."

45062 INVLD_OPCODE

EventType="information"

Message="Invalid OpCode: <n>"

Audio Management logs

This section contains Audio Management logs.

28673 AM_SW_EXCEPTION

EventType="error"

Message="Software exception: <n>"

28674 AM_SQL_EXCEPTION

EventType="error"

Message="SQL exception: <n>"

28675 AM_DB_ERROR

EventType="error"

Message="Error while accessing the DB."

28676 USER_BEGIN_SESSION

EventType="information"

Message="User: <n>, Group: <n> - is beginning a session at: <n>"

28677 USER_END_SESSION

EventType="information"

Message="User: <n>, Group: <n> - is ending a session"

28678 USER_NOT_ACTIVE

EventType="warning"

Message="User: <n>, Group: <n> - status is not active"

28679 USER_UPLOAD_FILE

EventType="information"

Message="User: <n>, is uploading files."

28680 READ_ERROR

EventType="error"

Message="Error while reading from: <n>"

28681 WRITE_ERROR

EventType="error"

Message="Error while writing to file: <n>"

28682 DELETE_ERROR

EventType="error"

Message="Error while deleting: <n>"

28683 INVLD_FILE_OR_DIR

EventType="error"

Message="Invalid file or directory: <n>"

28684 DIR_CREATED

EventType="information"

Message="Directory created: <n>"

28685 SEG_ID_GENERATED

EventType="information"

Message="New generated seg id: <n>"

28686 SEG_ID_RELEASED

EventType="information"

Message="Seg id released: <n>"

28687 PKG_ID_GENERATED

EventType="information"

"Message="New generated package id: <n>"

28688 PKG_ID_RELEASED

EventType="information"

"Message="Package id released: <n>"

28689 MAX_VER_REACHED

EventType="information"

Message="Max number of versions reached for physseg id: <n>"

28690 MAX_VER_NUMBER_EXCEEDED

EventType="warning"

Message="Max version number exceeded for physseg id: <n>"

28691 PKG_MAX_VER_REACHED

EventType="information"

Message="Max number of versions reached for pkg id: <n>"

28692 PKG_MAX_VER_NUMBER_EXCEEDED

EventType="warning"

Message="Max version number reached for pkg id: <n>"

28693 MAX_SET_DEPTH_REACHED

EventType="warning"

Message="Max set depth reached for set id: <n>"

28694 MAX_SEQ_DEPTH_REACHED

EventType="warning"

Message="Max sequence depth reached for seq id: <n>"

28695 NO_SEG_IN_DB

EventType="information"

Message="No segments in DB"

28696 AM_INVLD_SEG_ID

EventType="warning"

Message="Invalid segment id: <n>"

28697 INVLD_PHYS_SEG_ID

EventType="warning"

Message="Invalid phys segment id: <n>, ver: <n>"

28698 AM_INVLD_PKG_ID

EventType="warning"

Message="Invalid package id: <n>, ver: <n>"

28699 AM_INVLD_PE_TYPE

EventType="warning"

Message="Invalid PE Type: <n>"

28700 AM_INVLD_PROG_GRP

EventType="warning"

Message="Invalid program group: <n>"

28701 AM_INVLD_SELECTOR_TYPE

EventType="warning"

Message="Invalid selector type: <n>"

28702 AM_INVLD_SELECTOR_VAL

EventType="warning"

Message="Invalid selector value: <n>"

28703 AM_ZIP_ARCHIVE_EXTRACTED

EventType="information"

Message="Zip archive extracted: <n>"

28704 SET_INFINITE_LOOP

EventType="warning"

Message="Infinite loop in set id: <n>"

28705 SEQ_INFINITE_LOOP

EventType="warning"

Message="Infinite loop in sequence id: <n>"

28706 SEGID_NOT_UNIQUE

EventType="information"

Message="Seg id: <n> is not unique"

28707 ALIAS_NOT_UNIQUE

EventType="information"

Message="Alias: <n> is not unique"

28708 SELECTOR_VALUE_NOT_UNIQUE

EventType="information"

Message="Selector value: <n> is not unique"

28709 SEGID_AND_ALIAS_NOT_UNIQUE

EventType="information"

Message="Seg id <n> and alias <n> are not unique"

28710 NO_PERM_TO_CACHE

EventType="information"

Message="No permission to set cache for user: <n>"

28711 NO_PERM_TO_LOCK

EventType="information"

Message="No permission to change lock status for user: <n>"

28712 INVLD_LOCK_STATUS

EventType="information"

Message="Seg id: <n> cannot be added to locked package: <n>"

28713 INVLD_PKG_FORMAT

EventType="warning"

Message="Invalid package format, segment id: <n> cannot be added to package: <n>"

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)<n>"

47105 FTL01 LANG_VER_PROV_PROBLEM

EventType="error"

Message="The langver.dat file was not able to be provisioned. (severity = MAJOR)<n>"

47106 FTL02 IPS_PROVISIONER_TERMINATION

EventType="error"

Message="The provisioner experienced early termination. (severity = CRITICAL)<n>"

47106 FTL02 IPS_PROVISIONER_TERMINATION / APS DATA BASE IS DOWN

EventType="error"

Message="The provisioner experienced early termination. (severity = CRITICAL)<n>" 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)<n>"

47135 FTL31 FILE_ACCESS_FAILURE

EventType="error"

Message="A file cannot be accessed. Probable causes: incorrect file permissions or full filesystem. (severity = CRITICAL)<n>"

File Upload logs

This section contains File Upload logs.

43009 FT_SW_EXCEPTION

EventType="error"

Message="Software exception: <n>"

43010 FT_SQL_EXCEPTION

EventType="error"

Message="SQL exception: <n>"

43011 FT_IO_FILE_ERR

EventType="error"

Message="IO file error: <n>"

43012 FTP_CONNECT

EventType="information"

Message="Connected to host IP: <n>"

43013 FTP_CONNECT_ERROR

EventType="error"

Message="Could not connect to host IP: <n>"

43014 FTP_CDW_FAILED

EventType="warning"

Message="Could not change directory to: <n>"

43015 FTP_FILE_FAILED

EventType="warning"

Message="File <n> could be not transferred."

43016 FT_ZIP_ARCHIVE_EXTRACTED

EventType="information"

Message="ZIP archive extracted: <n>"

Administration logs

This section contains Administration logs.

26625 CM_SW_EXCEPTION

EventType="error"

Message="Software exception: <n>"

26626 CM_SQL_EXCEPTION

EventType="error"

Message="SQL exception: <n>"

26627 CM_DB_ERR

EventType="error"

Message="Error while accessing the DB."

26628 NULL_VALUE

EventType="warning"

Message="Null value for: <n>"

26629 CREATE_USER_ERR

EventType="error"

Message="Error creating user: <n>"

26630 CREATE_DIR_ERR

EventType="error"

Message="Error creating directory: <n>"

26631 CREATE_NODE_ERR

EventType="error"

Message="Error creating node: <n>"

26632 REMOVE_NODE_ERR

EventType="error"

Message="Error removing node: <n>"

26633 HOSTF_UPDATE_ERR

EventType="error"

Message="Error updating host file: <n>"

26634 NODE_NOT_ENABLED

EventType="information"

Message="Node not enabled: <n>"

26635 CM_INVLD_PROG_GRP

EventType="warning"

Message="Invalid program group: <n>"

26636 CM_INVLD_SEG_ID

EventType="warning"

Message="Invalid segment id: <n>"

26637 CM_INVLD_PKG_ID

EventType="warning"

Message="Invalid package id: <n>"

26638 CM_INVLD_PE_TYPE

EventType="warning"

Message="Invalid PE Type: <n>"

26639 CM_INVLD_SELECTOR_TYPE

EventType="warning"

Message="Invalid selector type: <n>"

26640 CM_INVLD_SELECTOR_VAL

EventType="warning"

Message="Invalid selector value: <n>"

26641 INVLD_PROV_SET

EventType="warning"

Message="Invalid provisionable set: <n>"

26642 INVLD_NODE_ID

EventType="warning"

Message="Invalid node id: <n>"

26643 INVLD_USER_ID

EventType="warning"

Message="Invalid user id: <n>"

26644 INVLD_SYS_PARM_VALUE

EventType="warning"

Message="Invalid sys parm value: <n>"

26645 INVLD_ENTITY

EventType="warning"

Message="Invalid entity: <n> of entity type: <n>"

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: <n> is not unique"

26648 PRG_GRP_NOT_UNIQUE

EventType="information"

Message="Program group: <n> is not unique"

26649 PROV_SET_NOT_UNIQUE

EventType="information"

Message="Provision set: <n> is not unique"

26650 SELTYPE_DISPVAL_NOT_UNIQUE

EventType="information"

Message="Selector type display value: <n> is not unique"

26651 USER_NO_ACCESS

EventType="information"

Message="User: <n> has no access to program group: <n>"

26652 SELECTOR_TYPE_EXISTS

EventType="information"

Message="Selector type: <n> already exists"

26653 SELECTOR_VALUE_EXISTS

EventType="information"

Message="Selector value: <n> already exists"

26654 ASSOCIATION_EXISTS

EventType="warning"

Message="Association already exists between <n> and <n>"

26655 CHG_PERM_EXIT_CODE

EventType="information"

Message="Exit code: % while changing permission on: <n>"

26656 REM_NODE_EXIT_CODE

EventType="information"

Message="Exit code: % while removing node: % from <n>"

26657 REM_DIR_EXIT_CODE

EventType="information"

Message="Exit code: % while removing userdir for user: <n>"

26658 INCONSISTENT_ARRY_SIZE

EventType="warning"

Message="Inconsistent array sizes between <n> and <n>"

26659 CALLP_VAL_NOT_UNIQUE

EventType="information"

Message="CallP value: <n> is not unique"

26660 SELVAL_NOT_UNIQUE

EventType="information"

Message="Selector value: <n> is not unique"

26661 DISPVAL_NOT_UNIQUE

EventType="information"

Message="Selector type display value: <n> is not unique"

26662 CM_INVLD_AE_TYPE

EventType="warning"

Message="Invalid AE Type: <n>"

Viewing APS system alarms and logs

Viewing APS system alarms and logs

Step	Action

In a telnet connection to the CS 2000 Management Tool

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, you specify that the SNMP agent is to forward alarms/logs to syslog (refer to the Media Server 2000 Series Configuration Management document).

Note 2: For information about the APS logs and alarms that display, see "APS alarms" (page 21).

3 You have completed this procedure.

—End—

APS troubleshooting guide

CAUTION
Use extreme care when manually disabling NFS, Telnet, HTTP and/or HTTPS, and FTP services. Disabling these services will disrupt the APS functionality.

The APS relies on NFS, Telnet, HTTP and/or HTTPS, and FTP services being enabled on the CS 2000 Management Tools server to perform audio provisioning, the distribution of the audio files to the MS 2000, and general administration and maintenance functions. These services are enabled by default.

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

Trouble Indicator	Procedure to perform
Cannot get audio to the Media Server 2000 Series node from the APS	"Troubleshooting the APS provisioner" (page 44)
Audio on the Media Server 2000 Series node sounds distorted.	The Media Server 2000 Series supports audio G.711 A-law or Mu-law format, sampled at 8 kHz. This is the preferred format for audio for the Media Server 2000 Series. Therefore, ensure that the correct format has been selected in the audio file import dialog in the APS GUI (refer to the Media Server 2000 Series 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

Trouble Indicator	Procedure to perform
Cannot log in to the APS	"Troubleshooting APS login problems" (page 48)
Cannot create a new APS Administration GUI user account	In a Telnet connection to the CS 2000 Management Tool, 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.

Troubleshooting the APS provisioner

Use the following procedures to troubleshoot the APS provisioner that has stopped for some unknown reason.

Troubleshooting the APS provisioner

Step	Action

In a telnet connection to the CS 2000 Management Tool

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 Media Server 2000 Series 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 a full provisioner process is already running.

Cause: Two full provisioner processes cannot run simultaneously.

Action:
- Perform the procedure "Removing provisioner lock files" (page 46). You may then wish to see if your provisioning process is running by performing the procedure "Checking for active audio provisioner processes" (page 47). 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 unnecessary 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" (refer to the Media Server 2000 Series Administration and Security document).

Message: Provisioner stop on <hostname> at <time> because node <Media Server 2000 Series_node> is not provisionable.

Action:
Make the Media Server 2000 Series 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 Media Server 2000 Series, perform the "Creating a provision set" procedure (refer to the Media Server 2000 Series Configuration Management document).
- To enable provisioning on the Media Server 2000 Series, perform the "Enabling provisioning of a Media Server 2000 Series node" procedure (refer to the Media Server 2000 Series Configuration Management document)

5 You have completed this procedure.

—End—

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

Step	Action

In a telnet connection to the CS 2000 Management Tool

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.

—End—

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

Step	Action

In a telnet connection to the CS 2000 Management Tool

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.

—End—

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

Step Action

At your console

1 Verify that the URL in your browser address window is correct. The URL should be: 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 CS 2000 Management Tool

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 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	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 CS 2000 Management Tool process and let the server re-start automatically, by entering the following command:

```
/opt/uas/aps/scripts/killDbServer.sh
```

A message eventually displays indicating that the server is re-starting.

11 Enter the following command to check the status of the database:

```
/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	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 should display.

If	Do
the sql prompt does not display	step 14
the sql prompt does display	step 26

14 Determine whether you already re-started the Oracle database once before during this procedure.

If	Do
you have already re-started the database once before	step 27
you have not already re-started the database once before	step 15

15 Restart the Oracle database by entering the following command:

```
/opt/servman/bin/servstart DATABASE
```

16 Kill the CS 2000 Management Tool process and let the server re-start automatically, by entering the following command:

```
/opt/uas/aps/scripts/killDbServer.sh
```

A message eventually displays indicating that the server is re-starting. 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 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	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 CS 2000 Management Tool is entered in the browser address window, but the login page is not accessible, an Application Launch Point page should 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 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	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 CS 2000 Management Tool process and let the server re-start automatically, by entering the following command:

```
/opt/uas/aps/scripts/killDbServer.sh
```

A message eventually displays indicating that the server is re-starting. 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 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	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.

—End—

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 re-start the Oracle database as part of APS system recovery.

Starting the APS Oracle database

Step	Action

In a telnet connection to the CS 2000 Management Tool

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 CS 2000 Management Tool process and let the server re-start automatically, by entering the following command:

```
/opt/uas/aps/scripts/killDbServer.sh
```

A message eventually displays indicating that the server is re-starting.

> ***Note:*** The web server and the Java servlet engine will be re-started as a result of this command. CS 2000 Management Tools users may be temporarily impacted while the web server re-starts.

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.

—End—

Troubleshooting APS database connections

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 resolve connection problems between the APS and the Oracle database.

Troubleshooting APS database connections

Step	Action

Corrective actions for database connection alarms

1 Determine if the database is up and running. Commands to query and start the database are shown below.

a. Query the database

```
# servquery -status -group DATABASE

Oracle Instance is DOWN.
Oracle Listener is DOWN

# servquery -status all
```

```
APP NAME                    STATUS
=======                     ======
DATABASE                    NOT RUNNING
CINOTIFIER                  NOT RUNNING
BACKUP_MANAGER              NOT RUNNING
APS                         NOT RUNNING
.
.
.
```

Note: The instance and listener status should be "UP" for an in-service condition. Displayed above are outputs in which the database is down.

b. If the output from the above commands indicate that the database is down (NOT RUNNING) and the listener and instance are down, then enter the following command:

```
# servstart DATABASE
```

c. Repeat step "a" to verify that the database is up.

If	Do
The database is up	You are finished
The database is down	go to

2 If the database is still down, then the APS oracle account password may need to be reset:

a. Access the "apscli" tool

```
# apscli

APS Command Line Interface MAIN MENU

_____________________________________
1) Database Queries, Reports, Status, Checks
2) Audio Provisioner Actions
3) Restart APS Server Processes
4) Software Listing and Inventory
5) APS Database and Application File Backups,
Restores
6) APS SNMP Agent, configure, start, stop.
7) LOG files, Accessing and Viewing
8) View, access UAS node(s) conf file(s) backup
directory
9) Determine if APS Server Processes are running.
10) Audits and aps checking utilities.
11) Configure Audio Distribution HTTP/HTTPS
X) Exit
Enter a number or (X) --> 1
1
APS Command Line Interface MAIN MENU -> DATABASE

_____________________________________________________
1) Query Data Base Status
2) Stop Data Base
3) Start Data Base
4) REPORT - List UAS & AMS Nodes in the DB (Nodes,
IPs)
5) REPORT - List UAS & AMS Nodes in the DB (node,
IP, Enabled/Disabled, Last Prov Date)
6) REPORT - List APS System Parameters in the DB
7) Disable all UAS/AMS Node(s) from provisioning in
the DB
8) REPORT - List APS DB Tablespaces (bytes, blocks
free)
9) REPORT - Users Modified in APS DB between
DD-MM-YY and DD-MM-YY
10) REPORT - Audio Added in APS DB between DD-MM-YY
and DD-MM-YY
```

```
11) REPORT - Audio Package Report Activity between
DD-MM-YY and DD-MM-YY
12) REPORT - Audio Segments Not Assigned to a
Program Group
13) REPORT - Program Group Report between DD-MM-YY
and DD-MM-YY
14) Modify Passwords
X) Exit
Enter a number ----> 14
APS Command Line Interface MAIN MENU -> DATABASE ->
PASSWORD MGMT

_____
_____________
1) Reset Lion Password
2) Change Lion Password
3) Reset admin Password
4) Change admin Password
X) Exit
Enter a number ---> 1
Accessing the Oracle DB and changing the account ...
Please wait.
APS server manager start ...
SQL*Plus:  Release 9.2.0.7.0 - Production on Feb 2
13:40:52 2006
Copyright (c) 1982, 2002, Oracle Corporation.
All rights reserved.
Connected to:
Oracle9i Enterprise Edition Release 9.2.0.7.0 -
Production
JServer Release 9.2.0.7.0 - Production
SQL>
User altered.
SQL> Disconnected form Oracle9i Enterprise Edition
Release 9.2.0.7.0 - Production JServer Release
9,2,0,7.0 Production Completed ...
The APS dbserver software should be re-started to
use the new password.
Do you want to do this now?  (Y/N) ---> Y
Killing File Upload
Killing APS Db Server
Killing Db Server
Actions completed.
Changing LION's password in the Oracle database...
Changing LION's password in the Properties Server...
Successfully changed LION's password.
```

3 If problems continue with the database connection alarms, then contact your technical support organization.

—End—

IPM-1610 cPCI Board troubleshooting guide

The procedures that you perform to address operational issues pertaining to the IPM-1610 cPCI Board are determined by system problem LED indicators. 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 problem(s).

Trouble Indicator	Procedure to perform
Red LED indicator is ON	"Troubleshooting the IPM-1610 cPCI Board" (page 60)
LINK or ACT LED indicator is OFF	"Troubleshooting the IPM-1610 cPCI Board Ethernet connection" (page 61)
PWR LED indicator is OFF	"Troubleshooting the IPM-1610 cPCI Board power supply" (page 62)

Troubleshooting the IPM-1610 cPCI Board

The following procedures enable you to troubleshoot the IPM-1610 Board in the event that the Red LED indicator is ON.

Step	Action

Troubleshooting the IPM-1610 cPCI Board

1 Perform a board reset.

If	Do
the Red LED indicator is OFF	You are finished.
the Red LED indicator is ON	step 2

2 Upgrade the server with a new software load and valid configuration file.

If	Do
the Red LED indicator is OFF	You are finished.
the Red LED indicator is ON	Refer to the "Replacing the IPM-1610 board on a Media Server 2010" (page 78) procedure to replace the IPM-1610 Board if a hardware problem is suspected.

3 Contact Nortel Networks technical support if the problem persists.

—End—

Troubleshooting the IPM-1610 cPCI Board Ethernet connection

The following procedures enable you to troubleshoot the IPM cPCI Board Ethernet connection in the event that the LINK or ACT LED indicator is OFF.

Step	Action

Troubleshooting the IPM cPCI Board Ethernet connection

1 Plug in an active network cable for the port.

2 Verify that the other end of the cable is connected to the network.

If	Do
the LINK LED indicator is ON and the Ethernet ACT LED is flashing yellow	You are finished.
the LINK or Ethernet ACT LED indicator is OFF	step 3

3 Replace the cable.

If	Do
the LINK LED indicator is ON and the Ethernet ACT LED is flashing yellow	You are finished.
the LINK or Ethernet ACT LED indicator is OFF	Refer to the "Replacing the Media Server 2010 Chassis" (page 69) procedure to replace the Media Server 2010 chassis if a hardware problem is suspected.

4 Contact Nortel Networks technical support if the problem persists.

—End—

Troubleshooting the IPM-1610 cPCI Board power supply

The following procedures enable you to troubleshoot the IPM cPCI Board power supply in the event that the PWR LED indicator is OFF.

Step	Action

Troubleshooting the IPM cPCI Board power supply

1 Verify that the fuses are intact.

If	Do
a fuse is blown	Replace the fuse.
the PWR LED indicator is OFF	step 2

2 Verify that the power cable is properly connected.

If	Do
the PWR LED indicator is ON	You are finished.
the PWR LED indicator is OFF	Refer to the "Replacing the Media Server 2010 Chassis" (page 69) procedure to replace the Media Server 2010 chassis if a hardware problem is suspected.

3 Contact Nortel Networks technical support if the problem persists.

—End—

TP-6310 Board troubleshooting guide

The procedures that you perform to address operational issues pertaining to the TP-6310 Board are determined by system problem LED indicators. 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 problem(s).

Trouble Indicator	Procedure to perform
Red LED indicator is ON	"Troubleshooting the TP-6310 Board" (page 64)
GbE (Ethernet) LINK1 or LINK2 LED indicator is OFF	"Troubleshooting the TP-6310 Board GbE (Ethernet) connection" (page 65)
PSTN LED indicators are all OFF	This is normal operation in the MS2020 configuration.
Rx/Tx 1A is LED indicator is Blinking Green, Rx/Tx 1B LED indicator is OFF	This is normal operation in the MS2020 one-fiber link configuration.
Rx/Tx 1A LED indicator is Blinking Green (or Yellow), Rx/Tx 1B LED indicator is Blinking Yellow (or Green)	This is normal operation in the MS2020 two-fiber link configuration.
ATM Alarm 1A or 1B Red LED indicator is ON	This indicates that there is a severe loss of signal between the ATM and the server. Possible causes are the fiber is cut, the link is down, or the passport is down.
ATM Alarm 2A, 3A, 2B, and 3B Red LED indicators are ON	This is normal operation in the MS2020 configuration.

Troubleshooting the TP-6310 Board

The following procedures enable you to troubleshoot the TP-6310 Board in the event that the Red LED indicator is ON.

Step	Action

Troubleshooting the TP-6310 Board

1 Perform a board reset.

If	Do
the Red LED indicator is OFF	You are finished.
the Red LED indicator is ON	step 2

2 Upgrade the server with a new software load and valid configuration file.

If	Do
the Red LED indicator is OFF	You are finished.
the Red LED indicator is ON	Refer to the "Replacing the TP-6310 or SA-3 board on a Media Server 2020" (page 85) procedure to replace the TP-6310 Board if a hardware problem is suspected.

3 Contact Nortel Networks technical support if the problem persists.

—End—

Troubleshooting the TP-6310 Board GbE (Ethernet) connection

The following procedures enable you to troubleshoot the TP-6310 Board GbE (Ethernet) connection in the event that the LINK1 or LINK2 indicator is OFF.

Step	Action

Troubleshooting the TP-6310 Board GbE (Ethernet) connection

1 Plug in an active network cable for the port.

2 Verify that the other end of the cable is connected to the network.

If	Do
the LINK LED indicator is flashing green	You are finished.
the LINK LED indicator is OFF	step 3

3 Replace the cable.

If	Do
the LINK LED indicator is flashing green	You are finished.
the LINK LED indicator is OFF	Refer to the"Replacing the TP-6310 RTM on a Media Server 2020" (page 91) procedure to replace the TP-6310 RTM if a hardware problem is suspected.

4 Contact Nortel Networks technical support if the problem persists.

—End—

Restoring audio files to a Media Server 2000 Series node

In the event that a re-installation of a Media Server 2000 Series 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 Media Server 2000 Series node, contact your Nortel service representative.

Restoring audio files to a Media Server 2000 Series node

Step	Action

At your web browser interface

1 After the re-installation of the Media Server 2000 Series 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 "Enabling provisioning of a Media Server 2000 Series node" (refer to the Media Server 2000 Series Configuration Management document).

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 Media Server 2000 Series node" (refer to the Media Server 2000 Series Configuration Management document).

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.

—End—

Rebooting an APS

This procedure enables you to reboot an APS, as part of APS system recovery. Note that this procedure also causes a reboot of the CS 2000 Management Tool.

Rebooting an APS

Step	Action
	In a telnet connection to the CS 2000 Management Tool
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`
4	Enter the following command: `shutdown -i 6 -y`
5	You have completed this procedure.

—End—

Replacing the Media Server 2010 Chassis

This procedure enables you to replace a Media Server 2010 chassis, either:

- a DC-powered chassis installed in a Service Application Module frame (SAMF), Call Control Frame (CCF), or
- an AC-powered chassis installed in a standard telco rack.

We recommend that you read this procedure in its entirety before performing any of the steps outlined. Before you begin the procedure, arrange all materials, tools, and test equipment at the work location so as to minimize downtime.

WARNING
Static electricity damage

While handling circuit cards or cables, wear a wrist strap connected to a grounding point on the frame. This protects the cards and chassis against damage caused by static electricity.

WARNING
Observe the general safety precautions against personal injury and equipment damage outlined in the regional Installation Safety Manual at all times.

CAUTION
Possible equipment damage

Do not set components on any surface without first placing them in electrostatic bags.

Chassis replacement reasons

The following lists some of the reasons you may need to replace a Media Server 2010 chassis:

- The power supply fails.
- The multiple fans on the module fail.
- The Ethernet Rear Transition Module fails.
- The pins in the mid-plane are bent.
- A short or some other electrical fault occurs within the chassis.

Material requirements

The following is required in order to complete this procedure:

- a Media Server 2010 chassis
- An Installer ToolKit
- A Mounting Kit (part # NTRX5205) if you do not plan to use the existing mounting kit.

Before you begin

If you are replacing the chassis because of a LAN port failure, ensure that you have checked the following before you replace the chassis:

- Ensure that the Ethernet cables are properly connected to the two LAN ports on the chassis and to the Ethernet Routing Switch 8600 . Verify each cable connection using cable tags and job specifications.
- Ensure that there are no network problems causing the MS 2010 to lose connectivity.

Procedure overview

The following is an overview of the Media Server 2010 chassis replacement. These steps are described in detail in the next section.

1) Back up the ini and configuration files and lock the node(s)

2) Remove the MS 2010 chassis from the frame

3) Install the new MS 2010 chassis into the frame

4) Remove the IPM-1610 board from the old chassis

5) Insert the IPM-1610 board into the new chassis

6) Power up the MS 2010 chassis

Replacing the MS 2010 chassis procedure

The following procedures describe how to replace the MS 2010 chassis. If at any point you require assistance, contact Nortel Support.

Backing up the ini and configuration files and lock the node(s)

Step	Action
1	Back up the CMT server to ensure the configuration files are backed up. Refer to the procedure *Performing a backup of oracle data on*

an SPFS-based server in the *ATM/IP Solutions-level Security and Administration* document (NN10402-600).

Note: It is recommended to also make a backup copy of the /etc/bootptab file.

2 Ensure the node(s) is in an unlocked state.

Note: The state of the node (locked or unlocked) is stored in the ini file(s) that you will back up in the next step. Backing up an ini file with the node unlocked allows the node to come back up in an unlocked state.

3 Make a copy of the ini file(s), and make a note of the current software version before removing the board.

Note: If you have a 240-port Media Server 2010 with two 120-port TPMs, back up the ini files from both TPMs.

Refer to the procedures *Backing up the INI file to the IEMS* and *Backing up the INI file to the tftp server* in the *Media Server 2000 series Configuration Management* document (NN10340-511). Both backup procedures are recommended.

4 Perform a graceful lock of the node(s).

CAUTION
If you have a 240-port Media Server 2010, both 120-port TPMs will be taken out of service during this procedure. To ensure no active calls are dropped, make sure both TPMs are locked before proceeding.

Refer to the *Performing a Graceful Lock on a Media Server 2010 series node* procedure in the *Media Server 2000 Series Configuration Management* document (NN10340-511).

—End—

Removing the MS 2010 chassis from the frame

The following describes how to remove the MS2010 chassis from the frame. Use Figure "MS 2010 chassis and mounting kit" (page 74) as a guide. Keep the screws, washers, and mounting brackets that you will remove and place in a safe place for later use.

To remove a DC-powered chassis from a CCF/SAMF frame:

Step	Action
1	If necessary, remove the shear plates from the front and rear of the frame. ***Note:*** This step is only required if the shear plates prevent you from accessing cables or the chassis.
2	Turn the breaker that is powering the chassis to the "OFF" position.
3	Ensure LEDs on the chassis are no longer lit and disconnect the power cables from the MS 2010 chassis.
4	Remove the two Ethernet cables attached to the RTM at the rear of the chassis.
5	Remove the screw securing the ground cable to the chassis. Do not remove the ground cable from the mounting bracket.
6	Optionally, remove the screws and washers securing the rear mounting brackets to the rear frame upright. ***Note:*** It is not necessary to remove the rear mounting brackets from the frame, unless you are replacing the brackets.
7	Remove the screws and washers securing the rear mounting brackets to the front mounting brackets.
8	Remove the screws and washers securing the front mounting brackets to the frame upright.
9	Ease the chassis out of the frame and place on a flat surface.
10	Remove the screws securing the front mounting brackets to the chassis.
11	Ensure the power cables, Ethernet cables, and ground cable are in good condition. If they are not, they should be replaced.

—End—

To remove an AC-powered chassis from a standard telco rack:

Step	Action
1	Turn the power switch on the back of the chassis to the off position ("0").

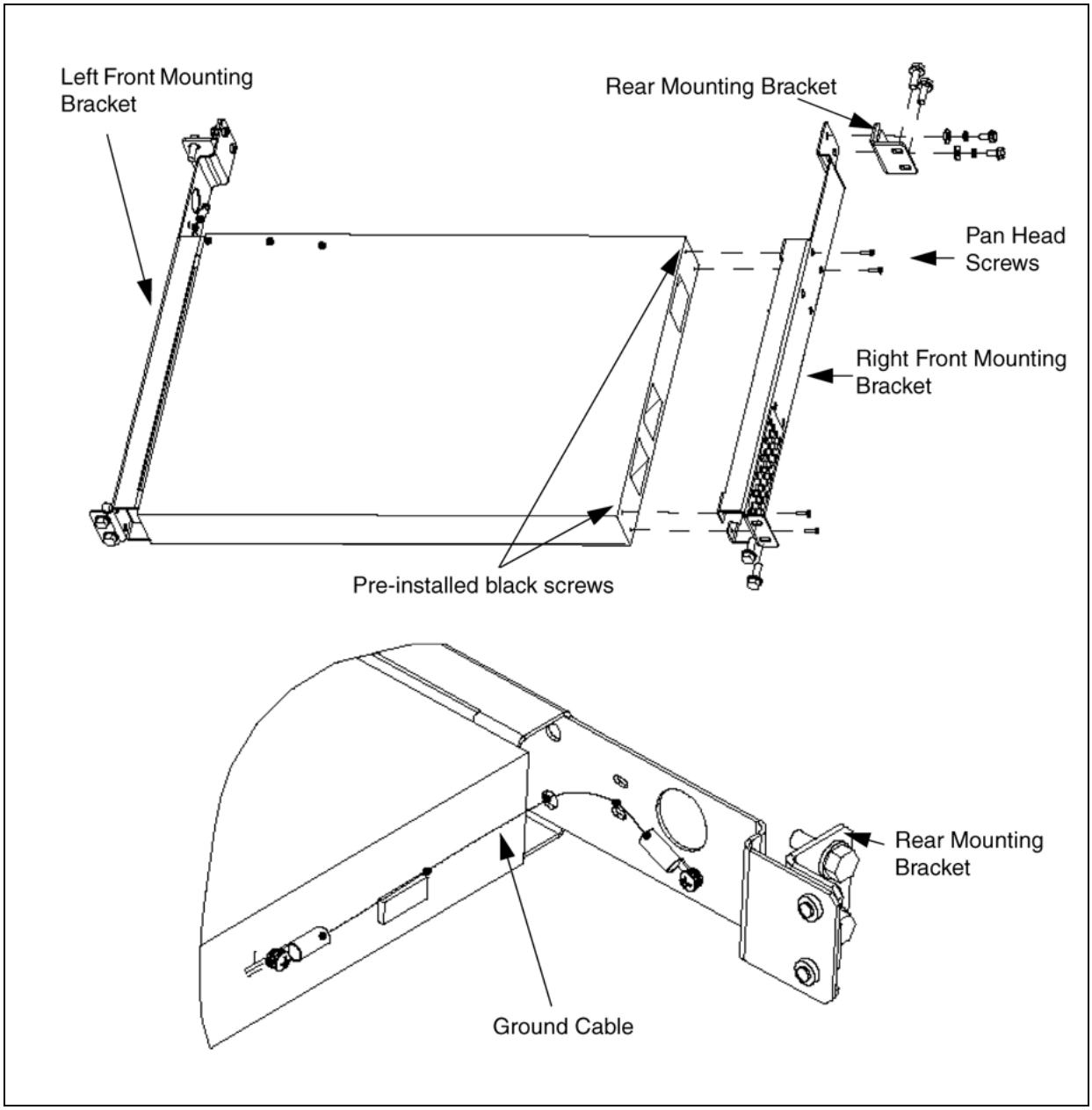
2 Ensure LEDs on the chassis are no longer lit and disconnect the power, Ethernet, and ground cables from the MS 2010 chassis.

3 Remove the chassis from the standard telco rack. Keep the mounting hardware for later use.

4 Ensure the power cables, Ethernet cables, and ground cable are in good condition. If they are not, they should be replaced.

—End—

MS 2010 chassis and mounting kit



Inserting the new MS 2010 chassis into the frame

To insert a DC-powered chassis into a CCF/SAMF frame:

Step	Action
1	Remove the four (4) black screws installed on each side of the new chassis. Discard the screws removed in a safe and proper manner.

2 Secure the front mounting brackets to the new chassis. Four (4) Pan Head Machine screws are required per mounting bracket. See Figure "MS 2010 chassis and mounting kit" (page 74) for details.

3 Insert the chassis into the shelf position and secure the chassis to the frame upright using the screws and washers removed earlier.

4 Secure the rear mounting brackets to the front mounting brackets using the screws and washers removed earlier.

5 If you removed the rear mounting brackets from the frame earlier, secure the rear mounting brackets to the rear frame upright using the screws and washers provided.

6 Remove the ground screw and lock washer installed on the chassis at the ground location. Discard in a safe and proper manner.

7 Secure the Ground Cable from the Left Front Mounting Bracket to the chassis using the screw and washer removed earlier.

8 Verify that the breaker is in the "OFF" position and connect the power cable from the breaker module to the chassis.

9 Connect the two (2) Ethernet cables from the Ethernet Routing Switch 8600 to the rear of the chassis. See Figure "Left side rear view of the MS 2010 chassis" (page 75). Use the cable tags and job specifications to verify each cable connection. Form the cables along the left rear upright to the termination on the chassis.

10 Secure the Ethernet cables to the upright using ty-raps.

—End—

Left side rear view of the MS 2010 chassis

To insert an AC-powered chassis into a standard telco frame:

Step	Action
1	Insert the new chassis into the telco rack in the original location.
2	Use the original mounting hardware to secure the chassis to the rack.
3	Verify that the power switch on the back of the chassis is in the off position ("0") and connect the cables.

—End—

Removing the IPM-1610 board from the old MS 2010 chassis

Step	Action
1	Remove the screws from the plate securing the board to the old chassis.
2	Press the red ejector buttons on the two black ejector/injector latches of the old chassis.
3	Slowly pull on the two ejector/injector latches to unseat the board and ease the board from the slot.

—End—

Inserting the IPM-1610 board into the new MS 2010 chassis

Step	Action
1	Make sure the black ejector/injector latches on the new chassis are in the open (pulled out) position.
2	Hold the IPM-1610 board horizontally to insert it into the new chassis.
3	Align the board with the grooves on each end of the slot and insert the board into the slot of the new chassis. Ease the board all the way into the slot until the ejector/injector latches touch the chassis.
4	Press the two black ejector/injector latches inward, toward the middle of the board, until you hear a click.
5	Attach the screws on the front panel of the board to secure and ground the board to the chassis.
6	Install the shear plates on the front and rear of the frame.

—End—

Powering up the chassis

Step	Action
1	If powering up a DC-powered chassis in a CCF/SAMF frame, turn the breaker that is connected to the chassis to the "ON" position.
2	If powering up an AC-powered chassis, turn the power switch on the back of the chassis to the on position ("1"). When the board powers up, communication begins between the board and the server. The ini and configuration files are automatically restored to the node.
3	Check the activity lights on the front of the Media Server 2010 IPM-1610 board. • The PWR LED is on (right side of the board). • The SWAP READY blue LED does not remain on (right side of the board). • Both ETH LEDs indicate a connection (solid green) with activity (blinking orange). • The red Fail LED is off (left side of the board). • The ACT LED is on (left side of the board). ***Note:*** It may take up to 2 minutes for the ACT LED to illuminate.
4	From the IEMS GUI, ensure that the MS 2010 is in an unlocked state and that the software version remains unchanged. ***Note:*** Ensure that both TPMs are unlocked if you have a 240-port MS 2010.
5	You have completed this procedure.

—End—

Replacing the IPM-1610 board on a Media Server 2010

This procedure enables you to replace an IPM-1610 cPCI VoIP communication board.

The Media Server 2010 components are hot swappable, so they can be removed from the chassis without taking the Media Server 2010 out of service.

WARNING
Static electricity damage
While handling circuit cards or cables, wear a wrist strap connected to a grounding point on the frame. This protects the cards against damage caused by static electricity.

CAUTION
Possible equipment damage
Do not set components on any surface without first placing them in electrostatic bags.

CAUTION
During this procedure, you will execute a hard reset on the Media Server 2010. If you perform a hard reset on a 240-port Media Server 2010, both 120-port TPMs on that Media Server will be taken out of service. Active calls will be dropped! Make sure both TPMs are locked before performing a hard reset.

Replacing the IPM-1610 board

Step	Action
1	Back up the CMT server to ensure the configuration files are backed up. Refer to the procedure *Performing a backup of oracle data on an SPFS-based server*in the *ATM/IP Solutions-level Security and Administration* document (NN10402-600). ***Note:*** It is recommended to also make a backup copy of the /etc/bootptab file.
2	Ensure the node in an unlocked state.

Note: The state of the node (locked or unlocked) is stored in the ini file that you will back up in the next step. Backing up the ini file with the node unlocked allows the node to come up in an unlocked state after replacing the board.

3 Make a copy of the ini file, and make a note of the current software version before replacing the board. Refer to the procedures *Backing up the INI file to the IEMS* and *Backing up the INI file to the tftp server* in the *Media Server 2000 series Configuration Management*document (NN10340-511).

Note: If you have a 240-port Media Server 2010 with two 120-port TPMs, back up the ini files from both TPMs.

4 Perform a graceful lock of the node(s). Refer to the *Performing a Graceful Lock of a Media Server 2000 series node* procedure in the *Media Server 2000 Series Configuration Management* document (NN10340-511).

5 Attach an electrostatic discharge wrist strap to a grounding point on the Media Server 2010 chassis.

6 Remove the screws from the plate securing the board to the chassis.

7 Press the red ejector buttons on the two black ejector/injector latches.

8 Begin to unseat the board by slowly pulling on the two black ejector/injector latches. Do not remove the board.

Wait for the blue SWAP READY LED to light, indicating the board can be removed.

Note: If the blue SWAP READY LED doesn't light after a few minutes, check to see that the board is locked. If the board is locked, you can safely remove the board.

9 Pull on the two ejector/injector latches and ease the board from the slot.

10 Record the MAC address of the board you just removed.

11 Record the MAC address of the replacement board for the BootP/TFTP configuration.

12 Update the MAC address on the server.

a. At your workstation, Telnet to the SPFS-based server.

```
> telnet <IP address>
```

where

< IP address> is the IP address of the server.

b. When prompted, enter your user ID and password.

c. Change to the root user.

```
$ su - root
```

d. When prompted, enter the root password.

e. Access the command line interface.

```
# cli
```

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

f. Enter 2 to access the Configuration menu.

Example response

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Application Configuration
5 - CORBA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)
19 - backup_config (Backup Configuration)
X - exit
Select -
```

g. Enter 11 to access the Bootp Configuration.

Example response

```
Bootp Configuration
1 - bootp_add (Add Entries To The Bootptab File)
2 - bootp_del (Delete Entries From The Bootptab
File)
3 - bootp_list (List Out The Bootptab File)
```

```
4 - bootp_restore (Restore Bootptab File From The
Last Version)
X - exit
select -
```

h. Enter 3 to list the bootp information.

i. Make a copy of the information associated with the IP of the old board you removed.

Example

```
47.142.134.127:\
bf=MS2010.cmp
-fb;/swd/ams/47.142.134.127.ini:\
gw=47.142.134.1:\
hd=/swd/ams:\
ht=ether:\
ha=00908F042B46:\
ip=47.142.134.127:\
sa=47.142.134.124:\
sm=255.255.255.0:\
vm=rfc1048:
```

You are returned to the bootp configuration menu.

> ***Note:*** If you copy and paste the information from the old board (above), do not include the colon backslash (:\) when you paste the text. The colon backslash is not part of the data.

j. Enter 1 to add the new board to the bootp file.

k. Enter the information associated with the old board you removed, with the exception of the MAC address (hardware address [ha]).

For the hardware [ha] address, enter the MAC address of the new replacement board.

> ***Note:*** The information from the old board needs to be associated with the new board. The MAC address is the only thing different, as each board has a unique hardware address.

l. Enter ok to accept the current settings you just entered.

Example response

```
Asking bootpd at pid 24554 to reload /etc/bootptab.
=== "bootp_add" completed successfully
```

m. Enter 3 to list the bootp information.

n. Verify that the new information for the replacement board was entered correctly.

o. If you are adding a second MAC address, repeat steps j through n above.

p. Enter 2 to delete the bootp information for the old board you replaced.

q. Enter the MAC address (hardware address [ha]) of the old board you replaced.

r. Enter ok to accept the current settings you just entered.

Example response

```
in remove
after sed
Asking bootpd at pid 24554 to reload
/etc/bootptab.
=== "bootp_del" completed successfully
```

s. If you are deleting a second MAC address, repeat steps p through r above.

t. Enter X until you have backed out of the CLI tool.

u. Type: exit $

v. Minimize the CMT Telnet session

13 Make sure the black ejector/injector latches are in the open (pulled out) position before inserting the replacement board.

14 Hold the IPM-1610 replacement board horizontally to insert it into the chassis.

15 Align the board with the grooves on each end of the slot and insert the board into the slot. Ease the board all the way into the slot until the ejector/injector latches touch the chassis.

16 Press the two black ejector/injector latches inward, toward the middle of the board, until you hear a click.

17 Attach the screws on the front panel of the board to secure and ground the board to the chassis.

When the board powers up, communication begins between the board and the server. The ini and configuration files are automatically restored to the node.

18 Perform a reset to burn the configuration into Flash memory.

a. At the Windows desktop interface, open a standard web-browser application such as Microsoft Internet Explorer (version 5.0 and higher) or Netscape Navigator (version 7.0 and higher).

b. Enter the IP address of an MS 2000 Series node in the web-browser address field.

c. In the Enter Network Password window that opens, enter the appropriate user name and password, and then click OK.

d. Click the Reset menu button on the left side of the screen.

e. When the Burn configuration into flash memory screen displays, select the Burn radio button

f. Click the Reset button to burn the device configuration to flash memory.

19 If the Media Server 2010 has 240 port capacity (containing two IPM-1610 boards), perform a graceful lock on both nodes. Refer to the *Performing a Graceful Lock of a Media Server 2000 series node* procedure in the *Media Server 2000 Series Configuration Management*document (NN10340-511).

CAUTION
If you perform a hard reset on a 240-port Media Server 2010, both 120-port TPMs are taken out of service. Active calls will be dropped! Make sure both TPMs are locked before proceeding.

20 Perform a hard reset on the Media Server 2010 by cycling power.

a. At the top of the frame, turn the breaker associated with your Media Server 2010 to the off position.

b. After a few seconds, turn the breaker to the on position.

c. Check the activity lights on the front of the Media Server 2010 IPM-1610 board.

- After one to two minutes, the Green LED on the left side of the board is illuminated.
- The red Fail LED is off (left side of the board).
- The blue LED does not remain on (right side of the board).
- The PWR LED is on (right side of the board).
- Both ETH LEDs indicate a connection (solid green) with activity (blinking orange).
- The ACT LED is on (left side of the board).

Note: It may take up to 60 seconds for the ACT LED to illuminate.

21 You have completed this procedure.

—End—

Replacing the TP-6310 or SA-3 board on a Media Server 2020

This procedure enables you to replace an TP-6310 or SA-3 board.

The Media Server 2020 components are hot swappable, so they can be removed from the chassis without taking the Media Server 2020 out of service.

WARNING
Static electricity damage
While handling circuit cards or cables, wear a wrist strap connected to a grounding point on the frame. This protects the cards against damage caused by static electricity.

CAUTION
Possible equipment damage
Do not set components on any surface without first placing them in electrostatic bags.

CAUTION
During this procedure, you will execute a hard reset on the Media Server 2020. A Hard reset will take the Media Server out of service; any active calls will be dropped. Make sure the Media Server is locked before performing a hard reset.

Replacing the TP-6310 or SA-3 board

Step	Action
1	Back up the CMT server to ensure the configuration files are backed up. Refer to the procedure *Performing a backup of oracle data on an SPFS-based server* in the *ATM/IP Solutions-level Security and Administration*document (NN10402-600). ***Note:*** It is recommended to also make a backup copy of the /etc/bootptab file.
2	Ensure the node in an unlocked state. ***Note:*** The state of the node (locked or unlocked) is stored in the ini file that you will back up in the next step. Backing up the ini

file with the node unlocked allows the node to come up in an unlocked state after replacing the board.

3 Make a copy of the ini file, and make a note of the current software version before replacing the board. Refer to the procedures *Backing up the INI file to the IEMS* and *Backing up the INI file to the tftp server* in the *Media Server 2000 series Configuration Management* document (NN10340-511). Both backup procedures are recommended.

Note: If you have a 240-port Media Server 2010 with two 120-port TPMs, back up the ini files from both TPMs.

4 Perform a graceful lock of the node(s). Refer to the *Performing a Graceful Lock of a Media Server 2000 series node* procedure in the *Media Server 2000 Series Configuration Management* document (NN10340-511).

5 Attach an electrostatic discharge wrist strap to a grounding points on the Media Server 2020 chassis.

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. Disconnect all laser sources when working with fiber-optic cables.

CAUTION

Damage to fiber optic cables

Take care when handling fiber optic cables. Do not crimp or bend fiber optic cables.

6 Remove the cables attached to the board.

7 Remove the screws from the brackets securing the board to the chassis.

8 Press the red ejector buttons on the two black ejector/injector latches.

9 Pull on the two ejector/injector latches and ease the board from the slot.

10 Record the MAC address of the board you just removed.

11 Record the MAC address of the replacement board for the BootP/TFTP configuration.

12 Update the MAC address on the server.

a. At your workstation, Telnet to the SPFS-based server.

```
> telnet <IP address>
```

where

< IP address> is the IP address of the server.

b. When prompted, enter your user ID and password.

c. Change to the root user.

```
$ su - root
```

d. When prompted, enter the root password.

e. Access the command line interface.

```
# cli
```

Example response

```
Command Line Interface
1 - View
2 - Configuration
3 - Other
X - exit
select -
```

f. Enter 2 to access the Configuration menu.

Example response

```
Configuration
1 - NTP Configuration
2 - Apache Proxy Configuration
3 - DCE Configuration
4 - OAMP Application Configuration
5 - CORBA Configuration
6 - IP Configuration
7 - DNS Configuration
8 - Syslog Configuration
9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)
19 - backup_config (Backup Configuration)
X - exit
Select -
```

g. Enter 11 to access the Bootp Configuration.

Example response

```
Bootp Configuration
1 - bootp_add (Add Entries To The Bootptab File)
2 - bootp_del (Delete Entries From The Bootptab
File)
3 - bootp_list (List Out The Bootptab File)
4 - bootp_restore (Restore Bootptab File From The
Last Version)
X - exit
select -
```

h. Enter 3 to list the bootp information.

i. Make a copy of the information associated with the IP of the old board you removed.

Example

```
47.142.134.127:\
bf=MS2010.cmp
-fb;/swd/ams/47.142.134.127.ini:\
gw=47.142.134.1:\
hd=/swd/ams:\
ht=ether:\
ha=00908F042B46:\
ip=47.142.134.127:\
sa=47.142.134.124:\
sm=255.255.255.0:\
vm=rfc1048:
```

You are returned to the bootp configuration menu.

Note: If you copy and paste the information from the old board (above), do not include the colon backslash (:\\) when you paste the text. The colon backslash is not part of the data.

j. Enter 1 to add the new board to the bootp file.

k. Enter the information associated with the old board you removed, with the exception of the MAC address (hardware address [ha]).

For the hardware [ha] address, enter the MAC address of the new replacement board.

Note: The information from the old board needs to be associated with the new board. The MAC address is the only thing different, as each board has a unique hardware address.

l. Enter ok to accept the current settings you just entered.

Example response

```
Asking bootpd at pid 24554 to reload /etc/bootptab.
=== "bootp_add" completed successfully
```

m. Enter 3 to list the bootp information.

n. Verify that the new information for the replacement board was entered correctly.

o. If you are adding a second MAC address, repeat steps j through n above.

p. Enter 2 to delete the bootp information for the old board you replaced.

q. Enter the MAC address (hardware address [ha]) of the old board you replaced.

r. Enter ok to accept the current settings you just entered.

Example response

```
in remove
after sed
Asking bootpd at pid 24554 to reload /etc/bootptab.
=== "bootp_del" completed successfully
```

s. If you are deleting a second MAC address, repeat steps p through r above.

t. Enter X until you have backed out of the CLI tool.

u. Type: exit $

v. Minimize the CMT Telnet session

13 Make sure the black ejector/injector latches are in the open (pulled out) position before inserting the replacement board.

14 Hold the TP-6310 replacement board horizontally to insert it into the chassis.

15 Align the board with the grooves on each end of the slot and insert the board into the slot. Ease the board all the way into the slot until the ejector/injector latches touch the chassis.

16 Press the two black ejector/injector latches inward, toward the middle of the board, until you hear a click.

17 Attach the screws on the front panel of the board to secure and ground the board to the chassis.

When the board powers up, communication begins between the board and the server. The ini and configuration files are automatically restored to the node.

Note: Cover all unoccupied slots in the front and rear of the Media Server 2020 chassis with blank panels to maintain internal airflow pressure. See the most current release notes for more information before changing any configuration.

18 Attach the cables to the board.

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. Disconnect all laser sources when working with fiber-optic cables.

CAUTION
Damage to fiber optic cables
Take care when handling fiber optic cables. Do not crimp or bend fiber optic cables.

19 Perform a reset to burn the configuration into Flash memory.

a. At the Windows desktop interface, open a standard web-browser application such as Microsoft Internet Explorer (version 5.0 and higher) or Netscape Navigator (version 7.0 and higher).

b. Enter the IP address of an MS 2000 Series node in the web-browser address field.

c. In the Enter Network Password window that opens, enter the appropriate user name and password, and then click OK.

d. Click the Reset menu button on the left side of the screen.

e. When the Burn configuration into flash memory screen displays, select the Burn radio button

f. Click the Reset button to burn the device configuration to flash memory.

20 You have completed this procedure.

—End—

Replacing the TP-6310 RTM on a Media Server 2020

This procedure enables you to replace an TP-6310 RTM (Rear Transition Module).

The Media Server 2020 components are hot swappable, so they can be removed from the chassis without taking the Media Server 2020 out of service.

WARNING
Static electricity damage
While handling circuit cards or cables, wear a wrist strap connected to a grounding point on the frame. This protects the cards against damage caused by static electricity.

CAUTION
Possible equipment damage
Do not set components on any surface without first placing them in electrostatic bags.

Replacing the TP-6310 RTM

Step	Action
1	Back up the CMT server to ensure the configuration files are backed up. Refer to the procedure *Performing a backup of oracle data on an SPFS-based server* in the *ATM/IP Solutions-level Security and Administration* document (NN10402-600). ***Note:*** It is recommended to also make a backup copy of the /etc/bootptab file.
2	Ensure the node in an unlocked state. ***Note:*** The state of the node (locked or unlocked) is stored in the ini file that you will back up in the next step. Backing up the ini file with the node unlocked allows the node to come up in an unlocked state after replacing the board.
3	Make a copy of the ini file, and make a note of the current software version before replacing the board. Refer to the procedures *Backing up the INI file to the IEMS* and *Backing up the INI file to the tftp server* in the *Media Server 2000 series Configuration*

Management document (NN10340-511). Both backup procedures are recommended.

Note: If you have a 240-port Media Server 2010 with two 120-port TPMs, back up the ini files from both TPMs.

4 Perform a graceful lock of the node(s). Refer to the *Performing a Graceful Lock of a Media Server 2000 series node* procedure in the *Media Server 2000 Series Configuration Management* document (NN10340-511).

5 Attach an electrostatic discharge wrist strap to a grounding points on the Media Server 2020 chassis.

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. Disconnect all laser sources when working with fiber-optic cables.

CAUTION
Damage to fiber optic cables
Take care when handling fiber optic cables. Do not crimp or bend fiber optic cables.

6 Remove the cables attached to the RTM.

7 Remove the screws from the brackets securing the RTM to the chassis.

8 Press the red ejector buttons on the two black ejector/injector latches.

9 Grasp the panel and ease the RTM from the slot.

10 Make sure the black ejector/injector latches are in the open (pulled out) position before inserting the replacement RTM.

11 Hold the replacement RTM horizontally to insert it into the chassis.

12 Align the RTM with the grooves on each end of the slot and insert the RTM into the slot. Ease the RTM all the way into the slot until the ejector/injector latches touch the chassis.

13 Press the two black ejector/injector latches inward, toward the middle of the RTM, until you hear a click.

14 Attach the screws on the front panel of the RTM to secure and ground the RTM to the chassis.

Note: Cover all unoccupied slots in the front and rear of the Media Server 2020 chassis with blank panels to maintain internal airflow pressure. Seethe most current release notes for more information before changing any configuration.

15 Attach the cables to the RTM.

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. Disconnect all laser sources when working with fiber-optic cables.

CAUTION

Damage to fiber optic cables

Take care when handling fiber optic cables. Do not crimp or bend fiber optic cables.

16 Perform a reset to burn the configuration into Flash memory.

a. At the Windows desktop interface, open a standard web-browser application such as Microsoft Internet Explorer (version 5.0 and higher) or Netscape Navigator (version 7.0 and higher).

b. Enter the IP address of an MS 2000 Series node in the web-browser address field.

c. In the Enter Network Password window that opens, enter the appropriate user name and password, and then click OK.

d. Click the Reset menu button on the left side of the screen.

e. When the Burn configuration into flash memory screen displays, select the Burn radio button

f. Click the Reset button to burn the device configuration to flash memory.

17 You have completed this procedure.

—End—

Replacing the PEM on a Media Server 2020

This procedure enables you to replace the PEM (Power Entry Module).

WARNING
Static electricity damage
While handling any Media Server 2020 components or cables, wear a wrist strap connected to a grounding point on the frame. This protects the components against damage caused by static electricity.

CAUTION
Possible equipment damage
Do not set components on any surface without first placing them in electrostatic bags.

Replacing the PEM

Step	Action
1	Back up the CMT server to ensure the configuration files are backed up. Refer to the CS 2000 Core Manager Security and Administration document (NN10170-611).
2	Ensure the node in an unlocked state. ***Note:*** The state of the node (locked or unlocked) is stored in the ini file that you will back up in the next step. Backing up the ini file with the node unlocked allows the node to come up in an unlocked state after replacing the board.
3	Make a copy of the ini file, and make a note of the current software version before replacing the board. Refer to the *Backing up INI files to a Media Server 2000 series node* procedure in the *Media Server 2000 series Configuration Management* document (NN10340-511).
4	Perform a graceful lock of the node(s). Refer to the *Performing a Graceful Lock of a Media Server 2000 series node* procedure in the *Media Server 2000 Series Configuration Management* document (NN10340-511).
5	Attach an electrostatic discharge wrist strap to a grounding points on the Media Server 2020 chassis.

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. Disconnect all laser sources when working with fiber-optic cables.

CAUTION
Damage to fiber optic cables
Take care when handling fiber optic cables.
Do not crimp or bend fiber optic cables.

6 Remove power using the Media Server 2020 breakers.

7 Remove the power cable attached to the PEM.

8 Remove the remaining cables attached to the PEM.

9 Remove the four screws from the plate holding the PEM to the chassis.

10 Press the red ejector button on the black ejector/injector latch.

11 Pull the ejector/injector latch and ease the PEM from the slot.

12 Make sure the black ejector/injector latch is in the open (pulled out) position before inserting the replacement PEM.

13 Hold the replacement PEM horizontally to insert it into the chassis.

14 Insert the PEM into the slot. Ease the board all the way into the slot until the ejector/injector latch touch the chassis.

15 Press the black ejector/injector latch inward until you hear a click.

16 Attach the four screws to the PEM front plate to secure it to the chassis.

Note: Cover all unoccupied slots in the front and rear of the Media Server 2020 chassis with blank panels to maintain internal airflow pressure. Seethe most current release notes for more information before changing any configuration.

17 Attach the cables to the PEM, connecting the power cable last.

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. Disconnect all laser sources when working with fiber-optic cables.

CAUTION
Damage to fiber optic cables
Take care when handling fiber optic cables. Do not crimp or bend fiber optic cables.

18 Apply power using the Media Server 2020 breakers.

19 Perform a reset to burn the configuration into Flash memory.

a. At the Windows desktop interface, open a standard web-browser application such as Microsoft Internet Explorer (version 5.0 and higher) or Netscape Navigator (version 7.0 and higher).

b. Enter the IP address of an MS 2000 Series node in the web-browser address field.

c. In the Enter Network Password window that opens, enter the appropriate user name and password, and then click OK.

d. Click the Reset menu button on the left side of the screen.

e. When the Burn configuration into flash memory screen displays, select the Burn radio button

f. Click the Reset button to burn the device configuration to flash memory.

20 You have completed this procedure.

—End—

Replacing the Media Server 2020 power supply

This procedure enables you to replace the Media Server 2020 power supply.

WARNING
Static electricity damage
While handling any Media Server 2020 components or cables, wear a wrist strap connected to a grounding point on the frame. This protects the components against damage caused by static electricity.

CAUTION
Possible equipment damage
Do not set components on any surface without first placing them in electrostatic bags.

Replacing the power supply

Step	Action
1	Back up the CMT server to ensure the configuration files are backed up. Refer to the CS 2000 Core Manager Security and Administration document (NN10170-611).
2	Ensure the node in an unlocked state. ***Note:*** The state of the node (locked or unlocked) is stored in the ini file that you will back up in the next step. Backing up the ini file with the node unlocked allows the node to come up in an unlocked state after replacing the board.
3	Make a copy of the ini file, and make a note of the current software version before replacing the board. Refer to the *Backing up INI files to a Media Server 2000 series node* procedure in the *Media Server 2000 series Configuration Management* document (NN10340-511).
4	Perform a graceful lock of the node(s). Refer to the *Performing a Graceful Lock of a Media Server 2000 series node* procedure in the *Media Server 2000 Series Configuration Management* document (NN10340-511).
5	Attach an electrostatic discharge wrist strap to a grounding points on the Media Server 2020 chassis.
6	Remove power using the Media Server 2020 breakers.

7 Remove the cables attached to the power supply.

8 Remove the four screws from the plate holding the power supply to the chassis.

9 Press the red ejector button on the black ejector/injector latch.

10 Pull the ejector/injector latch and ease the power supply from the slot.

11 Make sure the black ejector/injector latch is in the open (pulled out) position before inserting the replacement power supply.

12 Hold the replacement power supply horizontally to insert it into the chassis.

13 Insert the power supply into the slot. Ease the board all the way into the slot until the ejector/injector latch touch the chassis.

14 Press the black ejector/injector latch inward until you hear a click.

15 Attach the four screws to the power supply front plate to secure it to the chassis.

Note: Cover all unoccupied slots in the front and rear of the Media Server 2020 chassis with blank panels to maintain internal airflow pressure. Seethe most current release notes for more information before changing any configuration.

16 Attach the cables to the power supply.

17 Apply power using the Media Server 2020 breakers.

18 Perform a reset to burn the configuration into Flash memory.

a. At the Windows desktop interface, open a standard web-browser application such as Microsoft Internet Explorer (version 5.0 and higher) or Netscape Navigator (version 7.0 and higher).

b. Enter the IP address of an MS 2000 Series node in the web-browser address field.

c. In the Enter Network Password window that opens, enter the appropriate user name and password, and then click OK.

d. Click the Reset menu button on the left side of the screen.

e. When the Burn configuration into flash memory screen displays, select the Burn radio button

f. Click the Reset button to burn the device configuration to flash memory.

19 You have completed this procedure.

—End—

Replacing the Fan Tray Unit on a Media Server 2020

This procedure enables you to replace the Fan Tray Unit.

The Media Server 2020 Fan Tray Unit is hot swappable, so it can be removed from the chassis without taking the Media Server 2020 out of service.

Note: Prepare the replacement Fan Tray Unit before removing the faulty Fan Tray Unit. It is imperative the chassis does not remain without the Fan Tray Unit for more than a short period of time.

WARNING
Static electricity damage
While handling any Media Server 2020 components or cables, wear a wrist strap connected to a grounding point on the frame. This protects the components against damage caused by static electricity.

CAUTION
Possible equipment damage
Do not set components on any surface without first placing them in electrostatic bags.

Replacing the fan tray unit

Step	Action
1	Attach an electrostatic discharge wrist strap to a grounding points on the Media Server 2020 chassis.
2	Release the two screws on the top left-hand corner and the bottom left-hand corner of the front panel of the Fan Tray Unit.
3	Pull the Fan Tray Unit's handle outward.
4	Pull the Fan Tray Unit from the slot.
5	Insert the Fan Tray Unit into its slot, until the front panel is flush with the chassis plate.
6	Verify that the fan is functioning correctly by checking to see if the software has reported any fan failure.

Note: You can also check the fans by removing the fan tray and checking that all of the fans are spinning. Then re-insert the fan tray.

7 Fasten the two screws at both the upper and lower ends of the Fan Tray Unit.

8 You have completed this procedure.

—End—

Replacing the fan filter on a Media Server 2020

This procedure enables you to replace the fan filter.

The Media Server 2020 fan filter can be removed from the chassis without taking the Media Server 2020 out of service.

Note: The NEBS compliant air filters need to be cleaned approximately every 90 days. Clean an air filter no more than three times, then replace the air filter.

WARNING
Static electricity damage
While handling any Media Server 2020 components or cables, wear a wrist strap connected to a grounding point on the frame. This protects the components against damage caused by static electricity.

CAUTION
Possible equipment damage
Do not set components on any surface without first placing them in electrostatic bags.

CAUTION
Possible equipment damage
Be sure to prepare all the equipment you need to clean the air filter before removing it from the chassis. It is imperative the chassis not remain without the Fan Tray Unit for long. Be sure to re-insert the Fan Tray Unit while you are cleaning the air filter and re-insert the air filter as soon as it is clean and dry.

Replacing the fan tray unit

Step	Action
1	Attach an electrostatic discharge wrist strap to a grounding points on the Media Server 2020 chassis.
2	Release the two screws on the top left-hand corner and the bottom left-hand corner of the front panel of the Fan Tray Unit.
3	Pull the Fan Tray Unit's handle outward.
4	Pull the Fan Tray Unit from the slot.

5 With your fingertips, grasp the inside of the steel frame of the air filter and pull it out of its slot.

6 Insert the Fan Tray Unit into its slot, until the front panel is flush with the chassis plate.

7 Verify that the fan is functioning correctly by checking to see if the software has reported any fan failure.

Note: You can also check the fans by removing the fan tray and checking that all of the fans are spinning. Then re-insert the fan tray.

8 Clean the air filter using one of the following options.

a. Use a vacuum cleaner to remove accumulated dust and dirt.

b. Use a standard hose nozzle and plain cool water to wash away collected dirt from the air filter. Set the air filter aside until it is completely dry and free of moisture before returning to service.

c. Where stubborn airborne dirt is present, the filter may be dipped in a solution of warm water and mild detergent. Rinse with clear water. Set the air filter aside until it is completely dry and free of moisture before returning to service.

9 Pull the Fan Tray Unit from the chassis.

10 Insert the air filter in its slot with the air direction arrow pointing toward the Fan Tray Unit.

11 Insert the Fan Tray Unit into its slot, until the front panel is flush with the chassis plate.

12 Verify that the fan is functioning correctly by checking to see if the software has reported any fan failure.

Note: You can also check the fans by removing the fan tray and checking that all of the fans are spinning. Then re-insert the fan tray.

13 Fasten the two screws at both the upper and lower ends of the Fan Tray Unit.

14 You have completed this procedure.

—End—

Carrier VoIP

Media Server 2000 Series Fault Management

Publication: NN10328-911
Document status: Standard
Document version: 05.02
Document date: 20 October 2006

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

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