CHAPTER 8

Troubleshooting the Cisco MGC Node

This chapter describes troubleshooting methods for the Cisco Media Gateway Controller (MGC) node. It includes the following sections to help you isolate system problems:

Troubleshooting Overview

This chapter uses the alarms and logs that appear at the Cisco MGC as the basis for isolating problems within the system. You can find a complete listing of alarms and logs in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

Typically, suggested corrective actions start with simple troubleshooting tasks and become increasingly more complex. It is easier, for example, to check LEDs and cabling than to perform a call trace. The suggested corrective actions point to other chapters in this manual, as well as to troubleshooting tools including the Cisco MGC software, the Cisco WAN Manager, and CiscoWorks.

Additionally, you will find examples of troubleshooting typical problems. The examples provide a logical sequence for troubleshooting that you can use as a model.

Note Troubleshooting of the Cisco MGC node should be performed by someone who has been trained in the complexities of the system, who has some experience administering the system, and who understands UNIX at the system administrator level.

The following sections contain various equipment failure scenarios for the solution, including

- Cisco SLT Failure
- Cisco MGC Failure
- Operating System Failure

Cisco SLT Failure

Each Cisco Signaling Link Terminal (SLT) has an Reliable User Datagram Protocol (RUDP)/User Datagram Protocol (UDP)/IP connection to each Cisco MGC for the transfer of Message Transfer Part (MTP) Level 3 (MTP3), ISDN User Part (ISUP), and Transaction Capabilities Application Part (TCAP) information. A Cisco SLT platform failure results in the surviving Cisco SLT platforms taking over the distribution of messages to the active Cisco MGC. Cisco SLT platforms should be provisioned so that half of the platforms can support the entire signaling load. The result is that a Cisco SLT platform failure has no significant effect on call processing.

There are several Cisco SLT failure scenarios to consider:

- An IP link failure between the Cisco SLT and the Cisco MGC, which indicates that it is impossible to transfer MTP3 messages. In this case, MTP Level 2 (MTP2) transmits Status Indication Processor Outage (SIPO) messages to the signaling transfer point (STP) to initiate switchover to another Cisco SLT.
- In the case where MTP2 failed (equivalent to a Cisco SLT failure), no SIPO messages are sent because MTP2 is inoperable. Instead, the mated STP pair detects the failure because of timer expiration or link unavailability and initiates the switchover to another SS7 link.
- If a Cisco MGC fault is detected by a Cisco SLT timer, a coordination mechanism causes SS7 messaging to flow to the newly active (formerly standby) Cisco MGC. The standby Cisco MGC assumes control for all calls in progress and all new calls.

Cisco MGC Failure

Cisco MGC hosts run in active-standby mode. The call-processing application is active on only one Cisco MGC platform at a time, and the application switches to the standby platform when a critical alarm occurs. The result is that Cisco MGC failure and switchover events are invisible to the SS7 signaling network.

Cisco MGC alarms can be configured as minor, major, or critical. Critical alarms are generated whenever any significant failure occurs. Any critical alarm causes a switchover to occur. For example, if the call engine or I/O channel controller (IOCC)-MTP in the active Cisco MGC should fail, there is a disconnection from the process manager and a switchover to the standby Cisco MGC.

Operating System Failure

An operating system (OS) or hardware failure in the active Cisco MGC can also cause a switchover to the standby Cisco MGC. The failover daemon in the standby Cisco MGC detects the failure of the active Cisco MGC and instructs the process manager to initiate a switchover. The standby Cisco MGC then takes over all call-processing functions. The switchover is transparent to all the Cisco SLTs.

Troubleshooting Using Cisco MGC Alarms

The Cisco MGC generates alarms to indicate problems with processes, routes, linksets, signaling links, and bearer channels. The *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide* lists all of the Cisco MGC alarms and logs, and provides descriptions, possible causes, and suggested actions. You can find procedures for alarms that require you to take corrective action in the "Alarm Troubleshooting Procedures" section on page 8-8.

The active alarm log files reside in the /opt/CiscoMGC/var/log directory. These alarm log files are archived based on the criteria set in the dmprSink.dat file. For more information on the dmprSink.dat file, refer to the "Configuring the Data Dumper" section on page A-2.

Troubleshooting using Cisco MGC alarms is described in the following sections:

Retrieving All Active Alarms

To retrieve all active alarms, log in to the active Cisco MGC, start a Man-Machine Language (MML) session, and enter the following command:

rtrv-alms

The system returns a response that shows all active alarms, in a format similar to the following:

```
Media Gateway Controller 2000-02-26 11:41:01
M  RTRV
   "LPC-01: 2000-02-26 09:16:07.806,"
   "LPC-01:ALM=\"SCMGC MTP3 COMM FAIL\",SEV=MJ"
   "IOCM-01: 2000-02-26 09:17:00.690,"
   "IOCM-01:ALM=\"Config Fail\",SEV=MN"
   "MGC1alink2: 2000-02-26 09:17:47.224,ALM=\"SC FAIL\",SEV=MJ"
   "MGC1alink3: 2000-02-26 09:17:47.225,ALM=\"SC FAIL\",SEV=MJ"
   "MGC1alink4: 2000-02-26 09:17:47.226,ALM=\"SC FAIL\",SEV=MJ"
   "MGC2alink1: 2000-02-26 09:17:47.227,ALM=\"SC FAIL\",SEV=MJ"
   "MGC2alink2: 2000-02-26 09:17:47.227,ALM=\"SC FAIL\",SEV=MJ"
   "MGC2alink4: 2000-02-26 09:17:47.229,ALM=\"SC FAIL\",SEV=MJ"
   "dpc5: 2000-02-26 09:17:47.271,ALM=\"PC UNAVAIL\",SEV=MJ"
   "ls3link1: 2000-02-26 09:16:28.174,"
   "ls3link1:ALM=\"Config Fail\",SEV=MN"
   "ls3link1: 2000-02-26 09:18:59.844,ALM=\"SC FAIL\",SEV=MJ"
```

Acknowledging Alarms

Acknowledging an alarm does not clear the alarm. You can still retrieve it with the **rtrv-alm** MML command. To acknowledge an alarm, log in to the active Cisco MGC, start an MML session, and enter the following command:

ack-alm:*comp***:"***alarmCategory***"**

Where:

- *comp*—The MML name of the component. A complete list of components can be found in the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*. You can retrieve a list of system components by entering the **rtrv-cfg:components** MML command.
- *alarmCategory*—MML name of the associated alarm category. The entered name must match exactly the name of the alarm as it is displayed.

For example, to acknowledge a signaling channel fail alarm (SC FAIL) that occurred on the link MGC2alink1, enter the following command:

```
ack-alm:MGC2alink1:"SC FAIL"
```

Clearing Alarms

You can clear an alarm for a affected component. Clearing the alarm removes it and any associated alarms from the internal processes list maintained by the Cisco MGC. To clear an alarm, log in to the active Cisco MGC, start an MML session, and enter the following command:

clr-alm: *comp*:"*alarmCategory*"

Where:

- *comp*—The MML name of the component. A complete list of components can be found in the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*. You can retrieve a list of system components by entering the **rtrv-cfg:components** MML command.
- *alarmCategory*—MML name of the associated alarm category. The entered name must match exactly the name of the alarm as it is displayed.

For example, to acknowledge a signaling channel fail alarm (SC FAIL) that occurred on the link MGC2alink1, enter the following command:

```
clr-alm:MGC2alink1:"SC FAIL"
```

Troubleshooting with System Logs

You can use system logs in conjunction with alarms to provide vital information that you can use in troubleshooting problems. A complete listing of system logs can be found in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

The active system log files reside in the /opt/CiscoMGC/var/log directory. These system log files are archived based on the criteria set in the dmprSink.dat file. For more information on the dmprSink.dat file, refer to the "Configuring the Data Dumper" section on page A-2.

Note Log level and destination can be controlled through settings in the XECfgParm.dat file. Refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide* for more information.

Viewing System Logs

The best method to use to view logs is to use the log viewer, which is part of the Cisco MGC viewer toolkit. The log viewer enables you to search for specific log information, accounts for log rotations, and makes new logs available. The log server is responsible for log rotation. The log server closes the current file, and creates a new file for current logging. The log viewer also has an option for exporting the results of a log file search to a UNIX file.

For more information on using the log viewer, refer to the "Using the Log Viewer" section on page 3-114.

To view a log file when you do not have the Cisco MGC viewer toolkit installed on your system, complete the following steps:

Step 1 Log in to the active Cisco MGC enter the following UNIX command to change to the /opt/CiscoMGC/var/log directory:

cd /opt/CiscoMGC/var/log

Step 2 Enter the following UNIX command to list the available logs:

ls

The system returns a response similar to the following:

```
alm.csv                       platform.log
cdr.bin                       platform_20010516141831.log
meas.csv                      platform_20010517040508.log
mml.log                       platform_20010518040508.log
mml_20010516141831.log        platform_20010519040508.log
mml_20010517040508.log        platform_20010520040508.log
mml_20010518040508.log        platform_20010521040508.log
```

Step 3 To view a specific system log file, enter the following command:

cat *log_file_name* | **more**

Where *log_file_name* is the name of the log file you want to view.

Note Because the log files are very large, use the more parameter to scroll through the file. You might prefer to print the file to find the information you need.

For example, you would enter the following command to view a specific platform log file:

cat platform_20010516141831.log | **more**

The system returns a response similar to the following:

```
Tue May  8 13:35:32:920 2001 | cdrDmpr (PID 15526) <Error>
GEN_ERR_GETCFGPARM: cdrDmprSink::readObj: Failed to get MGC_CDR_NODE_ID for facility *

Tue May  8 13:35:32:921 2001 | cdrDmpr (PID 15526) <Error>
GEN_ERR_GETCFGPARM: cdrDmprSink::readObj: Failed to get MGC_CDR_NODE_ID for facility *

Tue May  8 13:35:32:922 2001 | cdrDmpr (PID 15526) <Error>
GEN_ERR_GETCFGPARM: cdrDmprSink::readObj: Failed to get MGC_CDR_NODE_ID for facility
*Process id is 15517 and thead id is 1 in set the destination

Tue May  8 13:37:13:201 2001 | unknown (PID 15663) <Info>
/tmp/almM_input: installed time handler, hdlrId = 1

Tue May  8 13:37:31:786 2001 | engine (PID 15590) <Error>
CP_ERR_START_GWAY_AUDIT: engProcEvtHdlr::handleGoActiveLocal Failed to start GWAY
auditProcess id is 15508 and thead id is 1 in set the destination
Process id is 15509 and thead id is 1 in set the destination

--More--
```

Understanding System Log Messages

Each system log message uses the following format:

```
Timestamp, Process Name, Process ID, <Log Level>, Log ID:<Message Text>
```

- Timestamp—Displays the date and time on the system when the log message was created, for example, “May 8 01:35:23:047 2001”. The time displayed is down to the millisecond level.
- Process Name—Displays the name of the process that created the log message, for example, “engine”.
- Process ID—Displays the identification number of the process that created the log message, for example, “(PID29974)”.
- Log Level—Displays the severity level of the log message, for example, "Info".
- Log ID—Displays a short, symbolic name for the message, for example, “GEN_ERR_GETCFGPARM:”.
- Message Text—Displays the log message text, for example, “installed time handler, hdlrId = 1”. The message text can take up multiple lines, but is typically only a single line.

Changing the Log Level for Processes

In order to control the types of log messages being written to the system log file, you can use the **set-log** MML command to change the logging level for system processes. The Cisco MGC can generate a large number of logged events, which can result in large numbers of archived system log files in the opt/CiscoMGC/var/spool directory. For example, if the maxTime parameter in the dmprSink.dat file is set to 15 minutes, over 2000 files are created in the opt/CiscoMGC/var/spool directory daily. Therefore, you might want to limit the number of logs being created by changing the logging level of the Cisco MGC software processes.

Table 8-1 lists the logging levels that can be selected for the Cisco MGC software processes without severely degrading system performance.

Table 8-1 Processes and their Lowest Possible Logging Levels

Process	Lowest Logging Level Without Severe Performance Degradation
Engine	Informational (the debug level causes major performance impacts—do not set).
All others	Debug, but only a single process can be in debug at any point in time.

Caution Debug level logging provides extremely verbose output and, if misused, can cause severe system performance degradation.

To change the log level of a single process, log in to the active Cisco MGC, start an MML session, and enter the following command:

set-log:*process_name*:*log_level*[**,confirm**]

Where:

- *process_name*—Name of the process for which you want to change the logging level. Processes are listed in the “Understanding Processes” section on page 3-4.

- *log_level*—Desired logging level. Valid log levels are as follows:
  - CRIT—Critical level messages
  - WARN—Warning condition messages
  - ERR—Error condition messages
  - TRACE—Trace messages
  - INFO—Informational messages
  - DEBUG—Debug-level messages (lowest level). Do not set the process to this logging level unless directed to do so by the Cisco Technical Assistance Center (TAC).
- **confirm**—Used when changing the logging level of a process to debug (DEBUG).

Note Setting the logging level at a given level means that the information related to the levels above the selected level are included. In other words, setting a process to the INFO logging level means that information related to the TRACE, ERR, WARN, and CRIT levels are also displayed. The order of the levels shown above can also be viewed as a verbosity level, in that at CRIT, the least information is logged and at DEBUG the most information logged.

For example, to change the log level of the engine, enter the following command:

```
set-log:eng-01:info
```

To change the log level of all processes, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
set-log:all:log_level
```

Where *log_level* is the desired logging level. Valid log levels are as follows:

- CRIT—Critical level messages
- WARN—Warning condition messages
- ERR—Error condition messages
- TRACE—Trace messages
- INFO—Informational messages

Note Setting the logging level at a given level means that the information related to the levels above the selected level are included. In other words, setting a process to the INFO logging level means that information related to the TRACE, ERR, WARN, and CRIT levels are also displayed. The order of the levels shown above can also be viewed as a verbosity level, in that at CRIT, the least information is logged and at DEBUG the most information logged.

For example, to change the log level of all processes to warning, enter the command:

```
set-log:all:warn
```

Note The logging level of the process manager (PM-01) cannot be set using the **set-log:all:***log_level* MML command. You can only change the logging level of the process manager using the **set-log:pm-01:***log_level* MML command.

Note The **set-log:all:***log_level* MML command cannot be used to set all of the processes to the debug (DEBUG) logging level.

Note The disk monitor (DSKM-01) process does not accept log-level change requests.

Creating a Diagnostics Log File

You can create a diagnostics log file that records the MML commands and responses that you execute. To do this, perform the following steps:

Step 1 Create a diagnostics log file by logging in to the active Cisco MGC, starting an MML session, and entering the following command:

```
diaglog:filename:start
```

Where *filename* is the name of your diagnostics log file. Enter the name only, do not enter a suffix, such as .log.

Step 2 Perform your troubleshooting procedures.

Step 3 When you have finished troubleshooting and you want to view your diagnostics file, enter the following command at the active Cisco MGC:

```
diaglog:filename:stop
```

The file, which is given the name you entered in Step 1, without a suffix, can be found in the $BASEDIR/var/log directory. You can view the file using a text editor, such as vi.

Alarm Troubleshooting Procedures

This section contains alarms that require you to take corrective action. A complete list of alarms, including those that do not require you to take corrective action, can be found in the *Cisco Media Gateway Controller Software Release 7 Messages Reference Guide*.

All Conn Cntl Links Fail

This alarm occurs when the MGCP/SRCP session loses a heartbeat, indicating that the session is down.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the Ethernet interfaces between the Cisco MGC and the associated media gateway are working properly.

Note Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on the media gateway can be found in its associated documentation.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 2.

Note Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an Ethernet interface card on the media gateway can be found in its associated documentation.

Step 2 Verify that the near-end and far-end MGCP/SRCP sessions are operating normally. Refer to the documentation for the affected media gateway for more information on verifying the functioning of the MGCP/SRCP sessions.

If the MGCP/SRCP sessions are not operating normally, return the MGCP/SRCP sessions to normal operations, as described in the documentation for the affected media gateway. Otherwise, proceed to Step 3.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

All C7 IP Links Fail

This alarm occurs when communication is lost to all Cisco SLTs of a single protocol family. This defaults to a critical alarm, and causes an automatic switchover, if a standby Cisco MGC is present.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the Cisco SLTs are operating normally, as described in the "Checking Equipment Status" section on page 6-2 and the "Using the Cisco SLT Operating System to Check Status" section on page 6-4.

Step 2 Verify that the Ethernet interfaces between the Cisco MGC and the Cisco SLTs are working properly.

Note Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on the Cisco SLT can be found in the "Checking Equipment Status" section on page 6-2 and the "Using the Cisco SLT Operating System to Check Status" section on page 6-4.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 2.

Note Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an interface card on the Cisco SLT can be found in the "Replacing Hardware Components" section on page 6-13.

Step 3 Verify that the configuration for your system is correct. To verify the provisioning data for your Cisco MGC, use the **prov-rtrv** MML command, as described in the "Retrieving Provisioning Data" section on page 3-67. To verify the provisioning data for the Cisco SLTs, use show commands, as described in the "Using the Cisco SLT Operating System to Check Status" section on page 6-4.

If the configuration of your Cisco MGC is incorrect, begin a dynamic reconfiguration session, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

If the configuration of your Cisco SLTs is incorrect, modify the provisioning data for your system. Refer to the *Cisco Signaling Link Terminal document* for more information.

If the configuration of both the Cisco MGC and the Cisco SLTs are correct, then proceed to Step 4.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

All ISDN IP Conn Fail

This alarm occurs when communication is lost to all access servers. This alarm causes an automatic switchover, if a standby Cisco MGC is present.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the affected media gateways are operating normally, as described in the associated documentation.

Step 2 Verify that the Ethernet interfaces between the Cisco MGC and the media gateways are working properly.

Note Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on a media gateway can be found in its associated documentation.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 2.

Note Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an Ethernet interface card on the media gateway can be found in its associated documentation.

Step 3 Verify that the configuration for your system is correct. To verify the provisioning data for your Cisco MGC, use the **prov-rtrv** MML command, as described in the "Retrieving Provisioning Data" section on page 3-67. To verify the provisioning data for the media gateways, use show commands, as described in the associated documentation.

If the configuration of your Cisco MGC is incorrect, begin a dynamic reconfiguration session, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

If the configuration of your media gateways is incorrect, modify the provisioning data for the media gateways. Refer to the documentation associated with the media gateway for more information.

If the configuration of the Cisco MGC and the media gateways are correct, then proceed to Step 4.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

ANAL: ALoopCtrExceeded

This alarm occurs when an A-number analysis operation has gone into an infinite loop. The purpose of the alarm is to limit the number of passes spent in the analysis tree to 30.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Validate that there are no infinite loops in the A-number dial plan, as described in the "Verifying a Dial Plan Translation" section on page 3-118.

If there are infinite loops in your A-number dial plan, modify the settings in your A-number dial plan to remove the infinite loops, using the **numan-ed** MML command and reload the dial plan file, using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If their are no infinite loops in your A-number dial plan, then proceed to Step 2.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

ANAL: ATableFail_GetDigTree

This alarm occurs when an invalid path for A-number analysis has been given or that the A-number analysis table is not loaded. The problem is caused when an invalid path has been specified for A-number analysis or the A-number analysis table is not loaded.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: ATableFail_GetDigMod

This alarm occurs when a retrieval of a modification string failed during A-number analysis. The problem occurs when the modification table is not loaded or a pointer to a nonexistent location in the modification table is given.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: ATableFail_GetResult

This alarm occurs when access to the result table failed during A-number analysis. The problem occurs if the result table is not loaded or a pointer to a nonexistent location in the result table is given.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: BLoopCtrExceeded

The alarm occurs when a B-number analysis operation has gone into an infinite loop. The purpose of the alarm is to limit the number of passes spent in the analysis tree to 30.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Validate that there are no infante loops in the B-number dial plan, as described in the "Verifying a Dial Plan Translation" section on page 3-118.

If there are infinite loops in your B-number dial plan, modify the settings in your B-number dial plan to remove the infinite loops, using the **numan-ed** MML command and reload the dial plan file, using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If their are no infinite loops in your B-number dial plan, then proceed to Step 2.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

ANAL: BNum_GetFail_SrvcTbl

This alarm occurs during B-number analysis when a screening result is encountered and an attempt to read the service table to determine the name of the service performing the screening fails. This is due to corruption of either the result table or the service table.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: BNum_MdfyBFail_ AnnounceID

This alarm occurs during B-number analysis when an announcement result is encountered and analysis is unable to replace the last 4 digits of the B-number with the announcement ID. This is commonly caused by an out-of-range announcement Id (it should be 0-9999) or a B-number less than 4 digits long.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that all of the configured announcement IDs are within the range 0 through 9999, using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If any of the announcement IDs are outside of the range, modify its value using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

Step 2 Verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: BTableFail_GetDigTree

This alarm occurs when an invalid path for B-number analysis has been given or that the B-number analysis table is not loaded. The problem occurs when an invalid path has been specified for B-number analysis or the B-number analysis table is not loaded.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: BTableFail_GetDigMod

This alarm occurs when retrieval of a modification string failed during B-number analysis. The problem occurs if the modification table is not loaded or a pointer to a nonexistent location in the modification table is given.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: BTableFail_GetResult

This alarm occurs when access to the result table failed during B-number analysis. The problem occurs if the result table is not loaded or a pointer to a nonexistent location in the result table is given.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: Cause_GetFail_CauseTbl

This alarm occurs during cause analysis when the cause table is unreadable. This can be due to the cause table being corrupted, a failure in the underlying software, or the cause table being built without all the existing call context cause values.

Corrective Action

Step 1 Verify that the associated cause table contains all of the existing call context cause values, using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If the cause table is incomplete, modify its value using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

Step 2 Verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL:Cause_GetFail_DigModTbl

This alarm occurs during cause analysis when a B-number modification result is encountered and the digit modification string is unreadable. This can be due to the digit modification table being corrupted or an incorrect digit modification index being stored in the B-number modification result's data.

Corrective Action

Step 1 Verify that the associated B-number digit modification table is correct, using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If the information in the B-number digit modification table is incorrect, modify its value using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

Step 2 Verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: Cause_GetFail_InvldRsltType

This alarm occurs during cause analysis when a result is encountered that is not supported in cause analysis. This is due to corruption of the cause or location tables or the result table.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL:Cause_GetFail_LocTbl

This alarm occurs during cause analysis when the location table is unreadable. This can be due to the location table being corrupted, a failure in the underlying software, or the location table not being fully populated with all possible references from the cause table.

Corrective Action

Step 1 Verify that the associated location table contains all of the possible references from the cause table, using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If the location table does not contain all of the references, modify its value using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

Step 2 Verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL:Cause_GetFail_RsltTbl

This alarm occurs during cause analysis when the result table is unreadable. This can be due to the result table being corrupted, a failure in the underlying software, or the result table not being fully populated with all possible references from the cause and location tables.

Corrective Action

Step 1 Verify that the associated result table contains all of the possible references from the cause and location tables, using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If the result table does not contain all of the references, modify its value using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

Step 2 Verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL:Cause_InvldRslts_CauseTbl

This alarm occurs when cause analysis successfully reads the cause table but the value returned is logically invalid. Cause analysis gets two values from the cause table: an immediate result index and a location index. The immediate result index indicates that analysis should start reading results now, but the location index indicates that another table read is required to find the correct result table index. These results are logically incompatible. Most likely this results from a failure of the underlying software or a corruption of the cause table.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: Cause_MdfyBFail_AnnounceID

This alarm occurs during cause analysis when an announcement result is encountered and analysis is unable to replace the last 4 digits of the B-number with the announcement ID. This is commonly caused by an out-of-range announcement ID (it should be 0 to 9999) or a B-number less than 4 digits long.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the affected announcement ID is within the range 0 through 9999, using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If the announcement ID is outside of the range, modify its value using the **numan-ed** MML command and proceed to Step 2. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

Step 2 Verify that the affected B-number is at least 4 digits long, using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If the affected B-number is less than 4 digits long, modify its value using the **numan-ed** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 3.

Step 3 If you modified your dial plan, reload your dial plan file using the **chg-dpl** MML command. Otherwise, proceed to Step 4.

Step 4 Verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: Cause_MdfyBFail_AppPtInvld

This alarm occurs during cause analysis when a B-number modification result is encountered and the application point (where digits are inserted) specified is beyond the end of the digit string. This is caused by an incorrect application point being specified in the result data, a corrupt result table, or incorrectly constructed cause analysis values.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the specified application points in the result data is correct, using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If any of the application points are incorrect, modify their value using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

Step 2 Verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: Cause_Rte_LoopDetected

This alarm occurs during cause analysis when a route or announcement result is encountered. In these cases, the indicated route identifier is checked against a list of previously provided results. If a match is found, this alarm is raised and an error is returned to call processing. This is done to prevent calls from endlessly routing to a single route or series of routes infinitely due to cause analysis interactions.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: CustId/StartIdx Missing

This alarm occurs when the property CustGrpId or BOrigStartIndex are not present on the associated SS7 signaling service or trunk group. These are required to find the correct place to begin analysis.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the values of CustGrpId and BOrigStartIndex properties for the associated SS7 signaling service or trunk group are correct by logging in to the active Cisco MGC, starting an MML session, and entering the following command:

prov-rtrv:*component***:name="***comp_name***"**

Where:

- *component*—MML component type name for the SS7 signaling service or trunk group properties. Enter one of the following:
  - sigsvcprop—Component type for SS7 signaling service properties.
  - trnkgrpprop—Component type for trunk group properties.
- *comp_name*—MML name for the affected SS7 signaling service or trunk group.

For example, if you wanted to verify the properties for an SS7 signaling service called **ss7svc1**, you would enter the following command:

```
prov-rtrv:sigsvcprop:name="ss7svc1"
```

If your system has been properly configured for dial plan use, the system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-01 10:09:47
M  RTRV
   "session=active:sigsvcprop"
   /*
adjDestinations = 16
AlarmCarrier = 0
BOrigStartIndex = 0
BothwayWorking = 1
BTermStartIndex = 1
CctGrpCarrier = 2
CGBA2 = 0
CircHopCount = 0
CLIPEss = 0
CotInTone = 2010
CotOutTone = 2010
CotPercentage = 0
CustGrpId=2222
dialogRange = 0
ExtCOT = Loop
ForwardCLIinIAM = 1
ForwardSegmentedNEED = 1
GLARE = 0
GRA2 = 0
GRSEnabled = false
InternationalPrefix = 0
layerRetries = 2
layerTimer = 10
MaxACL = 3
maxMessageLength = 250
mtp3Queue = 1024
NationalPrefix = 0
NatureOfAddrHandling = 0
Normalization = 0
OMaxDigits = 24
OMinDigits = 0
OOverlap = 0
OwnClli = na
RedirMax = 3
ReleaseMode = Async
restartTimer = 10
RoutePref = 0
sendAfterRestart = 16
slsTimer = 300
srtTimer = 300
sstTimer = 300
standard = ANSI92
SwitchID = 0
TMaxDigits = 24
TMinDigits = 0
TOverlap = 0
variant = SS7-ANSI
VOIPPrefix = 0
```

Step 2 If you need to modify your settings, start a provisioning session as described in the "Starting a Provisioning Session" section on page 3-63.

Step 3 If the BOrigStartIndex property is not set to 1, enter the following command:

prov-ed:*component***:name="***comp_name***",BOrigStartIndex=1**

Where:

- *component*—MML component type name for the SS7 signaling service or trunk group properties. Enter one of the following:
  - ss7path—Component type for SS7 signaling services.
  - trnkgrp—Component type for trunk groups.
- *comp_name*—MML name for the affected SS7 signaling service or trunk group.

Step 4 If the CustGrpId property is missing from the affected SS7 signaling service or trunk group, enter the following command:

Note If you are modifying the CustGrpId value for an SS7 signaling service, you must set that SS7 signaling service to the out-of-service administrative state, as described in the "Setting the Administrative State" section on page 8-70. Once you have entered the CustGrpId value, you can return the SS7 signaling service to the in-service administrative state. You do not have to change the administrative state when you are

prov-ed:*component***:name="***comp_name***",CustGrpId=***number*

Where:

- *component*—MML component type name for the SS7 signaling service or trunk group properties. Enter one of the following:
  - ss7path—Component type for SS7 signaling services.
  - trnkgrp—Component type for trunk groups.
- *comp_name*—MML name for the SS7 signaling service or trunk group on which you are mapping the internal maximum ACL value to the value expected by the adjacent signaling point.
- *number*—Customer group ID number that is associated with your dial plan.

Step 5 Save and activate your provisioning session as described in the "Saving and Activating your Provisioning Changes" section on page 3-64.

ANAL: Data Failure Rcvd

This alarm occurs when during analysis, a data failure is found in the external routing engine.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: InvalidtrkGrpType

This alarm occurs when the analysis module has not provided a valid trunk group type. The problem occurs if the route analysis table specifies an invalid trunk group type.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Display the valid trunk group types using the **prov-rtrv** MML command as described in the "Retrieving Provisioning Data" section on page 3-67.

Step 2 Correct the invalid trunk group type in the route analysis table using the **numan-ed** MML command and reload the dial plan using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

ANAL: Prof_GetFail_DigModTbl

This alarm occurs during profile analysis when a B-number modification result is encountered and the digit modification string is unreadable. This can be due to the digit modification table being corrupted or an incorrect digit modification index being stored in the B-number modification result's data.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: Prof_GetFail_InvldRslt

This alarm occurs during profile analysis when a result is encountered that is not supported in profile analysis. This is due to corruption of either the NOA or NPI tables or the result table.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: Prof_GetFail_NOATbl

This alarm occurs during profile analysis when the NOA table is unreadable. This can be due to the NOA table being corrupted, a failure in the underlying software, or the NOA table being built without all the existing call context NOA values.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the NOA table uses all of the existing call context NOA values using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If the NOA table is missing any of the existing call context NOA values, add them using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

Step 2 Verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: Prof_GetFail_NPITbl

This alarm occurs during profile analysis when the NPI table is unreadable. This can be due to the NPI table being corrupted, a failure in the underlying software, or the NPI table not being fully populated with all the possible references from the NOA table.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the NPI table uses all of the possible references from the NOA table using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If the NPI table is missing any of the references from the NOA table, add them using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

Step 2 Verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: Prof_GetFail_RsltTbl

This alarm occurs during profile analysis when the result table is unreadable. This can be due to the result table being corrupted, a failure in the underlying software, or the result table not being fully populated with all the possible references from the NOA or NPI tables.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the result table uses all of the possible references from the NOA and NPI tables using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If the result table is missing any of the references from the NOA and NPI tables, add them using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

Step 2 Verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: Prof_InvldNPAValue

This alarm occurs during profile analysis when a 7-digit B-number is encountered and the NPA property is set against the originating trunk group. An NPA string of more or less than 3 characters is invalid. This is most likely caused by data corruption.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the NPA values have been properly provisioned for the trunk group using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If the NPA values are incorrect, modify them using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

Step 2 Verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: Prof_InvRslts_NOATbl

This alarm occurs when profile analysis successfully reads the NOA table but the value returned is logically invalid. Profile analysis gets two values from the NOA table: an immediate result index and an NPI index. An immediate result index indicates that analysis should start reading results now but an NPI index indicates that another table read is required to find the correct result table index. These results are logically incompatible. Most likely this results from a failure of the underlying software or a corruption of the NOA table.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: Prof_MdfyBFail_AppPtInvld

This alarm occurs during profile analysis when a B-number modification result is encountered and the specified application point (where digits are inserted) is beyond the end of the digit string. This is caused by an incorrect application point being specified in the result data, a corrupt result table, or incorrectly constructed Profile analysis values.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the specified application points in the result data is correct, using the **numan-rtrv** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If any of the application points are incorrect, modify their value using the **numan-ed** MML command and reload the dial plan file using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information. Otherwise, proceed to Step 2.

Step 2 Verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: RteStartIndexInvalid

This alarm occurs when the start index for the route analysis table is invalid.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the data for the provisioned route lists is correct by logging in to the active Cisco MGC, starting an MML session, and entering the following command:

```
prov-rtrv:rtlist:"all"
```

Step 2 If their is incorrect data for the route lists, correct it by using the **prov-ed** MML command. Otherwise, proceed to Step 3. Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information on provisioning route lists.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

ANAL: RteTableFail_GetRteList

This alarm occurs when access to the route list failed. The problem occurs if the index to the route list is not valid or if the route list is not loaded.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: RteTableFail_GetTrkAttrdata

This alarm occurs when access to the trunk group attribute data table failed. The problem occurs if the index to the trunk group attribute data table is not valid or if the table is not loaded.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: RteTableFail_GetTrkGrpdata

This alarm occurs when access to the trunk group data failed. The problem occurs if the index to the trunk group data is not valid or if the trunk group data table is not loaded.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: RteTableFail_GetTrunkList

This alarm occurs when access to the trunk group list failed. The problem occurs if the index to the trunk group list is not valid or if the trunk group list is not loaded.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

ANAL: TrunkGrpRsltCtrExceeded

This alarm occurs when the analysis module has provided the maximum number of candidate trunk groups allowed. The maximum number is 20. The purpose of the alarm is to limit the time spent searching for candidate trunk groups.

Corrective Action

To correct the problem identified by this alarm, verify that the dial plan file was loaded correctly, using the procedure described in "Verifying Proper Loading of a Dial Plan" section on page 8-69.

C7LNK ALGNMT LOST

This alarm occurs when the MTP2 for the C7 link between a Cisco SLT and an associated APC has lost alignment.

Corrective Action

To correct the problem identified by this alarm, use the diagnostics on the affected Cisco SLT to determine why the link has lost alignment, as described in the "Verifying the Link Alignment Status" section on page B-6.

C7DPC CONGESTION

This alarm occurs when a link in a signaling route towards a given DPC becomes congested or when a DPC is congested and has sent a congestion indication to the Cisco MGC.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify the status of the links associated with the affected DPC, as described in the "Retrieving the Service State of a Linkset" section on page 3-51.

If none of the links are out-of-service, this alarm has occurred because the DPC is congested. In this instance, corrective action is not necessary, and you must wait for the congestion condition to clear.

If any of the links are out-of-service, proceed to Step 2.

Step 2 Return the out-of-service links to service, as described in the "Setting the Service State of a Link or Linkset" section on page 8-60.

If that does not resolve the problem, proceed to Step 3.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

C7LNK CONGESTION

This alarm occurs when that the SS7 MTP2 link has encountered congestion such that it cannot receive any more messages. This alarm applies only to SS7 links that are terminated on I/O cards.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Reengineer your call traffic to reduce the number of calls coming to the affected link. If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 2.

Step 2 Add more links to the linkset associated with the affected link. To do this, you must either add additional I/O cards, or switch to Cisco SLTs. For more information on installing the I/O cards or Cisco SLTs, refer to the *Cisco Media Gateway Controller Hardware Installation Guide*. For more information on provisioning your new links, refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*.

If that does not resolve the problem, proceed to Step 3.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

C7LNK INHIBIT

This alarm occurs when a C7 link has been inhibited for maintenance.

Corrective Action

To correct the problem identified by this alarm, uninhibit the specified C7 link, as described in the "Setting the Service State of a Link or Linkset" section on page 8-60, when the maintenance is complete.

Config Fail

This alarm occurs when the configuration has failed.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Search the active system log file, as described in the "Viewing System Logs" section on page 8-4, for logs that indicate errors in the content of your provisioning data.

If there are no logs that indicate errors in the content of your provisioning data, proceed to Step 2.

If there are logs that indicate errors in the content of your provisioning data, start a dynamic reconfiguration session to change the settings for the component(s) identified in the log message(s), as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

If that corrects the problem, the procedure is complete. Otherwise, proceed to Step 2.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

DISK

This alarm occurs when the system disk is running out of space.

Corrective Action

To correct the problem identified by this alarm, delete any unnecessary files from your Cisco MGC, as described in the "Deleting Unnecessary Files to Increase Available Disk Space" section on page 8-112.

Ext Node Interface Fail

This alarm is generated when an SRCP session loses heartbeats with the remote gateway, indicating that the link to the gateway is down.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the remote media gateway is up and running by checking its LEDs. Refer to the documentation associated with the remote media gateway for more information on verifying its functioning using the LEDs.

If the remote gateway is not up and working, restore it to service using the procedures found in the documentation associated with the remote media gateway.

If the remote gateway is up and running, proceed to Step 2.

Step 2 Verify that the Ethernet interfaces between the Cisco MGC and the associated media gateway are working properly.

Note Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on the media gateway can be found in its associated documentation.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 3.

Note Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an Ethernet interface card on the media gateway can be found in its associated documentation.

Step 3 Verify that the near-end and far-end SRCP sessions are operating normally.

Step 4 If that does not resolve the problem, contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the .

FAIL

This alarm occurs when the component referenced in the alarm has failed. The failure may be service affecting, in which case other alarms are raised.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 If the component identified in the alarm text is in the system software, contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the .

If the component identified in the alarm text is a piece of system hardware, you should restart the component's software. Procedures for stopping and restarting the software of any of the elements of the Cisco MGC node can be found in Chapter 2, "Cisco MGC Node Component Startup and Shutdown Procedures". If that does not resolve the problem, proceed to Step 2.

Step 2 Replace the component identified in the alarm text. Procedures for replacing Cisco MGC host hardware can be found in the associated Sun Microsystems documentation. Procedures for replacing Cisco SLT hardware can be found in "Replacing a Cisco SLT" section on page 6-6. Procedures for replacing Cisco Catalyst 5500 MSR hardware can be found in "Replacing Hardware Components" section on page 7-5.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the .

FailoverPeerLost

This alarm occurs when the failover daemon on the standby Cisco MGC is not reachable.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the Ethernet interfaces between the active and standby Cisco MGCs and the Cisco Catalyst 5500 MSRs are working properly.

Note Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on the Cisco Catalyst 5500 MSRs can be found in the "Checking Equipment Status" section on page 7-1.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 2.

Note Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an Ethernet interface card on the Cisco Catalyst 5500 MSRs can be found in the "Replacing Hardware Components" section on page 7-5.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

FailoverPeerOOS

This alarm occurs when the failover daemon goes out-of-service in the standby Cisco MGC.

Corrective Action

To correct the problem identified by this alarm, check the alarms on the standby Cisco MGC, using the procedure in the "Retrieving All Active Alarms" section on page 8-3, and resolve those alarms.

Gen Fail

This alarm occurs when a failure has occurred due to resource exhaustion or configuration problems, including:

- Memory exhaustion.
- Queue overflow.
- Message congestion.
- IPC file cannot be opened.
- A timer has expired.

Log messages in the active system log file indicate the nature of the failure. For the majority of the failures, this alarm is informational and no user action is required. When this alarm is generated because an IPC file cannot be opened, you must take corrective action.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Search the active system log file, as described in the "Viewing System Logs" section on page 8-4, for logs that indicate that an IPC file cannot be opened.

If there are no logs that indicate that an IPC file cannot be opened, no further action is required.

If there are logs that indicate that an IPC file cannot be opened, proceed to Step 2.

Step 2 Shut down the Cisco MGC software on your standby Cisco MGC, as described in the "Shutting Down the Cisco MGC Software Manually" section on page 2-4.

Step 3 Restart the Cisco MGC software on your standby Cisco MGC, as described in the "Starting the Cisco MGC Software" section on page 2-2.

Step 4 Perform a manual switchover, as described in the "Performing a Manual Switchover" section on page 3-80.

Step 5 Shut down the Cisco MGC software on your newly standby Cisco MGC, as described in the "Shutting Down the Cisco MGC Software Manually" section on page 2-4.

Step 6 Restart the Cisco MGC software on your newly standby Cisco MGC, as described in the "Starting the Cisco MGC Software" section on page 2-2.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 7.

Step 7 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

IP CONNECTION FAILED

This alarm occurs when the Cisco MGC loses network (IP) connectivity to a Cisco SLT. This alarm is generated for each SS7 link associated with the affected Cisco SLT.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the affected Cisco SLT is up and running by performing the procedures in the "Checking Equipment Status" section on page 6-2.

If the affected Cisco SLT is not up and running, start it using the procedure in the "Cisco Signaling Link Terminal Startup Procedure" section on page 2-3. If this does not resolve the problem, replace the affected Cisco SLT as described in the "Replacing a Cisco SLT" section on page 6-6.

If the affected Cisco SLT is up and running, proceed to Step 2.

Step 2 Verify that the Ethernet interfaces between the Cisco MGC and the affected Cisco SLT are working properly.

> **Note** Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on the Cisco SLT can be found in the "Checking Equipment Status" section on page 6-2.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 3.

Note Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing components on the Cisco SLT can be found in the "Replacing Hardware Components" section on page 6-13.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

IP RTE CONF FAIL

This alarm occurs when a signaling channel is not using the route that it is was configured to use.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the provisioned settings for the identified IP route are correct, using the **prov-rtrv** MML command, as described in the "Retrieving Provisioning Data" section on page 3-67.

If the provisioned settings for your IP route are correct, proceed to Step 2.

If the provisioned settings for your IP route are incorrect, start a dynamic reconfiguration session to change the settings, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

IP RTE FAIL

This alarm occurs when a signaling channel that is provisioned with a next hop address if the system failed to add the required route.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the provisioned settings for the identified IP route are correct, using the **prov-rtrv** MML command, as described in the "Retrieving Provisioning Data" section on page 3-67.

If the provisioned settings for your IP route are correct, proceed to Step 2.

If the provisioned settings for your IP route are incorrect, start a dynamic reconfiguration session to change the settings, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

ISUP: COT Failure

This alarm occurs when a COT message was received indicating a failed continuity test.

Corrective Action

To correct the problem identified by this alarm, run a manual COT test, as described in the "Running a Manual Continuity Test" section on page 8-96.

LIF BER

This alarm occurs when an excessive bit error ratio is detected from a frame alignment signal. This might be caused by any source of electrical noise; for example, degraded transmission line, degraded line connectors, high-voltage electrical source located in proximity of line.

Corrective Action

To correct the problem identified by this alarm, isolate the source by testing the connections and transmission line for the identified component. When you have identified the source, resolve as necessary.

LIF FAIL

This alarm occurs when line interface (LIF) has failed. All physical lines to the Cisco MGC can raise this alarm.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the provisioned settings for the identified line interface are correct, using the **prov-rtrv** MML command, as described in the "Retrieving Provisioning Data" section on page 3-67.

If the provisioned settings for your line interface are correct, proceed to Step 4.

If the provisioned settings for your line interface are incorrect, proceed to Step 2.

Step 2 Place the identified line interface in the out-of-service administrative state, as described in the "Setting the Administrative State" section on page 8-70.

Start a dynamic reconfiguration session to change the settings, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

Step 3 Place the identified line interface in the in-service administrative state, as described in the "Setting the Administrative State" section on page 8-70.

If that does not resolve the problem, proceed to Step 4.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

LIF LOF

This alarm occurs when a loss of T1/E1 framing has been detected on the LIF. The physical line has a signal but has lost the framing pattern.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the framing format used on the port matches the framing format used on the line.

If the framing formats are different, change the framing format on the port to the other framing format. Otherwise, proceed to Step 2. If the alarm does not clear, proceed to Step 2.

Step 2 Change the line build-out setting. If the alarm does not clear, proceed to Step 3.

Step 3 Open the statistics report for the port and look for evidence of a bad line. Bursts of Latvia could indicate a timing problem.

If you find evidence of a bad line, perform loopback tests on the line to isolate the problem. Otherwise, proceed to Step 4. Once you have isolated the problem, resolve as necessary. If the alarm does not clear, proceed to Step 4.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

LIF LOS

This alarm occurs when the transmitted signal is lost in the T1/E1. The receiving end does not receive the signal. The physical line might have a break in it.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the cable connections are correct between the interface port and your service provider's equipment or T1/E1 terminal equipment.

If the cable was built on-site, check the cable connectors. A reversal of transmit and receive pairs or an open receive pair can cause this condition.

If the cable connections appear correct, then proceed to Step 2.

Step 2 Check your T1/E1 equipment, or ask your service provider to test your T1/E1 line and correct any errors found.

If the alarm does not clear, then proceed to Step 2.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

LIF SES

This alarm occurs when the LIF is automatically set to the out-of-service state because of severely errored seconds. The TDM line has a large amount of noise, causing an error rate greater than 10-3. Framing and signal are within tolerance. This indicates a degraded but functioning line.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the terminations and cabling for the LIF are working. If you can identify the source of the problem, resolve as necessary. Otherwise, proceed to Step 2.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

LIF YELLOW

This alarm occurs when the receiving end is reporting a loss of the transmitted signal. This is reported for T1/E1 facilities only.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Connect an external loopback cable to the affected port.

If no alarms are produced, proceed to Step 2

If alarms are produced, the port is causing the error. Replace the hardware component associated with the port. Refer to the associated media gateway documentation for more information on replacing the component.

Step 2 Check for an open, short, or wiring error in the cable between the network interface port and your service provider's network interface unit T1/E1 terminal equipment. An open transmit pair can cause this condition.

If you find a wiring problem, replace the cable. If that does not clear the alarm, proceed to Step 3.

If you do not find a wiring problem, then proceed to Step 3.

Step 3 If your port is configured to use D4 framing, the port may intermittently detect yellow alarms because the packet data may contain the pattern that is used to signal yellow alarm in D4 framing. If it is possible, switch to ESF framing in both the terminal equipment and the line equipment.

If that does not clear the alarm, proceed to Step 4.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

LIF: IDLE CHANGE

This alarm occurs when the physical line has failed because its cable is broken or not plugged in. This is reported for V.35 facilities only.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the V.35 cables between the port and the far-end are working correctly.

If you find a problem with a V.35 cable, replace the cable. If that does not correct the problem, proceed to Step 2.

If you do not find a problem with the V.35 cables, proceed to Step 2.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

LIF: LOST CD

This alarm occurs when the physical line has failed because its cable is broken or not plugged in. This is reported for V.35 facilities only.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the V.35 cables between the port and the far-end are working correctly.

If you find a problem with a V.35 cable, replace the cable. If that does not correct the problem, proceed to Step 2.

If you do not find a problem with the V.35 cables, proceed to Step 2.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

LIF: LOST CTS

This alarm occurs when the physical line has failed because its cable is broken or not plugged in. This is reported for V.35 facilities only.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the V.35 cables between the port and the far-end are working correctly.

If you find a problem with a V.35 cable, replace the cable. If that does not correct the problem, proceed to Step 2.

If you do not find a problem with the V.35 cables, proceed to Step 2.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

MMDB: Database unavailable

This alarm occurs when the main memory database is currently unavailable to provide any services. Recovery is attempted and the alarm clears when or if the database becomes available.

Corrective Action

To correct the problem identified by this alarm, delete any unnecessary files from your Cisco MGC, as described in the "Deleting Unnecessary Files to Increase Available Disk Space" section on page 8-112.

MMDB: Database cause failover

This alarm occurs when the main memory database is currently unavailable on a redundant system and is indicating that the system should failover. Recovery is attempted and the alarm clears when or if the database becomes available.

Corrective Action

To correct the problem identified by this alarm, delete any unnecessary files from your standby Cisco MGC, as described in the "Deleting Unnecessary Files to Increase Available Disk Space" section on page 8-112.

MMDB: Database nearly full

This alarm occurs when the main memory database has detected that allocated resources for data storage are nearly all utilized.

Corrective Action

To correct the problem identified by this alarm, delete any unnecessary files from your Cisco MGC, as described in the "Deleting Unnecessary Files to Increase Available Disk Space" section on page 8-112.

NAS: AuditResponse Failure

This alarm occurs when the identified media gateway fails to send a RESYNC RESP message back to the Cisco MGC within the audit time interval.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the affected media gateway is in the in-service state, as described in the "Retrieving Signaling Channel Attributes" section on page 3-48 and the "Verifying the Status of all Destinations" section on page 3-8.

If the affected media gateway is in-service, proceed to Step 2. Otherwise, proceed to Step 3.

Step 2 Verify that the configuration of the affected media gateway is correct. Refer to the documentation for the media gateway for more information.

If that does not resolve the problem, proceed to Step 4.

Step 3 Verify that the Ethernet interfaces between the Cisco MGC and the associated media gateway are working properly.

Note Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of an Ethernet interface on the media gateway can be found in its associated documentation.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 4.

Note Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an Ethernet interface card on the media gateway can be found in its associated documentation.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

NAS: CommsFailure

This alarm occurs when the Cisco MGC cannot communicate with the identified media gateway.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Determine whether the affected media gateway is up and running. Refer to the documentation for the media gateway for more information.

If the affected media gateway is not up and running, restore it to service. Refer to the documentation for the media gateway for more information.

If the affected media gateway is up and running, proceed to Step 2.

Step 2 Verify that the IP configuration parameters for the Cisco MGC and the affected media gateway are correct.

Note Use the **prov-rtrv** MML command, as described in the "Retrieving Provisioning Data" section on page 3-67, to retrieve the IP configuration information for the Cisco MGC. Refer to the documentation for the media gateway for information on retrieving the IP configuration data.

If the configuration of your Cisco MGC is incorrect, begin a dynamic reconfiguration session, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

If the configuration of the affected media gateway is incorrect, modify the provisioning data for your system. Refer to the documentation for the media gateway for more information.

If the configuration of both the Cisco MGC and the affected media gateway are correct, then proceed to Step 3.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

NAS: ResourceFailure

This alarm occurs when a continuity test (COT) has not been acknowledged by the indicated media gateway.

Corrective Action

To correct the problem identified by this alarm, run a manual COT on the indicated media gateway, as described in the Running a Manual Continuity Test, page 8-96.

OOS TRAFFIC RE-ROUTE

This alarm occurs when the traffic channels (bearer channels, IP network) on one side of the Cisco MGC have been lost, causing the Cisco MGC to reroute channels away from the affected component. This is generally due to a network or equipment failure, but might be due to a provisioning failure.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Other alarms associated with the affected component should also be displayed. Resolve those alarms first.

If resolving those alarms does not clear this alarm, proceed to Step 2.

Step 2 Verify that the traffic channel provisioning settings for the Cisco MGC and the affected media gateway are correct.

Note Use the **prov-rtrv** MML command, as described in the "Retrieving Provisioning Data" section on page 3-67, to retrieve the traffic channel provisioning data for the Cisco MGC. Refer to the documentation for the media gateway for information on retrieving the traffic channel data.

If the configuration of your Cisco MGC is incorrect, begin a dynamic reconfiguration session, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

If the configuration of the affected media gateway is incorrect, modify the provisioning data for your system. Refer to the documentation for the media gateway for more information.

If the configuration of both the Cisco MGC and the affected media gateway are correct, then proceed to Step 3.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

OverloadHeavy

This alarm occurs when the system has reached the threshold for overload level 3. The system performs an automatic switchover operation. If the call rejection percentage setting for overload level 3 is unchanged from its default value, all new calls are rejected until the abate threshold for overload level 3 is reached. This alarm is automatically cleared at that time. For more information, refer to the "Managing Automatic Congestion Control" section on page 3-75.

Corrective Action

If this alarm is caused by a rare spike in traffic, corrective action is not necessary. If this alarm occurs regularly, you should ensure that your links and routes are properly configured for load sharing, as described in the "SS7 Load Sharing Malfunction" section on page 8-52, and re-route some of your traffic to other Cisco MGCs.

Note This alarm can occur when a provisioning session is active during peak busy hours. If this should happen, the alarm can be cleared by stopping the provisioning session. For more information on the MML commands to manage a provisioning session, refer to the "Provisioning your Cisco MGC" section on page 3-63.

OverloadMedium

This alarm occurs when the system has reached the threshold for overload level 2. A percentage of new calls, based on the call rejection percentage setting for overload level 2, are rejected until the abate threshold for overload level 2 is reached. This alarm is automatically cleared at that time. For more information, refer to the "Managing Automatic Congestion Control" section on page 3-75.

Corrective Action

If this alarm is caused by a rare spike in traffic, corrective action is not necessary. If this alarm occurs regularly, you should ensure that your links and routes are properly configured for load sharing, as described in the "SS7 Load Sharing Malfunction" section on page 8-52, and re-route some of your traffic to other Cisco MGCs.

Note This alarm can occur when a provisioning session is active during peak busy hours. If this should happen, the alarm can be cleared by stopping the provisioning session. For more information on the MML commands to manage a provisioning session, refer to the "Provisioning your Cisco MGC" section on page 3-63.

OverloadLight

This alarm occurs when the system has reached the threshold for overload level 1. A percentage of new calls, based on the call rejection percentage setting for overload level 1, are rejected until the abate threshold for overload level 1 is reached. This alarm is automatically cleared at that time. For more information, refer to the "Managing Automatic Congestion Control" section on page 3-75.

Corrective Action

If this alarm is caused by a rare spike in traffic, corrective action is not necessary. If this alarm occurs regularly, you should ensure that your links and routes are properly configured for load sharing, as described in the "SS7 Load Sharing Malfunction" section on page 8-52, and re-route some of your traffic to other Cisco MGCs.

Note This alarm can occur when a provisioning session is active during peak busy hours. If this should happen, the alarm can be cleared by stopping the provisioning session. For more information on the MML commands to manage a provisioning session, refer to the "Provisioning your Cisco MGC" section on page 3-63.

PC UNAVAIL

This alarm occurs when a destination point code (DPC) is unavailable. This can be due to a network failure causing the DPC to become isolated, a local failure equipment failure causing a loss of connectivity, or a local provisioning failure causing the DPC or routes to it to be configured improperly.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Other alarms associated indicating problems with hardware, the SS7 links, or the network should also be displayed. Resolve those alarms first.

If resolving those alarms does not clear this alarm, proceed to Step 2.

Step 2 Ensure that the provisioning settings for the DPC and for all routes to the DPC and adjacent STPs match the settings used on the far-end, as described in the "Retrieving Provisioning Data" section on page 3-67.

If the configuration data associated with the DPC is incorrect, begin a dynamic reconfiguration session, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

If the configuration data associated with the DPC is correct, then proceed to Step 3.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

Peer IP Links Failure

This alarm occurs when the IP links to the peer Cisco MGC are removed or down.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the Ethernet interfaces for the active and standby Cisco MGCs are working properly.

> **Note** Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 2.

> **Note** Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

PEER LINK A FAILURE

This alarm occurs either because a communication path between peer modules was lost or a peer module has stopped communicating.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving a Failed Connection to a Peer" section on page 8-125.

PEER LINK B FAILURE

This alarm occurs either because a communication path between peer modules was lost or a peer module has stopped communicating.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving a Failed Connection to a Peer" section on page 8-125.

PEER MODULE FAILURE

This alarm occurs when communications to a peer module are lost, indicating failure.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving a Failed Connection to a Peer" section on page 8-125.

POM INACTIVITY TIMEOUT

This alarm occurs when the current provisioning session had been idle for 20 minutes without input any provisioning commands. If there is still no provisioning activity within the next five minutes, the session is terminated.

Corrective Action

To correct the problem identified by this alarm, enter some provisioning MML commands, or stop the provisioning session as described in the "Saving and Activating your Provisioning Changes" section on page 3-64. For more information about provisioning your Cisco MGC, refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide*.

POM SESSION TERMINATE

This alarm occurs when a provisioning session is terminated. Any additional provisioning commands are not accepted.

Corrective Action

If you want to restart your provisioning session, perform the steps listed in the "Starting a Provisioning Session" section on page 3-63, using the same source version set equal to the destination version name.

POM: DynamicReconfiguration

This alarm occurs when a dynamic reconfiguration procedure is started. It is cleared once the dynamic reconfiguration is successfully completed. Refer to the "Invoking Dynamic Reconfiguration" section on page 3-65 for more information.

Corrective Action

If necessary, you can clear the alarm, as described in the "Clearing Alarms" section on page 8-4, or you can complete the dynamic reconfiguration procedure, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

POM: PEER_SYNC_ERR

This alarm occurs when the standby Cisco MGC attempts to synchronize the contents of its configuration library while a provisioning session is in progress on the active Cisco MGC.

Corrective Action

To correct the problem identified by this alarm, either stop the provisioning session as described in the "Ending a Provisioning Session Without Activating your Changes" section on page 3-65, or save and activate your changes as described in the "Saving and Activating your Provisioning Changes" section on page 3-64.

PRI: B-Channel not available

This alarm occurs when the Cisco MGC has received a PRI "setup" message, and the requested B channel is not available or cannot be allocated to the call.

Corrective Action

If necessary, you can clear the alarm, as described in the "Clearing Alarms" section on page 8-4, or you can save and activate your provisioning session, as described in the "Saving and Activating your Provisioning Changes" section on page 3-64.

ProcM No Response

The process manager is not responding to state information changes from the failover daemon.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Stop the Cisco MGC software on the standby Cisco MGC, as described in the "Shutting Down the Cisco MGC Software Manually" section on page 2-4.

Step 2 Restart the Cisco MGC software on the standby Cisco MGC, as described in the "Starting the Cisco MGC Software" section on page 2-2.

Step 3 Perform a manual switchover, as described in the "Performing a Manual Switchover" section on page 3-80.

Step 4 Stop the Cisco MGC software on the newly standby Cisco MGC, as described in the "Shutting Down the Cisco MGC Software Manually" section on page 2-4.

Step 5 Restart the Cisco MGC software on the newly standby Cisco MGC, as described in the "Starting the Cisco MGC Software" section on page 2-2.

REPL: all connections failure

This alarm occurs when the Cisco MGC cannot establish communication to the peer Cisco MGC.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Verify that the Ethernet interfaces for the Cisco MGC are working properly.

Note Information on verifying the proper operation of an Ethernet interface on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system.

If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Otherwise, proceed to Step 2.

Note Information on removing and replacing an Ethernet interface card on the Cisco MGC host can be found in the Sun Microsystems documentation that came with your system.

Step 2 Verify the replicator configuration on the Cisco MGCs, as described in the "Verifying Proper Configuration of Replication" section on page 8-123.

If that does not resolve the alarm, proceed to Step 3.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

RSET CONFIG FAIL

This alarm occurs when the provisioning data for the SS7 route set to a DPC has invalid or incompatible parameter values. This does not occur due to a mismatch between the network topology and the DPC data.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Ensure that the provisioning settings for the DPC and for all routes to the DPC match the settings used on the far-end, as described in the "Retrieving Provisioning Data" section on page 3-67.

If the configuration data associated with the DPC is incorrect, begin a dynamic reconfiguration session, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

If the configuration data associated with the DPC is correct, then proceed to Step 3.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

SC CONFIG FAIL

This alarm occurs when the provisioning parameters for the data link layer of a signaling channel are inconsistent or invalid. The signaling channel may already be provisioned. The configuration file might be corrupted and cannot be read by the system.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Place the affected signaling channel in the out-of-service state, as described in the "Setting the Service State of a Signaling Channel" section on page 8-58.

Step 2 Start a provisioning session, as described in the "Starting a Provisioning Session" section on page 3-63.

Step 3 Remove the affected signaling channel from your configuration using the **prov-dlt** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 MML Command Reference Guide* for more information.

Step 4 Referring to your local provisioning parameters, re-provision the signaling channel using the prov-add MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 MML Command Reference Guide* for more information.

Step 5 Save and activate your provisioning session, as described in the "Saving and Activating your Provisioning Changes" section on page 3-64.

Step 6 Place the signaling channel in the in-service state, as described in the "Setting the Service State of a Signaling Channel" section on page 8-58.

If that does not resolve the problem, proceed to Step 8.

Step 7 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

SC FAIL

This alarm occurs when the signaling channel is down and unable to process traffic. As a result, the signaling channel is failing to negotiate a D-channel session, automatic restarts are not able to recover the session, and the data link-layer has failed. This can occur when SS7 SLTM/SLTA fails or when a PRI D-channel fails.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Ensure that the near-end and far-end data link terminations are operating.

If the near-end or far-end data link terminations are not operating, fix as necessary.

If the near-end and far-end data link terminations are operating, proceed to Step 2.

Step 2 Ensure that the provisioning settings for the signaling channel match the settings used on the far-end, as described in the "Retrieving Provisioning Data" section on page 3-67.

If the configuration data for the signaling channel is incorrect, begin a dynamic reconfiguration session, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

If the configuration data for the signaling channel is correct, then proceed to Step 3.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

SC M-OOS

This alarm occurs when the signaling channel has been manually set to the out of service state.

Corrective Action

To correct the problem identified by this alarm, return the signaling channel to the in-service state as described in the "Setting the Service State of a Signaling Channel" section on page 8-58.

srcpAudit: GwBackhaulProto

This alarm occurs when the returned backhaul protocol is different from what the Cisco MGC expects, which is a value of none. A mismatch here might cause minimal, partial, or complete signaling/call-control failure.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: GwBackhaulSes

This alarm occurs when the number of backhaul sessions is different from what the Cisco MGC expects. The Cisco MGC is expecting the value to match the provisioned value. Each backhaul session to the same IP address as the SRCP counts as 1. Some signaling information might be lost, leading to lost or failed calls.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: GwControlProto

This alarm occurs when the control protocol is different from what the Cisco MGC expects, which is a value of MGCP. A mismatch here might cause minimal, partial, or complete signaling failure.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: GwCoordProto

This alarm occurs when the coordination protocol is different from what the Cisco MGC expects, which is a value of SRCP 1.0. A mismatch here might cause alarms to be raised erroneously.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: GwCuIpAddr

This alarm occurs when the IP address of the media gateway (CU) reported by the media gateway is different from that configured in the Cisco MGC. The Cisco MGC is expecting the IP address to match the value provisioned for the remote IP address entry of the signaling channel path. This can lead to a communication failure by the control protocol.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: GwCuIpPort

This alarm occurs when the value of the IP port reported by the media gateway (CU) is different from that configured in the Cisco MGC. The Cisco MGC is expecting the IP port to match the provisioned value for the remote port entry for this signaling channel or signaling service.This can lead to a communications failure by the control protocol.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: GwNumOfLines

This alarm occurs when the number of lines in the media gateway partition is different from what the Cisco MGC expects. The Cisco MGC is expecting the number of lines to match the value provisioned for the total number of bearer lines associated with this signaling service. This may affect service if a call are made on nonexistent lines. Another error should be raised elsewhere in the system if a call is placed to a nonexistent line.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: GwSlotNum

This alarm occurs when the hardware for the media gateway is in a different slot than the Cisco MGC expects, which is a value of 0. This should not affect service but might be an issue in hardware troubleshooting.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: GwSuIpAddr

This alarm occurs when the IP address of the call agent (SU or MGC) reported by the media gateway is different from that configured in the Cisco MGC. The Cisco MGC is expecting the IP address to match the value provisioned for the local IP address entry for this signaling channel or signaling service. This can lead to a communications failure by the control protocol.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: GwSuIpPort

This alarm occurs when the IP port of the call agent (SU or Cisco MGC) reported by the media gateway is different from that configured in the Cisco MGC. The Cisco MGC is expecting the IP port value to match the value provisioned for the local port entry for this signaling channel or signaling service. This can lead to a communications failure by the control protocol.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: GwType

This alarm occurs when the media gateway is of a different type than the Cisco MGC expects, which is a value of VISM. This may or may not affect service depending on whether the Cisco MGC has media gateway-specific coding.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: LineCoding

This alarm occurs when the line coding used by the media gateway for that line is different from that configured in the Cisco MGC for that line, which is a value of Unknown. This might lead to corrupted data on the B-channels.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: LineLoopback

This alarm occurs when the line loopback for that line used by the media gateway is different from that configured in the Cisco MGC for that line, which is a value of n. A line may be in a loopback state when the Cisco MGC believes it is available.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: LineSigProto

This alarm occurs when the signaling protocol used by the media gateway for that line is different from that configured in the Cisco MGC for that line. The Cisco MGC is expecting the signaling type associated with the backhaul signaling to the same remote IP address as the SRCP for this signaling channel. Some signaling information might be lost, leading to lost or failed calls.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

srcpAudit: LineState

This alarm occurs when the line state for the line used by the media gateway is different from that configured in the Cisco MGC for that line, which is a value of e. A line might be disabled by the media gateway when the Cisco MGC believes it is available.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Resolving an SRCP Audit Alarm" section on page 8-97.

SSN FAIL

This alarm occurs when the SCP located by subsystem number (SSN) is not available.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Ensure that the provisioning settings for the SSN and the associated routes match the settings used on the far-end, as described in the "Retrieving Provisioning Data" section on page 3-67.

If the configuration data associated with the SSN is incorrect, begin a dynamic reconfiguration session, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

If the configuration data associated with the SSN is correct, then proceed to Step 2.

Step 2 Verify the network configuration to confirm that the SCP identified with the SSN is reachable.

If the SCP is not reachable, begin a dynamic reconfiguration session, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65, and reprovision your data for an SCP that is reachable, or remove the SSN and its associated data.

If the SCP is reachable, proceed to Step 3.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

Standby Warm Start

This alarm occurs on the active Cisco MGC when a warm start process begins in the IOCM. This alarm clears automatically when the warm start process completes successfully. This alarm also occurs on the standby Cisco MGC when the **prov-sync** MML command is entered on the active Cisco MGC. In that case, the alarm clears automatically when the synchronization of provisioning data is complete.

Corrective Action

Corrective action is only required when the alarm does not clear automatically. If this alarm does not clear automatically, verify that the pom.dataSync parameter in the XECfgParm.dat is set to *true* on each host, using the procedure in the "Rebooting Software to Modify Configuration Parameters" section on page 8-125.

SUPPORT FAILED

This alarm occurs when the identified entity cannot provide service because a supporting entity is not providing service. The supporting entity may be hardware or software.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Check for other alarms, as described in the "Retrieving All Active Alarms" section on page 8-3, that further identify the failed entity.

Step 2 Once you have identified the failed entity, replace it and restore it to service. If the entity is hardware, refer to the appropriate documentation for replacement. If it is software, attempt to reboot the software.

If the alarms clear, the procedure is complete. Otherwise, proceed to Step 3.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

SwitchoverFail

This alarm occurs when a switchover operation from the active Cisco MGC to the standby Cisco MGC has failed.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the "Recovering from a Switchover Failure" section on page 8-113.

XE Rsrc Fail

This alarm occurs when memory resources have been exhausted on the active Cisco MGC host. If this alarm occurs frequently you may need to add additional memory to your Cisco MGC. Refer to the Sun Microsystems documentation for your Cisco MGC host for more information about adding additional memory.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:

Step 1 Perform a manual switchover, as described in the "Performing a Manual Switchover" section on page 3-80.

Step 2 Stop the Cisco MGC software on the newly standby Cisco MGC, as described in the "Shutting Down the Cisco MGC Software Manually" section on page 2-4.

Step 3 Restart the Cisco MGC software on the newly standby Cisco MGC, as described in the "Starting the Cisco MGC Software" section on page 2-2.

SS7 Network Related Problems

The Cisco MGC node is considered to be a standard Service Switching Point (SSP) in an SS7 network. The SS7 network carries two types of signals:

- Circuit-related
- Noncircuit-related

The signals involved in the setup and teardown of bearer circuits are circuit-related. Non-circuit-related signals are used for all the ancillary services provided by the SS7 network, including database access and network management.

The SS7 protocol is composed of several levels or "parts," including the following:

- Message Transfer Part (MTP)—Levels 1 (MTP1) through 3 (MTP3)
- Signaling Connection Control (SCCP)
- Application Service Part (ASP)
- Transaction Capabilities Application Part (TCAP)
- Telephony User Part (TUP)
- ISDN User Part (ISUP)
- Broadband ISUP (BISUP)

There are many variations of different parts of the SS7 protocol stack. MTP has ANSI, ITU, Bellcore, and a number of national variations. Each country and each major carrier may have slightly different variations of a part to fit its particular needs.

The SS7 network needs to have the highest degree of reliability. Each switch with access to the SS7 network must be configured to a preconceived set of network parameters. There is some risk that the person configuring a switch will not use the correct set of parameters or values. This is the root cause of most SS7 problems at both the MTP layers and upper layers of the SS7 protocol. A single parameter value, such as an incorrect timer value, can cause SS7 connectivity to act improperly or fail completely.

The first, and most important, step in troubleshooting SS7 related problems is to understand, and fully document, the SS7 network topology and protocols. The protocol documents are used as a reference over the months and years of maintenance on the SS7 network.

Troubleshooting SS7 network problems is described in the following sections:

- Signaling Channel Problems, page 8-51
- Signaling Destination Problems, page 8-55
- SS7 Network Troubleshooting Procedures, page 8-58

Signaling Channel Problems

The Cisco MGC software generates signaling alarms if it detects problems with the transportation of data on a signaling channel or at a signaling destination.

Signaling alarms have four classifications of severity:

- Critical
- Major
- Minor
- Informational

Note Multiple alarms are likely to occur for severe failures. For example, SUPPORT FAIL and SC FAIL would typically occur with LIF LOS.

Signaling links are the dedicated communication channels that the Cisco MGC uses to transfer signaling information among itself, the Cisco SLTs, and the Signal Transfer Points (STPs). Signaling links provide the necessary delivery reliability for higher-layer SS7 signaling protocols.

You can use the Cisco MGC software and MML commands to manage signaling channels and lines. You can retrieve signaling channel attributes, change the states of signaling channels, and change the state of signaling lines. See Chapter 3, "Cisco MGC Node Operations," for detailed information.

Note For more information on MML commands, refer to the *Cisco Media Gateway Controller Software Release 7 MML Reference Guide*.

Because all types of signaling channels have basically the same functionality, they are managed similarly. Unless otherwise noted, all commands, counters, and alarms mentioned here are applicable to all types of signaling channels.

Signaling channel problems are described in the following sections:

SS7 Link is Out-of-Service

If an SS7 link is out-of-service on your system, perform the following steps:

Step 1 Change the service state of the SS7 link to in-service, as described in the "Setting the Service State of a Link or Linkset" section on page 8-60.

If the SS7 link returns to service, the procedure is complete. Otherwise, proceed to Step 2.

Step 2 If your system is using I/O cards to terminate the SS7 link, proceed to Step 3.

If your system is using Cisco SLTs to terminate the SS7 link, proceed to Step 4.

Step 3 Verify that MTP1 is working correctly on the affected I/O card by checking for the following indications:

a. Check the alarm LEDs on the affected I/O card. Dual green LEDs indicate that MTP1 is working correctly. Red or yellow LEDs indicate LOS, LOF and other errors.

If both LEDs are green proceed to Step 5. Otherwise, proceed to Step 3b.

b. Check for LIF alarms for the affected I/O card, as described in the "Retrieving All Active Alarms" section on page 8-3.

Perform the corrective actions for the alarm. These can be found in the "Alarm Troubleshooting Procedures" section on page 8-8.

Repeat Step 1. If the link returns to service, the procedure is complete. Otherwise, proceed to Step 4.

Step 4 Verify that MTP1 is working correctly on the affected Cisco SLT, as described in the "Identifying MTP1 Communication Problems" section on page B-11.

If MTP1 is working correctly on the affected Cisco SLT, proceed to Step 6. Otherwise, correct the MTP1 problems as described in the "Resolving MTP1 Communication Problems" section on page B-11.

Repeat Step 1. If the link returns to service, the procedure is complete. Otherwise, proceed to Step 6.

Step 5 Verify that MTP2 is working correctly on the Cisco MGC by searching for excessive SUREM/AERM errors and link failure messages in the active system log file, as described in the "Viewing System Logs" section on page 8-4.

If MTP2 is working correctly on the Cisco MGC, proceed to Step 8. Otherwise, correct the MTP2 problems as described in the "Resolving MTP1 Communication Problems" section on page B-11.

Repeat Step 1. If the link returns to service, the procedure is complete. Otherwise, proceed to Step 8.

Step 6 Verify that MTP2 is working correctly on the affected Cisco SLT, as described in the "Identifying MTP2 Communication Problems" section on page B-12.

If MTP2 is working correctly on the affected Cisco SLT, proceed to Step 7. Otherwise, correct the MTP2 problems as described in the "Resolving MTP2 Communication Problems" section on page B-12.

Repeat Step 1. If the link returns to service, the procedure is complete. Otherwise, proceed to Step 7.

Step 7 Troubleshoot the SS7 link by performing the procedures found in the "Troubleshooting SS7 Link Problems" section on page B-4.

If no problems can be found, proceed to Step 8. Otherwise, repeat Step 1. If the link returns to service, the procedure is complete. Otherwise, proceed to Step 8.

Step 8 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

SS7 Load Sharing Malfunction

If load sharing on your SS7 links and/or routes is not working properly, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command to verify the priority settings of your SS7 links:

```
prov-rtrv:c7iplnk:"all"
```

The system returns a response similar to the following:

```
   MGC-02 - Media Gateway Controller 2001-07-24 12:11:44
M  RTRV
   "session=active:c7iplnk"
   /*
NAME                LNKSET               IF             IPADDR      PORT
PEERADDR        PRI       SLC        TIMESLOT   NEXTHOP          NETMASK
----                ------               --             ------      ----
--------        ---       ---        --------   -------          -------
ls1link1            ls1                  enif1          IP_Addr1    7000
172.24.200.9    1         0          0          0.0.0.0          255.255.255.255
ls2lnk1             ls2                  enif1          IP_Addr1    7000
172.24.200.9    1         0          1          0.0.0.0          255.255.255.255
ls1link2            ls1                  enif1          IP_Addr1    7000
172.24.200.10   1         1          0          0.0.0.0          255.255.255.255
ls2lnk2             ls2                  enif1          IP_Addr1    7000
172.24.200.10   1         1          1          0.0.0.0          255.255.255.255
lk-3                ls-itu               enif1          IP_Addr1    7001
172.24.237.254  1         0          2          0.0.0.0          255.255.255.255
   */
```

The PRI field in the response shows the priority settings for your SS7 links. For load sharing to work properly, the priority settings for all of your links should be set to 1.

Step 2 Enter the following command to verify the priority settings of your SS7 routes:

prov-rtrv:ss7route:"all"

The system returns a response similar to the following:

```
MGC-02 - Media Gateway Controller 2001-07-24 12:25:05
M  RTRV
   "session=active:ss7route"
   /*
NAME                OPC                  DPC                  LNKSET     PRI
----                ---                  ---                  ------     ---
route1              opc1                 dpc1                 ls1         1
rout2               opc1                 dpc2                 ls2         1
rt3                 opc2                 scp2                 ls-itu      1
rt1                 opc2                 stp1                 ls-itu      1
rt2                 opc2                 scp1                 ls-itu      1
   */
```

The PRI field in the response shows the priority settings for your SS7 routes. For load sharing to work properly, the priority settings for all of your routes should be set to 1.

Step 3 Start a provisioning session, as described in "Starting a Provisioning Session" section on page 3-63.

Step 4 If any of the SS7 links show a priority other than 1, you must change the priority settings to ensure proper link load sharing. Before you can change the priority settings for the link, you must take the link out-of-service, as described in the "Setting the Service State of a Link or Linkset" section on page 8-60.

Step 5 Modify the priority settings of the link by entering the following command:

prov-ed:c7iplnk:name="*lnkname***",pri=1**

Where *lnkname* is the name of an SS7 link that does not have a priority of 1.

Repeat this step for each link that does not have a priority of 1.

Step 6 If any of the SS7 routes show a priority other than 1, you must change the priority settings to ensure proper route load sharing. Before you can change the priority settings for the route, you must take the route out-of-service, as described in the "Setting the Service State of a Signaling Point Code" section on page 8-60.

Step 7 Modify the priority settings of the link by entering the following command:

prov-ed:ss7route:name="*rtname***",pri=1**

Where *rtname* is the name of an SS7 route that does not have a priority of 1.

Repeat this step for each route that does not have a priority of 1.

Step 8 Save and activate your provisioning changes, as described in the "Saving and Activating your Provisioning Changes" section on page 3-64.

Physical Layer Failures

The major issues with the physical layer of an SS7 signaling link are related to cabling, clock source, and connector pinouts. The cable should be of high quality (shielded) and the connectors should be attached and crimped solidly. Since SS7 links are synchronous, one side of the link must provide the clock source and the other side must use this clock signal to read the bits.

Finally, the most common mistake is to use the wrong cable pinouts for a specific physical configuration. Make sure that the connector has the correct number of pins (RJ-45, DB-25) and that each pin maps to the correct signal. A number of different physical layers are supported, including ANSI T1, CEPT E1, and V.35. Make sure that the cable complies with the connector and the physical protocol being used.

If the configuration appears to be valid and the cable pinout is good, check that the signal is being sent and received correctly. Use a Bit Error Rate Tester (BERT) or perform a signal loopback on the interface. It is possible that the cable is bad, so try to replace it. Finally, it is possible that the line card is bad, so you might try replacing it too.

Configuration Errors

The most common mistake in SS7 signal link configuration is to misconfigure the Signal Link Code (SLC) for the SS7 link. This is a preconfigured code on both ends of the link. If the SLC or the point codes do not match, the link does not align and no transmission can take place.

For T1 and E1 connectors, an SS7 signaling link is carried in a single 56- or 64-kbps time slot. The time slot that is used must also agree on both sides of the link.

Make sure the MTP2 timers and thresholds agree with the network defaults. Confirm that the far-end switch or STP has the same values as your system.

When a Cisco SLT is used to terminate MTP2, confirm that the RUDP parameters agree on both sides and are consistent with the documentation.

Supporting Entity Failures

An SS7 signaling link has a hierarchy of network element entities that must be functioning before the link can function. These include the physical interface (discussed above) and the control software for the link. If any of these fail, the link also fails.

Incomplete Signaling

Link failures between the Cisco SLT and the Cisco MGC can be caused by

- Ethernet card failure on the Cisco SLT

- Ethernet card failure on the LAN switch
- LAN switch failure
- Fast Ethernet interface card failure on the Cisco MGC

In each of the above cases, it is impossible to transfer MTP3 signaling messages from the Cisco SLT to the Cisco MGC. Cisco SLT platform failure (which is equivalent to MTP2 failure) causes signaling messages to be unable to go to MTP3. The MTP2 layer on the Cisco SLT is supposed to transmit SIPO messages to the STP mated pair to initiate the changeover procedure. Cisco SLT platform failure on the SS7 network is detected by the mated STP pair, which detects timer expiration and link unavailability.

Changing Service States

Signal channels comply with the Generic Service State model defined in the "Physical Layer Failures" section on page 8-54. You can change the desired service state of a signaling channel using the following transition requests. Note that there is a difference between a desired service state and an actual service state, and the Cisco MGC might not be able to honor the request. For example, a signal channel that is out-of-service due to an equipment failure cannot transition to an in-service state upon request. The Cisco MGC attempts to bring the channel in-service, but it fails. The failure must be fixed before the transition can succeed.

- In-service (IS)—The signaling channel is requested to start providing service.
- Out-of-service (OOS)—The signaling channel is requested to stop providing service.

  For some protocols, this request is accepted, but not granted until after all calls have been released. During the interim period, the channel's service state appears as OOS, PEND.
- Forced out-of-service (FOOS)—The signaling channel is requested to stop providing service immediately regardless of related call states, and to drop currently active calls.
- Inhibit (INH)—The signaling channel is requested to be put into an inhibit state. This state is for SS7 signaling channels only and fails on other types of signaling channels.

  In this state, the channel is active but does not provide service for call processing. If the signaling channel is the last one in the signal path, the inhibit request is denied and an error is returned.
- Un-inhibit (UNH)—The signaling channel is requested to be removed from an INH state and to provide service for call processing. This state is for SS7 signaling channels only and fails on other types of signaling channels.

  Use this option (UNH), rather than the IS option, to return an inhibited signaling channel to service.

Note Changing the state of a signaling channel generates an alarm. For more information on retrieving and clearing alarms, see "Troubleshooting Using Cisco MGC Alarms" section on page 8-2

Signaling Destination Problems

Signaling destinations refer to the endpoints of a network. Typically, if signaling links are in service, the signaling destinations should also be in service.

For ISDN signaling, the signaling channel is in service if the Cisco MGC can talk to the media gateway and ISDN backhaul is configured. The destination is in service if the signaling channel is in service and the remote ISDN device is up.

Apparent mismatches can occur due to

- SS7 traffic restart handling (TRW/TRA)

- SS7 STP problems
- Configuration problems
- Software problems

An SS7 STP is treated as an adjacent point code (APC) to the Cisco MGC. SS7 MTP uses a message exchange called Signaling Link Test Message (SLTM)/Signaling Link Test Acknowledgment (SLTA) to confirm that the far-end point code is the one configured. The SLTM consists of the originating point code (OPC) of the Cisco MGC, an APC number, and an SS7 network indicator. If the values for these parameters match with the values used for these at the far-end switch, an SLTA is returned. If the value for any of these parameters do not match, the far-end switch does not send an SLTA. The Cisco MGC drops the link and tries to realign it. This process continues until the SLTM parameters match on both sides. The problem is manifested by the SS7 links dropping and recovering in roughly 30-second cycles (this is referred to as bouncing).

The following sections describe signaling destination problems:

Bouncing SS7 Links

Usually, this condition is caused by mismatched signaling link codes (SLCs) or DPCs/OPCs between the Cisco MGC and the far end. To resolve a bouncing SS7 condition, perform the following steps:

Step 1 Verify that the SLC, OPC, and DPC provisioning settings match with those used on the far end. To do this, enter the **prov-rtrv** MML command for the SS7 link, OPC, and DPC components, as described in the "Retrieving Provisioning Data" section on page 3-67, and compare the values found there with those used by the far end.

If the provisioning settings for the SLC, OPC, and DPC match with those used on the far end, proceed to Step 2. Otherwise, modify the settings to match with those used on the far end. Refer to the "Invoking Dynamic Reconfiguration" section on page 3-65 for more information about modifying the settings of a provisioned component. If that clears the problem, the procedure is complete. Otherwise, proceed to Step 2.

Step 2 Ensure that the local MTP3 timer settings match the network defaults by performing the "Verifying MTP3 Timers" section on page 8-63.

If the local MTP3 timer settings match the network defaults, proceed to Step 3. Otherwise, contact the far-end to determine whether their timer settings can be changed to match your settings. If that clears the problem, the procedure is complete. Otherwise, proceed to Step 3.

Step 3 View the system logs, as described in the "Viewing System Logs" section on page 8-4, looking for excessive alignment error monitoring (AERM) logs. If large numbers of AERM logs are present, proceed to Step 4. If no AERM logs are present, contact the Cisco TAC for assistance. Refer to the "Obtaining Technical Assistance" section on page xviii for more information about contacting the Cisco TAC.

Step 4 Determine why the link is not aligning properly by checking the alignment status on the Cisco SLT associated with the affected link, as described in the "Verifying the Link Alignment Status" section on page B-6.

Configuration Errors

If the SS7 DPC is fully associated, it can have the same SLTM/SLTA problems as described above.

If the SS7 DPC is quasi-associated, the most common cause for failure is a route misconfiguration. Review the route information between the Cisco MGC and the DPC to make sure that the APCs are valid, the route priorities are set correctly, and the route uses the appropriate linkset.

Traffic Restart

Make sure that the MTP3 traffic restart timers and thresholds agree with the network defaults. Confirm that the far-end switch or STP also has the same values.

SS7 Destination is Out of Service

A signaling destination is typically out of service when all of the SS7 links from the Cisco MGC to the destination or APC are out of service, or when all of the SS7 links from the destination to the APC are out of service.

To restore an SS7 destination to service, perform the following steps:

Step 1 Contact your SS7 provider and have them verify the links from the DPC to the associated STP.

Step 2 Verify the state of the signaling channels, as described in the "Retrieving Signaling Channel Attributes" section on page 3-48.

If any of the SS7 links are out-of-service, restore the links as described in the "SS7 Link is Out-of-Service" section on page 8-51. If all of the SS7 links to a destination are out-of-service, restore the destination as described in the "SS7 Destination is Out of Service" section on page 8-57.

SS7 Route is Out of Service

To restore an SS7 route to service, perform the following steps:

Step 1 Change the service state of the destination to in-service, as described in the "Setting the Service State of a Destination" section on page 8-59.

If the destination goes into service, the procedure is complete. Otherwise, proceed to Step 2.

Step 2 Verify the state of the signaling channels, as described in the "Retrieving Signaling Channel Attributes" section on page 3-48.

If none of the SS7 links are in-service, proceed to Step 3. If all or at least one of the SS7 links to the destination are in-service, then contact your SS7 provider and have them verify the links from the DPC to the associated STP.

Step 3 Determine why the link is not aligning properly by checking the alignment status on the Cisco SLT associated with the affected link, as described in the "Verifying the Link Alignment Status" section on page B-6.

SS7 Destination is Unavailable

An SS7 destination is unavailable when all of the routes to the destination are out-of-service. Perform the procedure defined in the "SS7 Route is Out of Service" section on page 8-57.

SS7 Network Troubleshooting Procedures

The following sections are procedures used to resolve problems associated with the Cisco MGC node's connection to the SS7 network:

Setting the Service State of a Signaling Channel

To set the service state of a signaling channel or linkset, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

set-sc-state:*sig_chan***:***serv_state*

Where:

- *sig_chan*—The MML name of the desired signaling channel or linkset.
- *serv_state*—The desired service state. The valid states are listed below:
  - IS—Places a signaling channel or linkset in service. This state is valid for all signaling channel or linkset types.
  - OOS—Takes a signaling channel or linkset out of service.This state is valid for all signaling channel or linkset types.

Note You must use the FOOS option to set the last link of a linkset OOS.

- FOOS—Forces a signaling channel or linkset out of service. This state is valid for all signaling channel or linkset types.
- INH—Inhibits an SS7 link. This state is valid only for SS7 signaling links.
- UNH—Uninhibits an SS7 link. This state is valid only for SS7 signaling links.

For example, to set the service state of a signaling channel called iplink1 to IS, enter the following command:

```
set-sc-state:iplink1:IS
```

Step 2 Verify that the state of the signaling channel or linkset has changed by entering the **rtrv-sc** command, as described in the "Retrieving Signaling Channel Attributes" section on page 3-48.

Setting the Service State of a Destination

To set the service state of a destination, perform the following steps:

Caution The **set-dest-state** command should only be used while you are dynamically reconfiguring the system. Do not use the **set-dest-state** command to take a signaling service out-of-service during a maintenance session, as all calls associated with the specified signaling service will be dropped. You should instead use the **blk-cic** command to block the CICs associated with the signaling service when you need to perform maintenance.

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

set-dest-state:*dest***:***serv_state*

Where:

- *dest*—The MML name of the desired destination, such as an SS7 point code, FAS signaling service, or IP FAS signaling service.
- *serv_state*—The desired service state. The valid states are listed below:
  - IS—Places a destination in service.
  - OOS—Takes a destination out of service.

Note Before you can take a NAS signaling service out of service, you must shut down the D channel on the associated media gateway. Refer to the documentation for the media gateway for more information on shutting down D channels.

For example, to set the service state of a destination called dpc1 to IS, enter the following command:

```
set-dest-state:dpc1:IS
```

Step 2 Verify that the state of the destination has changed by entering the **rtrv-dest** command, as described in the "Retrieving Signaling Destination Service States" section on page 3-50.

Setting the Service State of a Signaling Point Code

To set the service state of a signaling point code, perform the following steps:

Caution The **set-spc-state** command should only be used while you are dynamically reconfiguring the system. Do not use the **set-spc-state** command to take an SS7 signaling service out-of-service during a maintenance session, as all calls associated with the specified SS7 signaling service will be dropped. You should instead use the **blk-cic** command to block the CICs associated with the SS7 signaling service when you need to perform maintenance.

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

set-spc-state:*sig_pc***:***serv_state*

Where:

- *sig_pc*—The MML name of the desired signaling point code.
- *serv_state*—The desired service state. The valid states are listed below:
  - IS—Places a signaling point code in service.
  - OOS—Takes a signaling point code out of service.

For example, to set the service state of signaling point code called stp1 to IS, enter the following command:

```
set-spc-state:stp1:IS
```

Step 2 Verify that the state of the signaling channel has changed by entering the **rtrv-spc** command, as described in the "Retrieving the State of Point Codes" section on page 3-51.

Setting the Service State of a Link or Linkset

To set the service state of a link or linkset, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

set-lnk-state:*lname***:***serv_state*

Where:

- *lname*—The MML name of the desired link or linkset.
- *serv_state*—The desired service state. The valid states are listed below:
  - IS—Places a link or linkset in service.
  - OOS—Takes a link or linkset out of service.

Note You must use the FOOS option to set the last link of a linkset OOS.

  - FOOS—Forces a link or linkset out of service.
  - INH—Inhibits a link or linkset.
  - UNH—Uninhibits an link or linkset.

For example, to set the service state of a link called ls1-link1 to IS, enter the following command:

```
set-sc-state:ls1-link1:IS
```

Step 2 Verify that the state of the link or linkset has changed by entering the **rtrv-lnk** command, as described in the "Retrieving the Service State of a Linkset" section on page 3-51.

Setting the Service State of a Local Subsystem Number

To set the service state of a local subsystem number (LSSN), perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

set-lssn-state:*ssn***:***serv_state*

Where:

- *ssn*—The MML name of the desired LSSN.
- *serv_state*—The desired service state. The valid states are listed below:
  - IS—Places an LSSN in service.
  - OOS—Takes an LSSN out of service.

For example, to set the service state of an LSSN called lnp to IS, enter the following command:

```
set-lssn-state:lnp:IS
```

Step 2 Verify that the state of the LSSN has changed by entering the **rtrv-lssn** command, as described in the "Retrieving the State of All Local Subsystem Numbers" section on page 3-53.

Verifying MTP Timer Settings

When resolving signaling problems between the Cisco MGC and an associated SS7 network element (such as an STP), you may need to verify that the MTP2 and MTP3 timer settings used by the Cisco MGC conform to settings used by the associated SS7 network element. MML commands are used to retrieve the settings for the MTP2 and MTP3 timers on the Cisco MGC. The following subsections describe methods for verifying the MTP timer settings on the Cisco MGC.

Note Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information on the MTP timers.

The procedure used to verify the settings for MTP2 timers varies based on how SS7 signaling is terminated for your Cisco MGC. If you are using Cisco SLTs to terminate SS7 signaling, refer to the "Verifying MTP2 Timers for Cisco SLTs" section on page 8-62. If you are using I/O cards to terminate SS7 signaling, refer to the "Verifying MTP2 Timers for I/O Cards" section on page 8-62. The procedure to verify MTP3 timers is the same for both SS7 signaling termination methods.

If you find, after you verify the settings, that you need to modify the settings for the MTP timers, proceed to the "Modifying MTP Timer Settings" section on page 8-65.

Verifying MTP2 Timers for Cisco SLTs

To verify the values used for the MTP2 timers when you are using Cisco SLTs to terminate SS7 signaling, complete the following steps:

Step 1 Enter the following command at the Cisco SLT to display the settings for the MTP2 timers:

```
Router #show SS7 mtp2 timer channel
```

Where: *channel* specifies a channel, 0 through 3.

The system returns a message similar to the following:

```
SS7 MTP2 Timers for channel 0 in milliseconds
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
    T1 aligned/ready = 15000
      T2 not aligned = 5000
          T3 aligned = 3000
T4 Emergency Proving = 3000
   T4 Normal Proving = 3000
      T5 sending SIB = 200
      T6 remote cong = 3000
 T7 excess ack delay = 2000
  T8 errored int mon = 0
TA SIE timer = 20
       TF FISU timer = 20
        TO SIO timer = 20
       TS SIOS timer = 20
```

Step 2 Verify the MTP2 timers settings listed for the Cisco SLTs against the MTP2 timers used at the associated destination.

If the MTP2 timers settings match, your signaling problem has different cause. Continue troubleshooting the problem.

If the MTP2 timers settings do not match, perform the procedure in the "Modifying MTP2 Timers for Cisco SLTs" section on page 8-65.

Verifying MTP2 Timers for I/O Cards

To verify the values used for the MTP2 timers when you are using I/O cards to terminate SS7 signaling, complete the following steps:

Step 1 Log on to active Cisco MGC, start an MML session, and enter the following command to display the settings for the MTP2 timers:

Note If you use this command to verify the settings for the MTP2 timers when you are using Cisco SLTs to terminate SS7 signaling links, the displayed results reflect the default values for the SS7 variant assigned to the linkset, not the actual values used. Refer to the "Verifying MTP2 Timers for Cisco SLTs" section on page 8-62 for the procedure to obtain the actual settings used for these MTP2 timers.

```
prov-rtrv:sigsvcprop:name="protocol"
```

Where *protocol* is the MML name for the SS7 protocol family being used, such as SS7-ANSI or SS7-ITU.

The system returns a message similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-01 10:31:00
M  RTRV
   "session=active:lnksetprop"
   /*
mtp2AermEmgThr = 1
mtp2AermNrmThr = 4
mtp2CongDiscard = false
mtp2LssuLen = 1
mtp2MaxAlignRetries = 5
mtp2MaxMsuFrmLen = 272
mtp2MaxOutsFrames = 127
mtp2ProvingEmgT4 = 6
mtp2ProvingNormalT4 = 23
mtp2SuermThr = 64
mtp2T1 = 130
mtp2T2 = 115
mtp2T3 = 115
mtp2T5 = 1
mtp2T6 = 30
mtp2T7 = 10
mtp3ApcMtpRstrtT28 = 30
mtp3DlnkConnAckT7 = 10
mtp3FrcUnhT13 = 10
mtp3InhAckT14 = 20
mtp3LocInhTstT20 = 900
mtp3MaxSltTries = 2
mtp3MsgPriority = 2
mtp3MtpRstrtT24 = 100
mtp3RepeatRstrtT26 = 150
mtp3TfrUsed = false
mtp3TraSntT29 = 600
mtp3tstSltmT1 = 60
mtp3tstSltmT2 = 600
mtp3UnhAckT12 = 10
reference = ANSI92
rudpAck = enable
rudpKeepAlives = enable
rudpNumRetx = 2
rudpRetxTimer = 6
rudpSdm = enable
rudpWindowSz = 32
```

Step 2 Verify the MTP2 timers settings listed for the I/O cards against the MTP2 timers used at the associated destination.

If the MTP2 timers settings match, your signaling problem has different cause. Continue troubleshooting the problem.

If the MTP2 timers settings do not match, perform the procedure in the "Modifying MTP2 Timers for I/O Cards" section on page 8-66.

Verifying MTP3 Timers

To verify the values used for the MTP3 timers, complete the following steps:

Step 1 Log on to active Cisco MGC, start an MML session, and enter the following command to display the settings for the MTP3 timers:

prov-rtrv:sigsvcprop:name="*protocol***"**

Where *protocol* is the MML name for the SS7 protocol family being used, such as SS7-ANSI or SS7-ITU.

The system returns a message similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-01 10:31:00
M  RTRV
   "session=active:lnksetprop"
   /*
mtp2AermEmgThr = 1
mtp2AermNrmThr = 4
mtp2CongDiscard = false
mtp2LssuLen = 1
mtp2MaxAlignRetries = 5
mtp2MaxMsuFrmLen = 272
mtp2MaxOutsFrames = 127
mtp2ProvingEmgT4 = 6
mtp2ProvingNormalT4 = 23
mtp2SuermThr = 64
mtp2T1 = 130
mtp2T2 = 115
mtp2T3 = 115
mtp2T5 = 1
mtp2T6 = 30
mtp2T7 = 10
mtp3ApcMtpRstrtT28 = 30
mtp3DlnkConnAckT7 = 10
mtp3FrcUnhT13 = 10
mtp3InhAckT14 = 20
mtp3LocInhTstT20 = 900
mtp3MaxSltTries = 2
mtp3MsgPriority = 2
mtp3MtpRstrtT24 = 100
mtp3RepeatRstrtT26 = 150
mtp3TfrUsed = false
mtp3TraSntT29 = 600
mtp3tstSltmT1 = 60
mtp3tstSltmT2 = 600
mtp3UnhAckT12 = 10
reference = ANSI92
rudpAck = enable
rudpKeepAlives = enable
rudpNumRetx = 2
rudpRetxTimer = 6
rudpSdm = enable
rudpWindowSz = 32
```

Step 2 Verify the MTP3 timers settings listed against the MTP3 timers used at the associated destination.

If the MTP3 timers settings match, your signaling problem has different cause. Continue troubleshooting the problem.

If the MTP3 timers settings do not match, perform the procedure in the "Modifying MTP3 Timers" section on page 8-66.

Modifying MTP Timer Settings

As of Release 7.4(12), you can modify the settings for the MTP timers. For more information, refer to the *Release Notes for the Cisco Media Gateway Controller Software*.

When resolving signaling problems between the Cisco MGC and an associated SS7 network element (such as an STP), you may need to modify the MTP2 and MTP3 timer settings on the Cisco MGC, so that they conform to the settings used by that SS7 network element. You use MML commands to modify the settings for the MTP2 and MTP3 timers. The following subsections describe methods for modifying the settings of the MTP timers on the Cisco MGC.

The procedure used to modify the settings for MTP2 timers varies based on how SS7 signaling is terminated for your Cisco MGC. If you are using Cisco SLTs to terminate SS7 signaling, refer to the "Modifying MTP2 Timers for Cisco SLTs" section on page 8-65. If you are using I/O cards to terminate SS7 signaling, refer to the "Modifying MTP2 Timers for I/O Cards" section on page 8-66. The procedure for modifying MTP3 timers is the same for both SS7 signaling termination methods.

Note Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information on the MTP timers.

You might want to verify the new settings after the modification is complete. To do this, refer to the procedure in the "Verifying MTP Timer Settings" section on page 8-61.

Modifying MTP2 Timers for Cisco SLTs

Use the following MML commands at the Cisco SLT to modify the settings for the MTP2 timers:

```
Router (config)#ss7 mtp-variant standard channel
Router(config-standard)# parameters
```

Where:

- *standard*—Name of the SS7 standards used for your links. Valid values are Bellcore, ITU, NTT, and TTC
- *channel*—Specifies a channel, 0 through 3
- *parameters*—The timer number and the new value for the timer

Note Refer to the *Cisco Signaling Link Terminal* documentation for more information on the parameters for this command.

In the following example, the aligned/ready timer duration on channel 0 is set to 30,000 milliseconds:

```
Router(config)# ss7 mtp2-variant Bellcore 0
Router(config-Bellcore)# T1 30000
```

In the following example, the aligned/ready timer is restored to its default value of 13,000 milliseconds:

```
Router(config)# ss7 mtp2-variant Bellcore 0
Router(config-Bellcore)# no T1
```

You might want to verify the new settings after the modification is complete. To do this, refer to the procedure in the "Verifying MTP2 Timers for Cisco SLTs" section on page 8-62.

Modifying MTP2 Timers for I/O Cards

To modify the settings for the MTP2 timers when you are using I/O cards to provide SS7 signaling links, perform the following steps:

Step 1 Start a provisioning session as described in the "Starting a Provisioning Session" section on page 3-63.

Step 2 Modify the parameters for the desired MTP2 timers by entering the following command:

prov-ed:lnkset:name="*protocol***",***param_name***=***param_value*

Where:

- *protocol*—MML name for the SS7 protocol family being used, such as SS7-ANSI or SS7-ITU.
- *param_name*—Name of the MTP timer you want to change
- *param_value*—New value for the MTP timer

Note Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information on the parameters for this command.

In the following example, the MTP2 T2 timer, maximum period in a Not Aligned state before returning to an OOS state, is set to 120 tenths of a second:

prov-ed:lnkset:name="SS7-ANSI",mtp2T2=120

Step 3 Save and activate your provisioning session as described in the "Saving and Activating your Provisioning Changes" section on page 3-64.

Step 4 Reboot your system as described in the "Rebooting Your System to Modify Properties" section on page 8-124.

Modifying MTP3 Timers

To modify the settings for the MTP3 timers, perform the following steps:

Step 1 Start a provisioning session as described in the "Starting a Provisioning Session" section on page 3-63.

Step 2 Modify the parameters for the desired MTP3 timers by entering the following command:

prov-ed:lnkset:name="*protocol***",***param_name***=***param_value*

Where:

- *protocol*—MML name for the SS7 protocol family being used, such as SS7-ANSI or SS7-ITU.
- *param_name*—Name of the MTP timer you want to change
- *param_value*—New value for the MTP timer

Note Refer to the *Cisco Media Gateway Controller Software Release 7 Provisioning Guide* for more information on the parameters for this command.

In the following example, the MTP3 T1 timer, waiting for signaling link test acknowledgment message, is set to 65 tenths of a second:

```
prov-ed:lnkset:name="SS7-ANSI",mtp3tstSltmT1=65
```

Step 3 Save and activate your provisioning session as described in the "Saving and Activating your Provisioning Changes" section on page 3-64.

Step 4 Reboot your system as described in the "Rebooting Your System to Modify Properties" section on page 8-124.

Managing Japanese SS7 Signaling Link Tests

The following subsections detail the procedures used to manage the tests that can be run on a signaling link configured for Japanese SS7:

Starting an Japanese SS7 Signaling Link Test

To start a signaling link test on a link configured for Japanese SS7, log in to the active Cisco MGC, start an MML session, and enter the following command:

sta-ss7-slt:*link*

Where *link* is the MML name of a link configured for Japanese SS7.

For example, to start a signaling link test on a link called ls1-link1, you would enter the following command:

```
sta-ss7-slt:ls1-link1
```

Retrieving Results for a Japanese SS7 Signaling Link Test

To retrieves the results of a Japanese SS7 signaling link test, log in to the active Cisco MGC, start an MML session, and enter the following command:

rtrv-ss7-slt:*link*

Where *link* is the MML name of a link configured for Japanese SS7.

For example, to retrieve the results of a signaling link test run on a link called ls1-link1, you would enter the following command:

```
rtrv-ss7-slt:ls1-link1
```

The system returns a result that indicates the name of the link and the status of the signaling link test. The valid status responses are listed below:

- TEST PASSED
- TEST FAILED (reasons for failure may be any of the following:)
  - TEST TIMEOUT
  - LINK INACTIVE
  - LINKSET INACTIVE

  - ROUTE UNAVAILABLE
  - INVALID TEST PATTERN
  - INVALID SLC
  - FLOW CONTROL ON
  - UNKNOWN REASON
- COMPLETED *hh:mm:ss*
- TEST RUNNING

For example, here is a sample response to a signaling link test run on a link called ls1-link1:

```
Media Gateway Controller  - MGC-01 2000-01-12 15:18:41
M  RTRV
   "ls1link1:TEST PASSED; COMPLETED 15:18:34"
```

Managing Japanese SS7 Signaling Route Tests

The following subsections detail the procedures used to manage the tests that can be run on a signaling route configured for Japanese SS7:

- Starting a Japanese SS7 Signaling Route Test, page 8-68
- Retrieving Results for a Japanese SS7 Signaling Route Test, page 8-68

Starting a Japanese SS7 Signaling Route Test

To start a signaling route test on a route configured for Japanese SS7, log in to the active Cisco MGC, start an MML session, and enter the following command:

sta-ss7-srt:*pt_code***:lset="***linkset***"**

Where:

- *pt_code*—MML name of an adjacent point code (APC) or destination point code (DPC) configured for Japanese SS7.
- *linkset*—MML name of a linkset associated with the specified destination.

For example, to start a signaling route test on a point code called dpc1 associated with a linkset called ls1, you would enter the following command:

sta-ss7-srt:dpc1:lset="ls1"

Retrieving Results for a Japanese SS7 Signaling Route Test

To retrieves the result of a Japanese SS7 signaling route test, log in to the active Cisco MGC, start an MML session, and enter the following command:

rtrv-ss7-srt:*pt_code***:lset="***linkset***"**

Where:

- *pt_code*—MML name of an adjacent point code (APC) or destination point code (DPC) configured for Japanese SS7.
- *linkset*—MML name of a linkset associated with the specified destination.

For example, to retrieve the results of a signaling route test run on a point code called dpc1 associated with a linkset called ls1, you would enter the following command:

```
rtrv-ss7-srt:dpc1:lset="ls1"
```

The system returns a result that indicates the name of the link and the status of the signaling route test. The valid status responses are listed below:

- TEST PASSED
- TEST FAILED (reasons for failure may be any of the following:)
  - TEST TIMEOUT
  - LINK INACTIVE
  - LINKSET INACTIVE
  - ROUTE UNAVAILABLE
  - INVALID TEST PATTERN
  - INVALID SLC
  - FLOW CONTROL ON
  - UNKNOWN REASON
- COMPLETED *hh:mm:ss*
- TEST RUNNING

For example, here is a sample response to a signaling route test run on a point code called dpc1 associated with a linkset called ls1:

```
Media Gateway Controller  - MGC-01 2000-01-12 15:20:09
M  RTRV
   "dpc1:TEST FAILED; TEST TIMEOUT; COMPLETED 15:20:01"
```

Verifying Proper Loading of a Dial Plan

Step 1 Search the active system log file, as described in the "Viewing System Logs" section on page 8-4, for logs that indicate that the dial plan was loaded incorrectly.

If the dial plan was not loaded correctly, reload the dial plan using the **chg-dpl** MML command. Refer to the *Cisco Media Gateway Controller Software Release 7 Dial Plan Guide* for more information.

If there are no logs that indicate that the dial plan was loaded incorrectly, then proceed to Step 2.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

Bearer Channel Connection Problems

Bearer channels are the focus of everything that the Cisco MGC does. The main function of the Cisco MGC is to ensure that an ingress bearer channel at one endpoint can be successfully connected to an egress bearer channel at another endpoint.

The state of the bearer channels is often a good indicator of the overall health of the system. Procedures for determining the state of your bearer channels can be found in the "Verifying CIC States" section on page 3-13.

Troubleshooting Bearer Channel Connection Procedures

The following sections contains procedures that are related to resolving problems associated with the Cisco MGC node's bearer channel connections:

Setting the Administrative State

You can use the **set-admin-state** MML command to change the administrative state of various components. A platform info log is generated every time the **set-admin-state** MML command is entered. An alarm is generated every time the **set-admin-state** MML command is entered at either the Cisco MGC, media gateway, signaling service, or trunk group level.

The procedures that describe how to use this command are listed below:

Setting the Administrative State of a Cisco MGC

To set the administrative state of a Cisco MGC, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

set-admin-state:*mgc***:***state*

Where:

- *mgc*—The MML name of the desired Cisco MGC.
- *state*—The desired administrative state. The valid states are listed below:
  - lock—Makes all bearer channels unavailable for call processing. If the state is set to lock, active calls go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed.
  - unlock—Makes all bearer channels available for call processing. If the state is set to unlock, the Cisco MGC becomes available. New calls are allowed to use the unlocked bearer channels.
  - reset—Clears local and remote blocking on all bearer channels and they take on the blocking view of remote side.

For example, to set the administrative state of a Cisco MGC called mgc1 to unlock, enter the following command:

set-admin-state:mgc1:unlock

Step 2 Verify that the state of the Cisco MGC has changed by entering the **rtrv-admin-state** MML command, as described in the "Retrieving the Administrative State of a Cisco MGC" section on page 3-59.

Setting the Administrative State of a Media Gateway

To set the administrative state of an associated media gateway, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

set-admin-state:*gway***:***state*

Where:

- *gway*—The MML name of the desired media gateway.

Note Not all media gateway types are applicable. Supported types are CU, MUX, MGW, and AVM external nodes.

- *state*—The desired administrative state. The valid states are listed below:
  - lock —Makes all bearer channels associated with the media gateway unavailable for call processing. If the state is set to lock, active calls on the affected bearer channels go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed on the affected bearer channels.
  - unlock—Makes all bearer channels associated with the media gateway available for call processing. If the state is set to unlock, the media gateway becomes available. New calls are allowed to use the affected bearer channels.

   - reset—Clears local and remote blocking on the bearer channels associated with the media gateway and these bearer channels take on the blocking view of remote side.

For example, to set the administrative state of a media gateway called sfgway to lock, enter the following command:

```
set-admin-state:sfgway:lock
```

Step 2 Verify that the state of the media gateway has changed by entering the **rtrv-admin-state** MML command, as described in the "Retrieving the Administrative State of a Media Gateway" section on page 3-60.

Setting the Administrative State of a Trunk Group

To set the administrative state of an trunk group, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

set-admin-state:*trkgrp***:***state*

Where:

- *trkgrp*—The MML name of the desired trunk group.

Note This command can only be used for time-division multiplexing (TDM) trunk groups. Allow the corresponding MML name for component type "0020".

- *state*—The desired administrative state. The valid states are listed below:
   - lock —Makes all bearer channels associated with the trunk group unavailable for call processing. If the state is set to lock, active calls on the affected bearer channels go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed on the affected bearer channels.
   - unlock—Makes all bearer channels associated with the trunk group available for call processing. If the state is set to unlock, the media gateway becomes available. New calls are allowed to use the affected bearer channels.
   - reset—Clears local and remote blocking on the bearer channels associated with the trunk group and these bearer channels take on the blocking view of remote side.

For example, to set the administrative state of a trunk group called trunkgrp1 to lock, enter the following command:

```
set-admin-state:trunkgrp1:lock
```

Step 2 Verify that the state of the trunk group has changed by entering the **rtrv-admin-state** MML command, as described in the "Retrieving the Administrative State of a Trunk Group" section on page 3-60.

Setting the Administrative State of a Signaling Service

To set the administrative state of a signaling service, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

set-admin-state:*sig_srv***:***state*

Where:

- *sig_srv*—The MML name of the desired signaling service. The following signaling service types are valid for this command:
  - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
  - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
  - Signaling service or routeset associated with a DPC.
  - EISUP signaling service.
- *state*—The desired administrative state. The valid states are listed below:
  - lock —Makes all bearer channels associated with the signaling service unavailable for call processing. If the state is set to lock, active calls on the affected bearer channels go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed on the affected bearer channels.
  - unlock—Makes all bearer channels associated with the signaling service available for call processing. If the state is set to unlock, the media gateway becomes available. New calls are allowed to use the affected bearer channels.

For example, to set the administrative state of a signaling service called nassrv1 to lock, enter the following command:

set-admin-state:nassrv1:lock

Step 2 Verify that the state of the Cisco MGC has changed by entering the **rtrv-admin-state** MML command, as described in the "Retrieving the Administrative State of a Signaling Service" section on page 3-60.

Setting the Administrative State of Spans

To set the administrative state of a single span, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

set-admin-state:*sig_srv***:span=***x***:***state*

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
  - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.

  - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
  - Signaling service or routeset associated with a DPC.
  - EISUP signaling service.
- *x*—A16-bit value that identifies an ISDN/PRI physical cable.
- *state*—The desired administrative state. The valid states are listed below:
  - lock —Makes all bearer channels associated with the span unavailable for call processing. If the state is set to lock, active calls on the affected bearer channels go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed on the affected bearer channels.
  - unlock—Makes all bearer channels associated with the span available for call processing. If the state is set to unlock, the span becomes available. New calls are allowed to use the affected bearer channels.

For example, to set the administrative state of span number 2 associated with a signaling service called ss7svc1 to unlock, you would enter the following command:

```
set-admin-state:ss7svc1:span=2:lock
```

Step 2 Verify that the state of the bearer channels have changed by entering the **rtrv-admin-state** MML command, as described in the "Retrieving the Administrative State of Spans" section on page 3-61.

To set the administrative state of a bearer channel or a range of bearer channels in a span, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-admin-state:sig_srv:span=x,bc=y[,rng=range]:state
```

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
  - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
  - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
  - Signaling service or routeset associated with a DPC.
  - EISUP signaling service.
- *x*—A16-bit value that identifies an ISDN/PRI physical cable.
- *y*—A numeric value that identifies the non-ISUP bearer channel number.
- *range*—A value such that *y*+*range* is a valid bearer channel number. The administrative state for all bearer channels between *y* and *y*+*range* are retrieved.
- *state*—The desired administrative state. The valid states are listed below:

- lock—Makes the specified bearer channels unavailable for call processing. If the state is set to lock, active calls on the affected bearer channels go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed on the affected bearer channels.
- unlock—Makes the specified bearer channels available for call processing. If the state is set to unlock, the bearer channels become available. New calls are allowed to use the affected bearer channels.

For example, to set the administrative state of bearer channels numbers 2 through 6, associated with a signaling service called ss7svc1, to unlock, you would enter the following command:

```
rtrv-admin-state:ss7svc1:span=2,bc=2,rng=5:unlock
```

Step 2 Verify that the state of the bearer channels have changed by entering the **rtrv-admin-state** MML command, as described in the "Retrieving the Administrative State of Spans" section on page 3-61.

Setting the Administrative State of CICs

To set the administrative state of a CIC or a range of CICs, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

set-admin-state:*sig_srv***:cic=***number***[,rng=***range***]:***state*

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
  - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
  - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
  - Signaling service or routeset associated with a DPC.
  - EISUP signaling service.
- *number*—A valid CIC number.
- *range*—A value such that *y+range* is a valid CIC number. The administrative state for all CICs between *y* and *y+range* are retrieved.
- *state*—The desired administrative state. The valid states are listed below:
  - lock—Makes all bearer channels associated with the CICs unavailable for call processing. If the state is set to lock, active calls on the affected bearer channels go into pending state, where calls remain up until either party voluntarily releases the call. New calls are disallowed on the affected bearer channels.
  - unlock—Makes all bearer channels associated with the CICs available for call processing. If the state is set to unlock, the CICs become available. New calls are allowed to use the affected bearer channels.
  - reset—Clears local and remote blocking on the bearer channels associated with the CICs and these bearer channels take on the blocking view of remote side.

For example, to set the administrative state of CICs 2 through 11, associated with a signaling service called ss7svc1, to lock, you would enter the following command:

set-admin-state:ss7svc1:cic=2,rng=9:lock

Step 2 Verify that the state of the Cisco MGC has changed by entering the **rtrv-admin-state** MML command, as described in the "Retrieving the Administrative State of CICs" section on page 3-62.

Querying Local and Remote CIC States

In the course of troubleshooting problems with your bearer channels, you may need to query the local and remote states of the related CICs, to verify that they match. To query the local and remote states of a single CIC or a range of CICs, log in to the active Cisco MGC, start an MML session, and enter the following command:

query-cic:*pt_code***:cic=***number***[,rng=***range***]**

Where:

- *pt_code*—The MML name for the point code associated with the affected CICs.
- *number*—The number of the first CIC in the range of affected CICs.
- *range*—A number such that *number+range* is the number of the last CIC in the range of affected CICs. All CICs between *number* and *number+range* are displayed.

Note Not all SS7 variants support the querying of CICs. If this command is executed on a signaling service that is configured for an SS7 variant that does not support the querying of CICs, an error code, SABT, is returned once the query operation times out. Refer to the *Cisco Media Gateway Controller Software Release 7 MML Command Reference Guide* for more information on the SABT error code.

Note The Cisco MGC software can be configured to issue individual or group supervision messages for point codes that are associated with an ISUP signaling service. ISUP signaling services issue group supervision messages by default. If an ISUP signaling service is configured to issue individual supervision messages, the *range* option cannot be used with this command. Querying of CICs associated with an ISUP signaling service configured to issue individual supervision messages can only be done one CIC number at a time.

For example, to query the state of CICs 20 through 24, associated with a point code called dpc1, you would enter the following command:

query-cic:dpc1:cic=20,rng=4

The system responds with a message similar to the following:

```
Media Gateway Controller  - MGC-01 2000-01-12 15:19:51
M  RTRV
   "dpc1:CIC=20;LPST=IS;LSST=IDLE;RPST=IS;RSST=IDLE"
   "dcp1:CIC=21;LPST=IS;LSST=IDLE;RPST=IS;RSST=IDLE"
   "dpc1:CIC=22;LPST=IS;LSST=IDLE;RPST=IS;RSST=IDLE"
   "dpc1:CIC=23;LPST=IS;LSST=IDLE;RPST=IS;RSST=IDLE"
   "dpc1:CIC=24;LPST=OOS;LSST=IDLE_LOC_BLOC;RPST=IS;RSST=IDLE"
```

The response lists the local and remote primary and secondary states of the requested CICs. If the response indicates that the mismatch is due to a problem on the local side, you can attempt to resolve the state mismatch using the instructions in the "Resolving Local and Remote CIC State Mismatch" section on page 8-77. If the response indicates that the mismatch is due to a problem on the remote side, you must contact the personnel at the remote site to resolve the problem.

The valid values for the fields found in the response to this command are as follows:

- LPST and RPST—Local primary state and remote primary state
  - IS—In-Service
  - OOS—Out-of-Service
  - TRNS—Transient; the state is currently being changed
- LSST and RSST—Local secondary state and remote secondary state
  - N/A—Not available
  - UNEQUIPPED—Unequipped
  - IC_BUSY—Incoming is busy
  - IC_BUSY_LOC_BLOC—Incoming is busy, blocked locally
  - IC_BUSY_REM_BLOC—Incoming is busy, blocked remotely
  - IC_BUSY_BOTH_BLOC—Incoming is busy, blocked both remotely and locally
  - OG_BUSY—Outgoing is busy
  - OG_BUSY_LOC_BLOC—Outgoing is busy, blocked locally
  - OG_BUSY_REM_BLOC—Outgoing is busy, blocked remotely
  - OG_BUSY_BOTH_BLOC—Outgoing is busy, blocked both remotely and locally
  - IDLE—The circuit is idle, available for use
  - IDLE_LOC_BLOC—Idle, blocked locally
  - IDLE_REM_BLOC—Idle, blocked locally
  - IDLE_BOTH_BLOC—Idle, blocked both locally and remotely

Resolving Local and Remote CIC State Mismatch

When the local and remote states for CICs do not match and the problem lies with the local CIC states, you can attempt to resolve the mismatch using an MML command. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

```
query-cic:pt_code:cic=number[,rng=range],rslv
```

Where:

- *pt_code*—The MML name for the point code associated with the affected CICs.
- *number*—The number of the first CIC in the range of affected CICs.
- *range*—A number such that *number+range* is the number of the last CIC in the range of affected CICs. The system attempts to resolve state mismatches for all CICs between *number* and *number+range*.

Note The **rslv** option can only be used if your system used ANSI SS7 signaling. If your system uses ITU SS7 signaling and you use this command, the **rslv** option is ignored and a regular **query-cic** operation is performed.

Note The Cisco MGC software can be configured to issue individual or group supervision messages for point codes that are associated with an ISUP signaling service. ISUP signaling services issue group supervision messages by default. If an ISUP signaling service is configured to issue individual supervision messages, the *range* option cannot be used with this command. Resolving of local and remote CIC state mismatch can only be done one CIC number at a time for point codes associated with an ISUP signaling service configured to issue individual supervision messages.

If the command fails in its attempt to resolve the local and remote CIC state mismatch, contact the Cisco TAC for assistance. Refer to the "Obtaining Technical Assistance" section on page xviii for more information about contacting the Cisco TAC.

Performing CIC Validation Tests

When performing initial turn-up of circuits or in troubleshooting certain problems with your bearer channels, you may want to perform a circuit validation test to verify that the properties defined in the Cisco MGC for the affected bearer channels match the associated properties defined in the far-end exchange.

Note CIC validation tests can only be performed on CICs associated with ANSI SS7-based DPCs.

To perform a circuit validation test, complete the following steps:

Step 1 Start an MML session on the active Cisco MGC and validate the properties for a particular circuit identification code (CIC) using the following command:

vld-cic:*dest_pc***:cic=***number*

Where:

- *dest_pc*—The MML name for the DPC associated with the affected CIC.
- *number*—The trunk identification number for the affected CIC.

If the circuit validation test is passed, the system returns a message similar to the following:

```
Media Gateway Controller - MGC-01 2000-03-07 09:35:19
 M  RTRV
    "dms100-pc:CIC=105,PASSED"
```

If the circuit validation test is failed, the system returns a message similar to the following:

```
Media Gateway Controller - MGC-01 2000-03-07 09:35:19
 M  RTRV
    "dms100-pc:CIC=105,FAIL"
    LOC: GRP=DIG,SEIZ=EVEN,ALM=UNK,COT=NONE
    LOC: TRK=1003,A_CLLI=dms1003****,Z_CLLI=na*********
    REM: GRP=DIG,SEIZ=ODD,ALM=SOFT,COT=STAT
```

The fields in the LOC line are values associated with the Cisco MGC. The fields in the REM line are values associated with the far-end exchange. The valid values for those fields are described below.

- GRP—Circuit group carrier indicator. The values in these fields should be the same in the LOC and REM lines. The valid values for this field are:
  - UNK—Unknown circuit group carrier type
  - ANL—Analog circuit group carrier type
  - DIG—Digital circuit group carrier type
  - AND—Analog and digital circuit group carrier type
- SIEZ—Double seizing indicator. The values for this field in the LOC line should be logically opposite to the value for the REM line. The valid values for this field are:
  - NONE—No circuit control. When one line is set to NONE, the other should be set to ALL.
  - ALL—All circuit control. When one line is set to ALL, the other should be set to NONE.
  - EVEN—Even circuit control. When one line is set to EVEN, the other should be set to ODD.
  - ODD—Odd circuit control. When one line is set to ODD, the other should be set to EVEN.
- ALM—Alarm carrier indicator. The values in these fields should be the same in the LOC and REM lines. The valid values for this field are:
  - UNK—Unknown alarm carrier
  - SOFT—Software alarm carrier
  - HARD—Hardware alarm carrier
- COT—Continuity check requirements indicator. The values in these fields should be the same in the LOC and REM lines. The valid values for this field are:
  - UNK—Unknown continuity check requirements
  - NONE—No continuity check requirements
  - STAT—Statistical continuity check requirements
  - PERC—Per call continuity check requirements
- TRK—Trunk number. This field is always displayed in the LOC line. It is only displayed in the REM line when the circuit identification names for the Cisco MGC and the far-end exchange do not match.
- A_CLLI—Common language location identifier (CLLI) code for either the far-end exchange or the Cisco MGC. The CLLIs for each are sorted alphabetically, and the A_CLLI field is populated with the CLLI that is found to be first. This field is always displayed in the LOC line. It is displayed in the REM line only when the CLLIs for the Cisco MGC and the far-end exchange do not match.
- Z_CLLI—CLLI code for either the far-end exchange or the Cisco MGC. The CLLIs for each are sorted alphabetically, and the Z_CLLI field is populated with the CLLI that is found to be second. This field is always displayed in the LOC line. It is displayed in the REM line only when the CLLIs for the Cisco MGC and the far-end exchange do not match.

If the circuit validation test passes, proceed to Step 14.

If the circuit validation test fails, proceed to Step 2.

Step 2 Determine which settings are not correct by comparing the values displayed in the LOC field (from the Cisco MGC) to those in the REM field (from the associated far-end exchange), based on the field descriptions found above.

Step 3 Consult your provisioning records to determine whether the settings on the Cisco MGC and/or the associated far-end exchange need to be modified to resolve the error.

If the settings on the Cisco MGC need to be modified to resolve the error, proceed to Step 4.

If the settings on the associated far-end exchange need to be modified to resolve the error, contact the provider that operates the switch and work with them to resolve the configuration error.

Step 4 Identify the signaling service associated with the affected DPC using the following command:

prov-rtrv:ss7path:"all"

The system returns a message similar to the following:

```
mgc-01 - Media Gateway Controller 2000-09-26 15:55:17
M RTRV
"session=active:ss7path"
/*
NAME      DPC        MDO              CUSTGRPID CUSTGRPTBL SIDE
----      ---        ---              --------- ---------- ----
ss7am401a am401a-pc  ANSISS7_STANDARD 0000      0101       network
ss7am702b am702b-pc  ANSISS7_STANDARD 0000      0101       network
ss7inet1  inetsp1-pc ANSISS7_STANDARD 0000      0101       network
ss7am408a am408a-pc  ANSISS7_STANDARD 0000      0101       network
ss7am408b am408b-pc  ANSISS7_STANDARD 0000      0101       network
ss7inet2  inetsp2-pc ANSISS7_STANDARD 0000      0101       network
ss7dms    dms100-pc  ANSISS7_STANDARD 0000      0101       network
ss7am401b am401b-pc  ANSISS7_STANDARD 0000      0101       network
ss7am608b am608b-pc  ANSISS7_STANDARD 0000      0101       network
ss7sc2200 sc2200-pc  ANSISS7_STANDARD 0000      0101       network
```

The response lists the SS7 signaling services and their associated DPCs. Search for the DPC associated with the trunk to identify the name of the SS7 signaling service. In the example, **dms100-pc** is the name of the DPC associated with the trunk. The SS7 signaling service names are in the column to the immediate left of the DPCs, so the name of the associated SS7 signaling service in the example is **ss7dms**.

Step 5 Identify the MML names of the mismatched settings for the affected signaling service found in Step 4 using the following command:

prov-rtrv:sigsvcprop:name="*sig_serv*"

Where *sig_serv* is the MML name of the affected signaling service.

The system returns a message similar to the following:

```
MGC-01 - Media Gateway Controller 2000-09-26 15:57:29
M RTRV
"session=active:sigsvcprop"
/*
adjDestinations = 16
AlarmCarrier = 0
BOrigStartIndex = 0
BothwayWorking = 1
BTermStartIndex = 0
CctGrpCarrier = 2
CGBA2 = 0
CircHopCount = 0
CLIPEss = 0
CotInTone = 2010
CotOutTone = 2010
CotPercentage = 0
dialogRange = 0
ExtCOT = Loop
ForwardCLIinIAM = 1
ForwardSegmentedNEED = 1
GLARE = 0
GRA2 = 0
```

```
GRSEnabled = false
InternationalPrefix = 0
layerRetries = 2
layerTimer = 10
maxMessageLength = 250
mtp3Queue = 1024
NationalPrefix = 0
NatureOfAddrHandling = 0
Normalization = 0
OMaxDigits = 24
OMinDigits = 0
OOverlap = 0
OwnClli = na
RedirMax = 3
restartTimer = 10
RoutePref = 0
sendAfterRestart = 16
slsTimer = 300
srtTimer = 300
sstTimer = 300
standard = ANSI92
SwitchID = 0
TMaxDigits = 24
TMinDigits = 0
TOverlap = 0
variant = SS7-ANSI
VOIPPrefix = 0
```

The response above can be mapped to the response to the circuit validation test in Step 1, as listed below:

- CctGrpCarrier—The value in this field maps to the value in the GRP field, as follows:
  - 0—Equal to UNK (unknown carrier) in the GRP field.
  - 1—Equal to ANL (analog carrier) in the GRP field.
  - 2—Equal to DIG (digital carrier) in the GRP field.
  - 3—Equal to AND (analog and diglossia carrier) in the GRP field.
- Glare—The value in this field maps to the value in the SEIZ field, as follows:
  - 0 or 3—Equal to NONE (no circuit control) in the SEIZ field.
  - 1—Equal to ALL (all circuit control) in the SEIZ field.
  - 2—Equal to ODD (odd circuit control) in the SEIZ field when the OPC is less than the associated DPC. Equal to EVEN (even circuit control) in the SEIZ field when the OPC is greater than the associated DPC.
- AlarmCarrier—The value in this field maps to the value in the ALM field, as follows:
  - 0—Equal to UNK (unknown) in the ALM field.
  - 1—Equal to SOFT (software handling) in the ALM field.
  - 2—Equal to HARD (hardware handling) in the ALM field.
- CotPercentage and ExtCOT—The values in these field maps to the value in the COT field, as follows:
  - CotPercentage is undefined and ExtCOT is *not* set to *Loop* or *Transponder*—Equal to UNK (unknown continuity check requirements) in the COT field.
  - CotPercentageis set to any value and ExtCOT is not set to *Loop* or *Transponder*—Equal to NONE (no continuity check requirements) in the COT field.

- CotPercentage is greater than 0 and less than 100 and ExtCOT is set to *Loop* or *Transponder*—Equal to STAT (statistical continuity check requirements) in the COT field.
- CotPercentage is set to 100 and ExtCOT is set to *Loop* or *Transponder*—Equal to PERC (per call continuity check requirements) in the COT field.

Step 6 Start a provisioning session as described in the "Starting a Provisioning Session" section on page 3-63.

Step 7 Modify the appropriate signaling service settings using the following command:

prov-ed:sigsvcprop:name="*sig_svc***",***param_name***="***param_value***",***param_name***="***param_value***",...**

Where:

- *sig_svc*—The MML name for the affected signaling service.
- *param_name*—The MML name for a mismatched setting.
- *param_value*—The correct value for a mismatched setting.

For example, to change the settings for the COT to per call and seizing (glare) to no circuit control for the ss7dms signaling service, you would enter the following command:

prov-ed:sigsvcprop:name="ss7dms",ExtCOT="Loop", CotPercentage="100",GLARE="0"

Step 8 If your Cisco MGC is provisioned for a switched environment and you need to modify the COT and/or seizing (glare) properties, the trunk group properties need to be modified.

If you need to modify the trunk group properties, proceed to Step 9.

If you do not need to modify the trunk group properties, proceed to Step 12.

Step 9 Identify the trunk group associated with the affected DPC using the following command:

prov-rtrv:trnkgrp:svc="*sig_serv***"**

Where: *sig_serv*—The MML name of the SS7 signaling service identified in Step 4.

The system returns a message similar to the following:

```
MGC-01 - Media Gateway Controller 2000-09-26 15:55:17
M RTRV
"session=active:trnkgrp"
/*
NAME   CLLI       SVC     TYPE       SELSEQ    QABLE
----   ---        ---     -----      ------    ------
1003   DMS100CLLIss7dms   TDM_ISUP   ASC       N
```

The response lists the trunk group associated with the affected SS7 signaling service. The MML name of the trunk group is found in the NAME column. In the example, **ss7dms** is the name of the SS7 signaling service associated with the trunk. The trunk group names are in the first column, so the name of the associated trunk group in the example is **1003**.

Step 10 Identify the MML names of the mismatched settings for the affected trunk group found in Step 9 using the following command:

prov-rtrv:trnkgrpprop:name="*trnk_grp***"**

Where: *trnk_grp*—The MML name of the affected trunk group.

The system returns a message similar to the following:

```
mgc-01 - Media Gateway Controller 2000-09-26 15:57:29
M RTRV
"session=active:trnkgrpprop"
/*
BOrigStartIndex = 1
BTermStartIndex = 2
```

```
CarrierIdentity = 0333
CLLI = GR31764KB5
CompressionType = 1
CotPercentage = 1
CustGrpId = V123
EchoCanRequired = 0
ExtCOT = Loop
GLARE = 2
Npa = 919
RingNoAnswer = 100000
SatelliteInd = 0
ScreenFailAction = 0
*/
```

Step 11 Modify the appropriate trunk group settings using the following command:

prov-ed:trnkgrp:name="*trnk_grp***",***param_name***="***param_value***",***param_name***="***param_value***",...**

Where:

- *trnk_grp*—The MML name for the affected trunk group.
- *param_name*—The MML name for a mismatched setting.
- *param_value*—The correct value for a mismatched setting.

Note The values for the COT and/or seizing properties entered here should match the values set in Step 7.

For example, to change the settings for the COT to per call and seizing (glare) to no circuit control for the trnkgrpdms trunk group, you would enter the following command:

prov-ed:ztrnkgrp:name="trnkgrpdms",ExtCOT="Loop", CotPercentage="100",GLARE="0"

Step 12 Activate your new configuration as described in the "Saving and Activating your Provisioning Changes" section on page 3-64.

Step 13 Return to Step 1 and enter the **vld-cic** command again.

If the response indicates that the test has passed, proceed to Step 14.

If the response indicates that the test has failed, resume performing this procedure from Step 2 and modify the mismatched settings identified in the latest command response.

Step 14 Repeat Steps 1 through 13 for each additional CIC you want to test.

Resolving ISDN D-Channel Discrepancies

When there is a mismatch between the D-channels configured on the Cisco MGC and those configured on the associated media gateway, an ISDN log message is generated. To resolve the log message, complete the following steps:

Step 1 Enter the following command at the active Cisco MGC to change directories:

cd $BASEDIR/etc

Step 2 Determine the component IDs associated with the D-channel number identified in the log text by searching for the D-channel number in the data files.

For example, if the log message contains the following text:

```
PROT_ERR_ISDN:Error message from ISDN:Receive MGMT_ERROR_IND for set 1, channel 2854
```

The D-channel number in the example is **2854**. Therefore, you would search for occurrences of D-channel **2854** in the data files.

Enter the following command to search the data files for the identified D-channel number:

```
grep d_num *.dat
```

Where *d_num* is the D-channel number identified in the alarm message.

The system returns a message similar to the following:

```
sigChanDev.dat:001002bd  00160002  1  0034015e  00030011  00060001  2854
sigChanDev.dat:001002be  00160002  1  0034015e  00030011  00060002  2854
```

The response lists the data file(s) in which the D-channel number found, along with the associated properties. In the example above, the D-channel number, **2854**, is found twice in the **sigChanDev.dat** file. The component IDs are in the column immediately following the data file name. So, in this example, the component IDs are **001002bd** and **001002be**.

Step 3 Determine the MML name of an IP link associated with one of the component IDs you identified in Step 2 using the following command:

```
grep comp_ID components.dat
```

Where: *comp_ID* — A component ID identified in Step 2.

The system returns a message similar to the following:

```
001002bd  0034015e  "bh531-31"             "IP link-backhaul svc mgx8260 EAST"
```

The response lists the properties associated with your selected component ID. The MML name for the IP link is in the third column in the response. In the above example, **"bh531-31"** is the MML name for the IP link.

Step 4 Repeat Step 3 for each component ID identified in Step 2.

Step 5 Start an MML session from the active Cisco MGC and enter the following command to determine the MML name for the signaling service associated with the IP link(s) identified in Step 3:

```
prov-rtrv:iplnk:name="ip_link"
```

Where: *ip_link* — The MML name for an IP link(s) identified in Step 3.

The system returns a message similar to the following:

```
Media Gateway Controller 2000-06-08 13:49:53
 M  RTRV
    "session=active:iplnk"
    /*
 NAME = bh531-31
 DESC = IP link-backhaul svc mgx8260 EAST
 SVC = bh531-3
 IF = enif1
 IPADDR = IP_Addr1
 PORT = 7007
 PEERADDR = 10.15.26.20
 PEERPORT = 7007
 PRI = 1
 SIGSLOT = 11
 SIGPORT = 38
    */
```

The response lists the properties associated with your selected IP link. The MML name for the signaling service associated with the link is in the SVC field. In the above example, **bh531-3** is the MML name for the signaling service. Note the values in the SIGSLOT and SIGPORT fields. These values are used later to determine whether the D-channel is defined on the media gateway.

Step 6 Enter the following command to retrieve the properties for the signaling service identified in Step 5:

rtrv-dest:*sig_serv*

Where *sig_serv* is the MML name for a signaling service identified in Step 5.

The system returns a message similar to the following:

```
Media Gateway Controller 2000-06-08 13:50:26
 M  RTRV
    "bh531-3:PKG=ISDNPRI,ASSOC=SWITCHED,PST=OOS,SST=UND"
```

Step 7 Log into the associated media gateway and determine whether the D-channel is defined. Refer to the documentation for the media gateway for information on how to verify whether the D-channel is defined.

For example, to determine whether a D-channel is defined for a Cisco MGX8260 media gateway, you would enter the following command:

lsdchan 12.39

The values, **12.39**, specify the D-channel. These numbers are determined by adding 1 to the SIGSLOT and SIGPORT values identified in Step 5.

The media gateway responds with a message that indicates whether the D-channel is defined.

Step 8 Consult your provisioning records and determine whether the identified D-channel should exist.

If your provisioning records indicate that the D-channel should exist, proceed to Step 9.

If your provisioning records indicate that the D-channel should *not* exist, proceed to Step 10.

Step 9 Define the D-channel on the associated media gateway. Refer to the documentation for the media gateway for information on how to define a D-channel.

The procedure is finished.

Step 10 Start a provisioning session as described in the "Starting a Provisioning Session" section on page 3-63.

Step 11 Delete the appropriate D-channel(s) using the following command:

prov-dlt:iplnk:name="*ip_link***",...**

Where *ip_link* is the MML name(s) for an IP link identified in Step 3.

For example, to delete a D-channel named bh531-31, you would enter the following command:

prov-dlt:iplink:name="bh531-31"

Step 12 Delete the signaling service associated with the D-channel(s) using the following command:

prov-dlt:ipfaspath:name="*sig_serv***"**

Where *sig_serv* is the MML name for a signaling service identified in Step 5.

For example, to delete a signaling service named bh531-3, you would enter the following command:

prov-dlt:ipfaspath:name="bh531-3"

Step 13 Activate your new configuration as described in the "Saving and Activating your Provisioning Changes" section on page 3-64.

Unblocking CICs

You may need to unblock a CIC or a range of CICs on your Cisco MGC. There are two types of blocking on a CIC, local and remote.

Unblocking Locally Blocked CICs

To unblock a single CIC, log in to your active Cisco MGC, start an MML session and enter the following command:

unblk-cic:*dest_pc***:CIC=***number*

Where:

- *dest_pc*—The MML name of the DPC associated with the CICs to be unblocked.
- *number*—The number of the affected CIC.

For example, to unblock CIC number 2, which is associated with a DPC called dpc1, you would enter the following command:

unblk-cic:dpc1:CIC=2

To unblock a range of CICs, log in to your active Cisco MGC, start an MML session, and enter the following command:

unblk-cic:*dest_pc***:CIC=***number***,RNG=***range*

Where:

- *point_code*—The MML name of a DPC associated with the CICs you want to unblock.
- *number*—The number of the first CIC in the range of CICs you want to unblock.
- *range*—Specifies the end of the range of CICs to be unblocked.

Note The Cisco MGC software can be configured to issue individual or group supervision messages for point codes that are associated with an ISUP signaling service. ISUP signaling services issue group supervision messages by default. If an ISUP signaling service is configured to issue individual supervision messages, the *range* option cannot be used with this command. Unblocking of CICs can only be done one CIC number at a time for point codes associated with an ISUP signaling service configured to issue individual supervision messages.

For example, to unblock CIC number 1 through 20, which are associated with a DPC called dpc1, you would enter the following command:

unblk-cic:dpc1:cic=1,rng=20

To verify that the CIC(s) have been successfully unblocked, retrieve the status of the affected CICs as described in the "Verifying CIC States" section on page 3-13. If the CIC(s) are still blocked, proceed to the "Resetting CICs" section on page 8-87.

Unblocking Remotely Blocked CICs

Generally, you cannot unblock a CIC that has been blocked remotely, because the block was set on the far-end. However, in some instances, a remotely blocked CIC is misreported, and you can fix this by resetting the CIC as described in the "Resetting CICs" section on page 8-87.

Resetting CICs

When trying to clear a blocked CIC or range of CICs, you may need to perform a reset on the affected CIC(s). To reset a single CIC, log in to your active Cisco MGC, start an MML session and enter the following command:

reset-cic:*dest_pc***:CIC=***number*

Where:

- *dest_pc*—The MML name of the DPC associated with the CICs to be reset.
- *number*—The number of the affected CIC.

For example, to reset CIC number 2, which is associated with a DPC called dpc1, you would enter the following command:

```
reset-cic:dpc1:CIC=2
```

To reset a range of CICs, log in to your active Cisco MGC, start an MML session, and enter the following command:

reset-cic:*dest_pc***:CIC=***number***,RNG=***range*

Where:

- *point_code*—The MML name of a DPC associated with the CICs you want to reset.
- *number*—The number of the first CIC in the range of CICs you want to reset.
- *range*—Specifies the end of the range of CICs to be reset.

Note The Cisco MGC software can be configured to issue individual or group supervision messages for point codes that are associated with an ISUP signaling service. ISUP signaling services issue group supervision messages by default. If an ISUP signaling service is configured to issue individual supervision messages, the *range* option cannot be used with this command. Resetting of CICs can only be done one CIC number at a time for point codes associated with an ISUP signaling service configured to issue individual supervision messages.

For example, to reset CICs number 1 through 20, which are associated with a DPC called dpc1, you would enter the following command:

```
reset-cic:dpc1:cic=1,rng=20
```

To verify that the CIC(s) have been successfully reset, retrieve the status of the affected CICs as described in the "Verifying CIC States" section on page 3-13. If the CIC(s) are still blocked, proceed to the "Resolving Stuck CICs" section on page 8-87.

Resolving Stuck CICs

A stuck or hung CIC is a condition that occurs when one or more bearer channels associated with a single call instance refuses to return to the idle call state, despite attempts to manually clear it down using the **reset-cic** MML command. Stuck CICs are generally caused when transient network glitches or configuration errors trigger protocol state machine errors. Typically these conditions result in a mismatch between the CIC's call state on the Cisco MGC and the call state for the associated span and bearer channel (also known as timeslot) on the media gateway.

The Cisco MGC is capable of automatically detecting and terminating stuck CICs. Refer to the *Release Notes for the Cisco Media Gateway Controller Software* for more information. With the addition of this functionality, the system runs an audit cron job once a day that verifies, using the **sta-aud** MML command, that the call states for the CICs on the Cisco MGC match the associated states for the spans and bearer channels on the media gateway. If the audit finds that the Cisco MGC call states on a CIC show that a call is in progress while the associated media gateway span and bearer channel states are idle, the system attempts to release the identified CIC using the **stp-call** MML command. The **stp-call** MML command monitors for the release of the CIC. If the CIC is not released within 1 to 2 minutes, the CIC is forcefully released. When a CIC is forcefully released, a minimal CDR is written, with a cause of Temporary Failure.

Note If you suspect that you have stuck CICs, and you do not want to wait for the audit cron job to be performed, or if the audit cron job appears to be unable to clear your stuck CICs, perform the steps identified in the "Manually Resolving Stuck CICs" section on page 8-88.

Note The format of the CDR is dependent upon how you have configured the associated XECfgParm.dat configuration parameters. For more information on XECfgParm.dat configuration, refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*. For more information on CDRs, refer to the *Cisco Media Gateway Controller Software Release 7 Billing Interface Guide*.

If you want to run the audit cron job more than once a day, increase the frequency of the audit in the mgcusr crontab entry. You must have system administration authority to use crontab. For more information on crontab, enter the UNIX command, **man crontab**, on your Cisco MGC.

Note The audit cron job will not be run by the system if the call engine's CPU load is greater than the limit set in the XECfgParm.dat file. For more information on XECfgParm.dat configuration, refer to the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

If you are running a release prior to Release 7.4(11), you must contact the Cisco TAC for assistance in clearing stuck CICs. Refer to the "Obtaining Technical Assistance" section on page xviii for more information about contacting the Cisco TAC.

Manually Resolving Stuck CICs

If you want to manually resolve stuck CICs, perform the follow steps:

Step 1 Set the logging level of the call engine process (eng-01) to *info*, using the procedure described in the "Changing the Log Level for Processes" section on page 8-6.

Step 2 Perform a call state audit, using the procedure described in the "Auditing Call States" section on page 8-91.

When you search the active system log file, look for a CP_INFO_CHAN_STATE message containing the following text:

```
NAS is idle, SC is busy
```

An example of this log message appears below:

```
Fri May 25 13:27:45:384 2001 | engine (PID 14217) <Info>
CP_INFO_CHAN_STATE:Mismatch in channel state, NAS is idle, SC is busy, span 0, channel 2
```

If you find this kind of CP_INFO_CHAN_STATE message in the active system log file, proceed to Step 3. Otherwise, contact the Cisco TAC for assistance. Refer to the "Obtaining Technical Assistance" section on page xviii for more information about contacting the Cisco TAC.

Step 3 There should be two associated CP_ERR_AUEP messages, one containing information on the affected span and bearer channel and another containing information on the affected CIC. Search the active system log file for a CP_ERR_AUEP message containing the following text:

```
Audit:failed to audit end point
```

An example of these messages appears below:

```
Fri May 25 13:27:45:384 2001 | engine (PID 14217) <Error>
CP_ERR_AUEP:Audit:failed to audit end point nassvc1[00140001]/0/2

Fri May 25 13:27:45:384 2001 | engine (PID 14217) <Error>
CP_ERR_AUEP:Audit:failed to audit end point dpc1[00130002]/ffff/2
```

In the first message, which contains information on the affected span and bearer channel, the text that immediately follows the word "point" identifies the following:

- The MML name of the media gateway destination associated with the affected span and bearer channel (nasssvc1 in the example).
- The internal hexadecimal code associated with the identified media gateway destination (00140001 in the example). This number appears in brackets.
- The affected span number, in hexadecimal (0 in the example).
- The affected bearer channel number, in hexadecimal (2 in the example).

In the second message, which contains information on the affected CIC, the text that immediately follows the word "point" identifies the following:

- The MML name of the DPC associated with the affected CIC (dpc1 in the example).
- The internal hexadecimal code associated with the identified DPC (00130002 in the example). This number appears in brackets.
- The affected span number, in hexadecimal (ffff in the example). This field for this type of message is always set to "ffff", because there is no correlation to span in SS7 networks.
- The affected CIC number, in hexadecimal (2 in the example).

Step 4 Convert the hexadecimal values for the span, bearer channel, and CIC into decimal values.

Step 5 Using the information gathered in steps 3 and 4, stop the call on an affected CIC for its associated DPC, using the procedure described in the "Stopping Calls on CICs" section on page 8-94.

Step 6 Using the information gathered in steps 3 and 4, stop the call on an affected span and bearer channel for its associated media gateway destination, using the procedure described in the "Stopping Calls on Spans" section on page 8-93.

Step 7 Reset the affected CIC using the procedure in the "Resetting CICs" section on page 8-87.

Step 8 Repeat steps 2 through 7, searching for additional sets of affected CICs, spans, and bearer channels, until you have addressed all of the stuck CICs identified by the call state audit.

Step 9 Repeat steps 2 and 3, performing a second call state audit and searching the active system log file to determine whether the previously identified CICs are still stuck.

If the previously identified CICs are still stuck, proceed to Step 10. Otherwise, proceed to Step 13.

Step 10 Forcefully end the call on the DPC and CICs identified in Step 3 by entering the following command:

kill-call:*dest_pc***:cic=***num***,confirm**

Caution The **kill-call** MML command forcibly ends calls locally. It does not send SS7 messages to the far-end. **Kill-call** should only be used when you are attempting to clear stuck CICs that cannot be cleared using the **stp-call** or **reset-cic** MML commands.

Where:

- *dest_pc*—MML name of the DPC identified in Step 3.
- *num*—Number of the stuck CIC identified in Step 3.

For example, to forcefully stop a call on CIC 215, which is associated with a DPC called dpc1, you would enter the following command:

```
kill-call:dpc1:cic=215,confirm
```

Repeat this step for each CIC you have identified as being stuck.

Step 11 Forcefully end the call on the signaling service, spans, and bearer channels identified in Step 3 by entering the following command:

kill-call:*sig_srv***:span=***span_num***,bc=***bear_chan***,confirm**

Caution The **kill-call** MML command forcibly ends calls locally. It does not send SS7 messages to the far-end. **Kill-call** should only be used when you are attempting to clear stuck CICs that cannot be cleared using the **stp-call** or **reset-cic** MML commands.

Where:

- *sig_srv*—MML name of the signaling service identified in Step 3.
- *span_num*—Number of the span identified in Step 3.
- *bear_chan*—Number of the stuck bearer channel identified in Step 3.

For example, to forcefully stop a call on bearer channel 2, which is on span 2, and is associated with a signaling service called nassvc1, you would enter the following command:

```
kill-call:nassvc1:span=2,bc=2,confirm
```

Repeat this step for each bearer channel you have identified as being stuck.

Step 12 Repeat steps 2 and 3, performing a third call state audit and searching the active system log file to determine whether the previously identified CICs are still stuck.

If the previously identified CICs are no longer stuck, proceed to Step 13. If these CICs are still stuck, perform a call trace as described in "Performing a Call Trace" section on page 8-102, and contact the Cisco TAC for assistance. Refer to the "Obtaining Technical Assistance" section on page xviii for more information about contacting the Cisco TAC.

Step 13 Set the logging level of the call engine (eng-01) to *err*, using the procedure described in the "Changing the Log Level for Processes" section on page 8-6.

Auditing Call States

To run a call state audit, which compares the call states of the CICs on the Cisco MGC with the associated states of the spans and bearer channels on the media gateway, perform the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

```
sta-aud
```

Note The Cisco MGC does not indicate when the **sta-aud** MML command has completed its call state audit process. Wait a few minutes before proceeding to the next step.

The results of the call state audit are sent to the active system log file.

Step 2 View the active system log file as described in the "Viewing System Logs" section on page 8-4. If you see any call state mismatch logs in the active system log file, contact the Cisco TAC for assistance in resolving the call state mismatch. Refer to the "Obtaining Technical Assistance" section on page xviii for more information about contacting the Cisco TAC.

Step 3 Once you have finished audit the call states, enter the following command:

```
stp-aud
```

Stopping Calls

You can use the **stp-call** MML command to stop calls gracefully on all traffic channels associated with a specified system resource. The **stp-call** MML command is described in the following sections:

Note The **stp-call** MML command forcefully stops calls if a calls do not gracefully stop within two minutes of the execution of the command. Refer to the *Release Notes for the Cisco Media Gateway Controller Software* for more information.

Stopping Calls on a Cisco MGC

To stop all active calls on all traffic channels on a Cisco MGC, log in to the active Cisco MGC, start an MML session, and enter the following command:

stp-call:*mgc***,confirm**

Where *mgc* is the MML name of the desired Cisco MGC.

For example, to stop all active calls on all traffic channels on a Cisco MGC called mgc1, enter the following command:

stp-call:mgc1,confirm

Stopping Calls on a Media Gateway

To stop all active calls on all traffic channels on a media gateway, log in to the active Cisco MGC, start an MML session, and enter the following command:

stp-call:*gway***,confirm**

Where *gway* is the MML name of the desired media gateway.

Note Not all media gateway types are applicable. Supported types are CU, MUX, MGW, and AVM external nodes.

For example, to stop all active calls on all traffic channels on a media gateway called sfgway, enter the following command:

stp-call:sfgway

Stopping Calls on a Trunk Group

To stop all active calls on all traffic channels associated with a trunk group, log in to the active Cisco MGC, start an MML session, and enter the following command:

stp-call:*trkgrp***,confirm**

Where *trkgrp* is the MML name of the desired trunk group.

Note This command can only be used for TDM trunk groups. Allow the corresponding MML name for component type "0020".

For example, to stop all active calls on all traffic channels associated with a trunk group called trunkgrp1, enter the following command:

stp-call:trunkgrp1,confirm

Stopping Calls on a Signaling Service

To stop all active calls on all traffic channels associated with a signaling service, log in to the active Cisco MGC, start an MML session, and enter the following command:

stp-call:*sig_srv***,confirm**

Where *sig_srv* is the MML name of the desired signaling service. The following signaling service types are valid for this command:

- For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
- For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
- For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
- Signaling service or routeset associated with a DPC.

- EISUP signaling service.

For example, to stop all active calls on all traffic channels associated with a signaling service called nassrv1, enter the following command:

```
stp-call:nassrv1,confirm
```

Stopping Calls on Spans

To stop all active calls on all bearer channels associated with a single span, log in to the active Cisco MGC, start an MML session, and enter the following command:

stp-call:*sig_srv***:span=***x***,confirm**

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
  - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
  - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
  - Signaling service or routeset associated with a DPC.
  - EISUP signaling service.
- *x*—A16-bit value that identifies an ISDN/PRI physical cable.

For example, to stop all active calls on all bearer channels on a signaling service called ss7svc1 associated with span number 1, enter the following command:

```
stp-call:ss7svc1:span=1,confirm
```

To stop all active calls on a bearer channel, or a range of bearer channels, for a span associated with a signaling service, log in to the active Cisco MGC, start an MML session, and enter the following command:

stp-call:*sig_srv***:span=***x***,bc=***y***[,rng=***range***],confirm**

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
  - For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
  - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
  - Signaling service or routeset associated with a DPC.
  - EISUP signaling service.
- *x*—A16-bit value that identifies an ISDN/PRI physical cable.
- *y*—A numeric value that identifies the non-ISUP bearer channel number.
- *range*—A value such that *y+range* is a valid bearer channel number. The administrative state for all bearer channels between *y* and *y+range* are retrieved.

For example, to stop all active calls on all bearer channel numbers 2 through 6, associated with a signaling service called ss7svc1, enter the following command:

```
stp-call:ss7svc1:span=2,bc=2,rng=5,confirm
```

Stopping Calls on CICs

To stop all active calls on a CIC, or a range of CICs, associated with a signaling service, log in to the active Cisco MGC, start an MML session, and enter the following command:

stp-call:*sig_srv***:cic=***number***[,rng=***range***],confirm**

Where:

- *sig_srv* is the MML name of the signaling service. The following signaling service types are valid for this command:
  – For in-band TDM up to MUX and then time switched to TDM media and sent to the Cisco MGC.
  – For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
  – For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP-> Cisco MGC).
  – Signaling service or routeset associated with a DPC.
  – EISUP signaling service.
- *number*—A valid CIC number.
- *range*—A value such that *y+range* is a valid bearer channel number. The administrative state for all bearer channels between *y* and *y+range* are retrieved.

For example, to stop all active calls on CICs 2 through 11, associated with a signaling service called ss7svc1, enter the following command:

```
stp-call:ss7svc1:cic=2,rng=9,confirm
```

Auditing an MGCP Media Gateway

You can audit an MGCP media gateway from the Cisco MGC. The procedure to audit an MGCP media gateway is described in the following sections:

- Starting an MGCP Media Gateway Audit, page 8-94
- Retrieving an MGCP Media Gateway Audit, page 8-95

Starting an MGCP Media Gateway Audit

You can run an audit on a single MGCP media gateway, or on all of your provisioned MGCP media gateways. The Cisco MGC does not prompt you to indicate when the audit is complete. Please wait a few moments before retrieving the audit results as described in the "Retrieving an MGCP Media Gateway Audit" section on page 8-95.

To run an audit on a single MGCP media gateway, log on to the active Cisco MGC, start an MML session, and enter the following command:

sta-aud-gw:*MGCP_sig_srv*

Where *MGCP_sig_srv* is the MML name of the MGCP signaling service associated with the MGCP media gateway.

For example, to start an audit on an MGCP media gateway associated with an MGCP signaling service called T-1-16, you would enter the following command:

```
sta-aud-gw:T-1-16
```

To run an audit all of your MGCP media gateways, log on to the active Cisco MGC, start an MML session, and enter the following command:

```
sta-aud-gw:all
```

Retrieving an MGCP Media Gateway Audit

You can retrieve an audit for a single MGCP media gateway, or for audits on all of your MGCP media gateways. To retrieve an audit for a single MGCP media gateway, log on to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-aud-gw:MGCP_sig_srv
```

Where *MGCP_sig_srv* is the MML name of the MGCP signaling service associated with the MGCP media gateway.

For example, to retrieve an audit on an MGCP media gateway associated with an MGCP signaling service called T-1-16, you would enter the following command:

```
rtrv-aud-gw:T-1-16
```

The system returns a response similar to the following:

```
Media Gateway Controller  - MGC-01 2000-01-12 15:19:51
M COMPLD
   "SP1-MGCP1:Audit gw received at 2000-01-12 15:19:51
Audit GW PASSED
pass pn
pass pt - not alarmed
pass sl - not alarmed
pass nl
pass bp
pass cp
pass rp
pass nb
pass uc
pass ic
pass us
pass is"
```

The response indicates whether the audit has passed or failed. If the audit has failed, refer to the documentation for the associated MGCP media gateway for more information on troubleshooting the identified problem.

To retrieve audits run on all of your MGCP media gateways, log on to the active Cisco MGC, start an MML session, and enter the following command:

```
rtrv-aud-gw:all
```

The system returns a response similar to the one shown above, with a set of data for every MGCP media gateway associated with your system.

Running a Manual Continuity Test

To run a manual continuity test (COT) on a specified remote switch CIC, log in to the active Cisco MGC, start an MML session, and enter the following command:

tst-cot:*pt_code***:cic=***number*

Where:

- *pt_code*—The MML name of the point code associated with the CIC to be tested.
- *number*—The identification number of the CIC to be tested.

For example, to run a manual COT on CIC number 5 of a DPC named dpc1, you would enter the following command:

tst-cot:dpc1:cic=5

If the manual COT test should fail, verify the COT settings for the Cisco MGC and the associated media gateway, as described in the "Verifying Continuity Test Settings" section on page 8-96.

Verifying Continuity Test Settings

Step 1 Verify that the COT properties for the associated SS7 signaling service or trunk group are correct by logging in to the active Cisco MGC, starting an MML session, and entering the following command:

prov-rtrv:*component***:name="***comp_name***"**

Where:

- *component*—MML component type name for the SS7 signaling service or trunk group properties. Enter one of the following:
  - sigsvcprop—Component type for SS7 signaling service properties.
  - trnkgrpprop—Component type for trunk group properties.
- *comp_name*—MML name for the affected SS7 signaling service or trunk group.

For example, if you wanted to verify the properties for an SS7 signaling service called **ss7svc1**, you would enter the following command:

prov-rtrv:sigsvcprop:name="ss7svc1"

If your system has been properly configured for dial plan use, the system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2001-06-01 10:09:47
M  RTRV
   "session=active:sigsvcprop"
   /*
adjDestinations = 16
AlarmCarrier = 0
BOrigStartIndex = 0
BothwayWorking = 1
BTermStartIndex = 1
CctGrpCarrier = 2
CGBA2 = 0
CircHopCount = 0
CLIPEss = 0
CotInTone = 2010
```

```
CotOutTone = 2010
CotPercentage = 0
CustGrpId=2222
dialogRange = 0
ExtCOT = Loop
ForwardCLIinIAM = 1
ForwardSegmentedNEED = 1
                .
        .
        .
```

Step 2 If your settings for the highlighted properties match what is displayed above, proceed to Step 5. Otherwise, you must modify the COT settings on your Cisco MGC. To begin modifying the COT settings, start a provisioning session as described in the "Starting a Provisioning Session" section on page 3-63.

Step 3 Enter the following command to modify the COT settings on your Cisco MGC:

prov-ed:*component***:name="***comp_name***",***cot_prop***=***value***,***cot_prop***=***value***,...**

Where:

- *component*—MML component type name for the SS7 signaling service or trunk group properties. Enter one of the following:
  - ss7path—Component type for SS7 signaling services.
  - trnkgrp—Component type for trunk groups.
- *comp_name*—MML name for the affected SS7 signaling service or trunk group.
- *cot_prop*—Name of the COT property you want to modify.
- *value*—Value for the specified COT property.

Step 4 Save and activate your changes as described in the "Saving and Activating your Provisioning Changes" section on page 3-64.

Step 5 Debug the COT settings on the associated media gateway using the **show cot dsp**, **show cot request**, **show cot summary**, and **debug cot detail** commands. Refer to the documentation for the associated media gateway for more information on these commands.

If debugging the COT settings on the media gateway does not reveal any problems, or does not fix the COT failure, proceed to Step 6.

Step 6 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

Resolving an SRCP Audit Alarm

If an SRCP audit alarm should occur on your Cisco MGC, use the following procedure to resolve the problem:

Step 1 Verify that the SRCP heartbeat is up and working.

If the SRCP heartbeat is up and working, proceed to Step 2.

If the SRCP heartbeat is not up and working, restart the SRCP heartbeat. If that does not resolve the alarm, proceed to Step 3.

Step 2 Verify the configuration on the affected media gateway. The value in the field identified in the alarm should match the value given in the alarm description.

If the configuration of your media gateway is incorrect, modify the configuration. The procedures for modifying the configuration of the media gateway can be found in the documentation for the media gateway.

If the configuration of the media gateway is correct, proceed to Step 3.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

Media Gateway IP Destination/Link Out-of-Service

If an IP link or destination to a media gateway is out-of-service, perform the following steps:

Note An IP destination to a media gateway is out-of-service when both IP links associated with the destination are out-of-service.

Step 1 Ping the affected MGC link from the associated media gateway, using the following UNIX command:

```
ping link_addr
```

Where *link_addr* is the IP address of the affected MGC link.

Repeat this step if the second link for the destination is also out-of-service.

If the links are unreachable, proceed to Step 2. Otherwise, proceed to Step 3.

Step 2 If your system is using I/O cards to terminate the SS7 link, proceed to Step 3.

If your system is using Cisco SLTs to terminate the SS7 link, proceed to Step 4.

Step 3 If the path between the Cisco MGC and the media gateway is defined using an MGCP signaling service, proceed to Step 4. If the path between the Cisco MGC and the media gateway is defined using a NAS signaling service, proceed to Step 5.

Step 4 Verify the MGCP interface on your media gateway is working properly. Refer to the documentation associated with the media gateway for more information.

If the MGCP interface on your media gateway is working properly, proceed to Step x. Otherwise, correct the problems with the MGCP interface as described in the documentation associated with the media gateway.

Step 5 Identify which Redundant Link Manager (RLM) group is configured on the media gateway by entering the **sh run** command. For more information on this command, refer to the documentation associated with the media gateway.

Step 6 Verify that the RLM group identified in Step 5 is defined under the D-channel serial interface. Refer to the documentation associated with the media gateway for more information.

If the RLM group is defined, proceed to Step 7. Otherwise, add the RLM group to the D-channel serial interface. Refer to the documentation associated with the media gateway for more information.

If the link(s) returns to service, the procedure is complete. Otherwise, proceed to Step 7.

Step 7 Reset the RLM group using the **shut/no shut** commands. Refer to the documentation associated with the media gateway for more information.

If the link(s) return to service, the procedure is complete. Otherwise, proceed to Step 8.

Step 8 Verify that RLM messages are being acknowledged by the Cisco MGC using the **debug** command. Refer to the documentation associated with the media gateway for more information.

If RLM messages are being acknowledged by the Cisco MGC, proceed to Step 10. Otherwise, proceed to Step 9.

Step 9 Verify that the configuration for RLM on the Cisco MGC matches the configuration on the media gateway. To display the configuration of the IP links on the Cisco MGC, enter the following MML command at the active Cisco MGC:

prov-rtrv:iplnk:"all"

The system returns a response similar to the following:

```
   MGC-02 - Media Gateway Controller 2001-07-26 12:57:48
M  RTRV
   "session=active:iplnk"
   /*
NAME                 SVC                IF                    IPADDR      PORT
PEERADDR        PEERPORT    PRI         SIGSLOT     SIGPORT     NEXTHOP       NETMASK
----                 ---                --                    ------      ----
--------        --------    ---         ------      -------     -------       -------
va-5300-202-1        va-5300-202            enif1             IP_Addr1    3001
172.24.200.19   3001        1           0           0           0.0.0.0    255.255.255.255
va-5300-202-2        va-5300-202            enif1             IP_Addr1    3001
172.24.200.19   3001        1           0           0           0.0.0.0    255.255.255.255
va-5300-203-1        va-5300-203            enif1             IP_Addr1    3001
172.24.200.20   3001        1           0           0           0.0.0.0    255.255.255.255
va-5300-203-2        va-5300-203            enif1             IP_Addr1    3001
172.24.200.20   3001        1           0           0           0.0.0.0    255.255.255.255
   */
```

Ensure that the IP addresses (IPADDR and PEERADDR) and the ports (PORT and PEERPORT) match the values used by the media gateway. If the values match, proceed to Step 10.

Otherwise, if the changes need to be made on the media gateway, refer to the documentation for your media gateway for more information. If the changes need to be made on the Cisco MGC, start a dynamic reconfiguration session to make your changes, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65.

If the changes resolve the problem, the procedure is complete. Otherwise, proceed to Step 10.

Step 10 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

CIC Mismatch (One-Way Audio)

If there is a mismatch between the CICs on your system and the far-end, perform the following steps:

Step 1 Verify that the CIC numbering scheme on the far-end matches the settings on your Cisco MGC. To do this, log in to your active Cisco MGC, start an MML session, and enter the following command:

prov-rtrv:*trnktype***:"all"**

Where *trnktype* is the type of trunk used on your system. Valid values are:

- nailedtrnk—Used in nailed trunk configurations, for the Cisco SC2200.

- switchtrnk—Used in switched trunk configurations, for the Cisco PGW 2200.

Note The Cisco PGW 2200 PSTN Gateway was formerly known as the Cisco VSC3000 Virtual Switch Controller. Some parts of this document may use this older name.

For a nailed trunk configuration, the system returns a response similar to the following:

```
MGC-02 - Media Gateway Controller 2001-07-26 14:21:40
M  RTRV
   "session=active:nailedtrnk"
   /*
NAME        SRCSVC     SRCSPAN     SRCTIMESLOT(CIC)  DSTSVC     DSTSPAN DSTTIMESLOT(CIC)
----        ------     -------     ----------------  ------     ------- ----------------
1           ss7svc1    ffff        1                 va-5300-202 0          1
2           ss7svc1    ffff        2                 va-5300-202 0          2
3           ss7svc1    ffff        3                 va-5300-202 0          3
4           ss7svc1    ffff        4                 va-5300-202 0          4
5           ss7svc1    ffff        5                 va-5300-202 0          5
6           ss7svc1    ffff        6                 va-5300-202 0          6
7           ss7svc1    ffff        7                 va-5300-202 0          7
8           ss7svc1    ffff        8                 va-5300-202 0          8
9           ss7svc1    ffff        9                 va-5300-202 0          9
10          ss7svc1    ffff        10                va-5300-202 0          10
11          ss7svc1    ffff        11                va-5300-202 0          11
12          ss7svc1    ffff        12                va-5300-202 0          12
13          ss7svc1    ffff        13                va-5300-202 0          13
14          ss7svc1    ffff        14                va-5300-202 0          14
```

For a switched trunk configuration, the system returns a response similar to the following:

```
MGC-100 - Media Gateway Controller 2001-07-30 09:47:28
M  RTRV
   "session=cotegress:switchtrnk"
   /*
NAME         SPAN         CIC          TRNKGRPNUM   CU                     ENDPOINT
----         ----         ---          ----------   --                     --------
1            ffff         1            3005         mgx-7-6         vism/e1-1/1@mgx7-6
2            ffff         2            3005         mgx-7-6         vism/e1-1/2@mgx7-6
3            ffff         3            3005         mgx-7-6         vism/e1-1/3@mgx7-6
4            ffff         4            3005         mgx-7-6         vism/e1-1/4@mgx7-6
5            ffff         5            3005         mgx-7-6         vism/e1-1/5@mgx7-6
6            ffff         6            3005         mgx-7-6         vism/e1-1/6@mgx7-6
7            ffff         7            3005         mgx-7-6         vism/e1-1/7@mgx7-6
8            ffff         8            3005         mgx-7-6         vism/e1-1/8@mgx7-6
9            ffff         9            3005         mgx-7-6         vism/e1-1/9@mgx7-6
10           ffff         10           3005         mgx-7-6         vism/e1-1/10@mgx7-6
11           ffff         11           3005         mgx-7-6         vism/e1-1/11@mgx7-6
12           ffff         12           3005         mgx-7-6         vism/e1-1/12@mgx7-6
13           ffff         13           3005         mgx-7-6         vism/e1-1/13@mgx7-6
14           ffff         14           3005         mgx-7-6         vism/e1-1/14@mgx7-6
```

If these settings do not match those used by the far-end, start a dynamic reconfiguration session, as described in the "Invoking Dynamic Reconfiguration" section on page 3-65, and correct your settings. Otherwise, proceed to Step 2.

If that resolves the mismatch, the procedure is complete. Otherwise, proceed to Step 2.

Step 2 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

Calls Fail at the Cisco MGC

If calls appear to be failing at the Cisco MGC, and the calls are not appearing on the associated media gateway, perform the following steps:

Step 1 Debug the interface on the media gateway associated with the Cisco MGC. For media gateways associated with a Cisco SC2200, the interface is Q.931. For media gateways associated with a Cisco PGW 2200, the interface is MGCP. Refer to the documentation for the associated media gateway for more information on debugging the interface.

If the calls in question do not appear on the media gateway, proceed to Step 2. Otherwise, resolve the problems with the interface as described in the documentation for the associated media gateway.

Step 2 Verify that the signaling channels are in-service, as described in the "Retrieving Signaling Channel Attributes" section on page 3-48.

If any of the signaling channels are out-of-service, attempt to bring them into service using the appropriate procedures. Otherwise, proceed to Step 3.

Step 3 Run a call trace as described in the "Performing a Call Trace" section on page 8-102, and contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

Modifying Redundant Link Manager Timers

As of Release 7.4(12), you can modify the values of your Cisco MGC's redundant link manager (RLM) timers. Refer to the *Release Notes for Cisco Media Gateway Controller Software* for more information.

If you want to change these timers, you must change them on the Cisco MGC and on the associated media gateway(s). To change the RLM timers, perform the following steps:

Note RLM keepalives are sent only when traffic has not been transmitted for some time, that is, when a signaling message is received, the RLM keepalive timer is reset. RLM keep a lives are sent by the media gateway to the Cisco MGC. If the RLM keepalive timer on the Cisco MGC expires, the system sets the IP link out-of-service. Increasing the RLM keepalive timer values on both sides can ensure that the IP link is not reset during transient conditions in the IP network, when the default values might be too stringent. However, if your system is in a continuous service configuration, increasing the values of the RLM keepalive timers reduces the system's ability to quickly detect a link failure. Systems in a simplex configuration would not be affected.

Step 1 Verify the current settings of your RLM timers on the Cisco MGC by logging in to the standby Cisco MGC, starting an MML session, and entering the following command:

prov-rtrv:lnksetprop:name="*mgc_name***"**

Where *mgc_name* is the MML name of the Cisco MGC host.

The system returns a response similar to the following:

```
   MGC-01 - Media Gateway Controller 2001-07-27 11:00:06
M  RTRV
   "session=active:lnksetprop"
   /*
linkEchoRetry = 3
```

```
linkLatencyTest = 600
linkOpenWait = 30
linkRecovery = 120
linkSwitch = 50
linkUpRecoveredMin = 600
port = 3000
PropagateSvcMsgBlock = false
timerCmdAck = 10
timerLinkDownMin = 100
timerLinkEcho = 10
unstableLink = 10
   */
```

All of the properties listed, except for port and PropagateSvcMsgBlock, are RLM timer properties.

Step 2 Start a provisioning session as described in the "Starting a Provisioning Session" section on page 3-63.

Step 3 Modify the RLM timer properties, as needed, using the following command:

prov-ed:lnkset:name="*mgc_name***",***prop_name***="***value***",***prop_name***="***value***",...**

Where:

- *mgc_name*—The MML name of the Cisco MGC host.
- *prop_name*—The name of the RLM timer property you want to modify.
- *value*—The value you want for the specified RLM timer property.

Step 4 Save and activate your provisioning changes as described in the "Saving and Activating your Provisioning Changes" section on page 3-64.

Step 5 Reboot your system as described in the "Rebooting Your System to Modify Properties" section on page 8-124.

Tracing

Tracing on the Cisco MGC is described in the following sections:

- Performing a Call Trace, page 8-102
- Alternatives to Call Tracing, page 8-108
- Performing a TCAP Trace, page 8-111

Performing a Call Trace

After checking all physical connections, signal links, bearer channels, and destinations, the person who is troubleshooting the Cisco MGC begins to suspect that the call engine is part of the problem. Performing a call trace while making a call provides details about what is occurring inside the call engine and indicates where the breakdown is occurring (if it is occurring within the call engine).

Call tracing is described in the following sections:

- Starting A Call Trace, page 8-103
- Stopping A Call Trace, page 8-105
- Retrieving Names of Open Call Trace Files, page 8-105

Starting A Call Trace

To start the call trace, perform the following steps:

Step 1 Log in to the active CiscoMGC, start an MML session, and enter the command.

This command can be entered in any one of five different formats:

1. **sta-sc-trc:***sig_path***:**[**log="***filenameprefix***"**][**,prd=***n*]**, confirm**
2. **sta-sc-trc:***sig_path***:span=***x*[**,rng=***y*][**,log="***filenameprefix***"**][**,prd=***n*]
3. **sta-sc-trc:***sig_path***:span=***x*[[**,tc=***z*]**,rng=***y*][**,log="***filenameprefix***"**][**,prd=***n*]
4. **sta-sc-trc:***trkgrp***:**[**log="***filenameprefix***"**][**,prd=***n*]**, confirm**
5. **sta-sc-trc:***trkgrp***:trk=***w*[**,rng=***y*][**,log="***filenameprefix***"**][**,prd=***n*]

Where:

- *sig_path*—The logical signaling destination, such as an SS7 point code, an FAS path, an IP FAS path, or a DPNSS path,
- *trkgrp*—The logical trunk group of interest.
- *filenameprefix*—Trace files are created and written to a file whose name can vary, depending on how the command is invoked. (A system log message is generated for each trace started. The filenames created as part of the **sta-sc-trc** command are contained in the log messages.) If the **log=** parameter is used, the value of this parameter is treated as a prefix to the filename.

  If no **log=** parameter is used, default *filenameprefix* values are used for each **sta-sc-trc** command. For example:

  – For **sta-sc-trc:***sig_path***:confirm** the filename is:

    sig_path_yyyymmddhhmmss.btr

  – For **sta-sc-trc:***trkgrp***:confirm** the filename is:

    trkgrp_sig_path_yyyymmddhhmmss.btr

  Where the filename (*yyyymmddhhmmss*) is a time stamp, organized as follows:

  – *yyyy*—Is the four-digit designation for the year, such as 2000, 2001, or 2002.
  – *mm*—Is the two-digit designation for the month (01 through 12).
  – dd—Is the two-digit designation for the day of the month (01 through 31).
  – *hh*—Is the two-digit designation for the hour of the day (00 through 23).
  – *mm*—Is the two-digit designation for the minutes (00 through 59).
  – *ss*—Is the two-digit designation for the seconds (00 through 59).
- *n*—The duration for which call trace information is collected, in seconds. At the expiration of this period, the system discontinues PDU collection on the signaling path and closes the log file. In the absence of this parameter, the default period is set to 1800 seconds (30 minutes), after which time the trace is stopped automatically.

- **confirm**—An option that is required to confirm a *sig_path* level trace or a *trkgrp* level trace command. This is required due to the large volume of data that can be generated and the potential performance impact of generating a large trace file. If the confirm option is not entered, the command is rejected, and you receive a message regarding the potential performance impact of this command.
- *x*—The span ID, an integer value denoting the traffic channel for the *sig_path* (NFAS only).
- *y*—The range. When used with "**span=***x***,**" *y* is an optional range of spans beginning with span *x* and continuing for *y* spans. When used with "**tc=***z*," *y* is an optional range of traffic channels beginning with *z* and continuing for *y* traffic channels. When used with "**trk=***w*," *y* is an optional range of contiguous trunks to be traced starting with trunk *w* and ending with trunk *y*.
- *y*—The traffic channel of interest in integer form.
- *w*—The trunk of interest in integer form.

The following paragraphs present examples of each of the five possible command variations:

1. A signaling path level trace traces all calls occurring on the signaling path. Use this format if the specific traffic channel the call uses is unknown.

   ```
   sta-sc-trc:sig_path:log="filenameprefix", prd=600, confirm
   ```

   In this form of the command, the confirm parameter is required.

2. A signaling path/span level trace traces calls at the span level. Use this format to reduce the amount of trace information if you know the span on which the call will be placed.

   ```
   sta-sc-trc:sig_path:span=x
   ```

   The confirm parameter is not needed in this form of the command because the volume of the trace file should not be an issue, nor should system performance.

3. A signaling path/span/traffic channel level trace traces calls at the TC or CIC level. Use this format if the traffic channel on which the call will be placed is known.

   ```
   sta-sc-trc:sig_path:span=x,tc=y
   ```

4. A trunk group level trace traces all calls at a trunk group level. Use this format if the trunk group on which the call will be placed is known.

   ```
   sta-sc-trc:trkgrp:confirm
   ```

   This form of the command requires the confirm parameter.

5. A trunk group/trunk level trace traces only calls for a given trunk (or CIC). Use this format if the trunk group and trunk on which the call will be placed is known.

   ```
   sta-sc-trc:trkgrp:trk=w
   ```

Note Refer to the *Cisco Media Gateway Controller Software Release 7 MML Command Reference Guide* for detailed information on using the **sta-sc-trc** command.

Step 2 Make the call.

Stopping A Call Trace

You can stop a call trace session using the **stp-sc-trc** MML command. To stop a call trace session on a particular signaling service, log in to the active Cisco MGC, start an MML session, and enter the following command:

stp-sc-trc:*sig_srv*|*trkgrp*

Where:

- *sig_srv*—MML name for the signaling service on which you are running a call trace.
- *trkgrp*—MML name for the trunk group on which you are running a call trace.

For example, to stop a call trace session on a trunk group called T-1-1, you would enter the following command:

stp-sc-trc:T-1-1

To stop all call trace sessions, log in to the active Cisco MGC, start an MML session, and enter the following command:

stp-sc-trc:all

The system returns a response similar to the following:

```
Media Gateway Controller 2000-03-21 15:28:03
M  COMPLD
   "ALL:Trace stopped for the following files:
   ../var/trace/_dpc1_20000321152752.btr
   "
```

Retrieving Names of Open Call Trace Files

To retrieve the names of call trace files for sessions that are in progress, log in to the active Cisco MGC, start an MML session, and enter the following command:

rtrv-sc-trc

The system returns a response similar to the following:

```
Media Gateway Controller 2000-03-21 15:28:03
M  RTRV
   "RTRV-SC-TRC:Trace in progress for the following files:
   ../var/trace/_dpc1_19991221131108.btr
   ../var/trace/sigtest_dpc2_19991221131109.btr
  "
```

Viewing the Call Trace

The MML command **sta-sc-trc** produces .btr (binary trace) files, which cannot be viewed with a text editor. The main part of the file name is set up in the **sta-sc-trc** command, as explained in the "Starting A Call Trace" section on page 8-103, and the Cisco MGC adds the .btr extension to these files. The .btr files can contain tracings from many calls all mixed together. Each tracing record in the file has a specific record type and records information of the type that relates to that record. Each record has a unique call ID that relates it to a specific call and is a recording of the external events that the MDL call model was exposed to while the recording was made. Each tracing record is not a recording of the actual MDL.

You can use the trace viewer to view and navigate through call trace outputs. For more information on using the trace viewer, refer to the "Using the Trace Viewer" section on page 3-117.

You can also view the call trace output data using the **get_trc.sh** UNIX script. **Get_trc.sh** uses the Conversion Analyzer and SimPrint utilities in combination to give a single common interface to all the trace tools. **Get_trc.sh** makes considerable use of the UNIX less utility for displaying file output and it is assumed that less is available on the system. You can start the script by entering the following UNIX command:

```
get_trc.sh filename
```

Where *filename* is the name of the call trace output data file (.btr) you want to view.

The script then displays a list of commands and prompts you to enter a command. The following commands are listed:

- S—Displays the call trace data using the SimPrint utility. For more information on SimPrint, refer to the "Understanding SimPrint" section on page 8-108.
- F—Displays the call trace data using the SimPrint utility, and a listing of the sent and received fields.
- D—Displays the data in the .trc file associated with this call trace. For more informaction on .trc files, refer to the "Understanding Trace Files" section on page 8-108.
- C—Converts the file created by this script to a .trc file.
- A—Displays the data in the .ca file associated with this call trace. For more information on .ca files, refer to the "Understanding the Conversion Analyzer" section on page 8-107.
- N—Displays the information for the next call ID in the list.
- P—Displays the information for the previous call ID in the list.
- L—Lists all of the call IDs in the data for this call trace.
- H—Provides help on displaying call trace data.
- Q—Closes the script.
- id—Displays the information for a call ID that you specify.

Deleting Call Trace Files

Call trace files can be rather large, and leaving these files on your disk after you no longer require them could raise capacity issues. Call trace files are deleted using UNIX commands, as described in the "Deleting Unnecessary Files to Increase Available Disk Space" section on page 8-112.

Understanding the Call Trace

Call traces record information in a trace file that shows how the Cisco MGC processed a specific call. Traces are most useful when you can be sure that a problem call is reaching the call engine and starting an instance of a Message Definition Language (MDL) state machine. You can determine whether the problem call is reaching the call engine by looking for the presence of non-idle circuits (**rtrv-cic**) or "new cmgCall" entries in the debug logs.

After you start a trace, all call-processing activity for calls originating from the specified destination is captured. This allows you to follow the call through the Cisco MGC to see where it fails.

The trace output is in binary format. It shows:

- The PDU that the Cisco MGC receives
- How the Cisco MGC decodes the PDU

- The PDU that the Cisco MGC sends out

Using call trace logs is easy if you remember how to locate the record of a call:

- You can easily locate incoming signal messages that cause instances of engine call objects to be started by searching backwards in the call trace for "new cmgCall."
- Similarly, you can find the end of a call by searching forward from the "new cmgCall" message for the next "end cmgCall" message.

If you are experiencing problems with call processing and need to contact Cisco for support, you should run a call trace before contacting Cisco's TAC. The trace file helps the Cisco TAC troubleshoot the problem more effectively. For some problems, the Cisco TAC cannot begin troubleshooting the problem until you supply the trace file, so it is a good practice to create this file before contacting them.

Understanding the Conversion Analyzer

The Conversion Analyzer is a viewer utility for .btr trace files. The Conversion Analyzer displays each record from a .btr file in a readable form (ASCII text) that can be viewed with any text editor; however, some useful sorting and display options are also available.

The .btr files serve as source files for .ca files. The .ca files are ASCII text output from the Conversion Analyzer obtained by redirection of the standard output to a file. There are two main sections in a .ca file. The header section contains a list of every signaling path defined on the Cisco MGC and a list of the message definition object (MDO) modules that are loaded. The main body contains a printout of every record. Each record has a record number, a timestamp, a call ID, and the print data that the record contains.

Understanding the Simulator Utility

The Simulator is a powerful MDO file processing utility that uses .mdo files to replay the events recorded in a .btr file. The front end of the Simulator reads the .btr file. The interpreter in the Simulator utility that loads the .mdo files and replays the events (.btr files) through the MDO, is the same interpreter used by the call engine in the Cisco MGC when .mdo files are used. As the interpreter steps through each line of object code (and the action of each object is interpreted) in the .mdo file, each object's print method is activated, which forms the next line of text in the .trc file.

The print method for each object contains text that directly relates to the appearance of the .mdl source code that produced the object in the .mdo file (through compilation of the .mdl source code with the MDL compiler). The .mdo files used with the Simulator when it is processing a .btr file to create a .trc file, must be the same .mdo files that were in use when the .btr file was originally recorded on the Cisco MGC. This is why the conversion from a .btr file to a .trc file is usually done on the Cisco MGC that originated the .btr file.

The interpreter is not used with .so files because those files interact directly with the call engine in the Cisco MGC, but the tracer can record a .btr file regardless of whether .mdo or .so files were used to process the call. The Simulator can, however, replay .btr files using .so files in place of .mdo files. This is a way of checking that the .so and .mdo files perform in exactly the same way, although .so is faster.

Because .so files do not contain MDO objects, there are no print methods available to the Simulator, so no .trc output is possible. When a .btr file is produced by a Cisco MGC using .so files, the replay in the Simulator must be done with the .mdo files that were used to produce the .so files in order to produce an accurate .trc file.

Understanding Trace Files

Trace files (.trc files) are text files that are produced by the Simulator utility. They contain detailed line by line trace information from the MDO code that was run in the simulation replay that produced the file, thus they contain MDL traces. The .trc extension is added by the **get_trc.sh** script if the source of the trace is a .btr file.

Trace files are source files for the SimPrint (SP) utility. They are text files and can be viewed with a text editor. The .trc file should be sent to Cisco TAC if expert analysis is required.

Understanding SimPrint

SimPrint (SP) is a viewing utility for .trc files. SP converts a .trc file into a sequence diagram that shows all of the external and internal events that occur in a .trc file. This is useful for getting an overview of what is occurring in the trace.

The following list defines the terms used in the call flow printouts generated by the SimPrint tool:

- LINE—Refers generically to the incoming and outgoing interfaces of the Cisco MGC.
- OCC—Originating Call Control state machine. The call is passed from the incoming interface to a protocol adapter, where it is converted into a generic message signaling unit (MSU) and sent to the OCC for parsing of MSU data to memory.
- LCM—Lightspeed Call Model state machine. The LCM is a generic call model containing event handlers to process generic call event data. This processing includes generic call analysis, requests for bearer channels, and transfer of the MSU to the appropriate TCC state machine. The LCM is also known as the Universal Call Model (UCM).
- ANALYSIS—The LCM can perform generic call analysis, based on the content of the MSU. The LCM exchanges data with the call processing engine to analyze the MSU. After analysis is complete, an available circuit is identified and the LCM sends a bearer channel seizure request message to the CPM state machine.
- CPM—Connection Plane Manager state machine. The CPM exchanges data with the call processing engine to seize and prepare a bearer channel for routing of the call data.
- CDR—Call Detail Record. CDR information is created as a result of LCM processing of the MSU.
- TRIGGER—Intelligent Network (IN) Trigger state machine. This state machine is used to send and receive IN trigger events to the Transfer Capabilities Application Part (TCAP) interface in the I/O channel controller (IOCC). This enables IN messages to be sent to a service control point (SCP).
- ENGINE—The call processing engine exchanges data with the LCM as generic call analysis is performed on the MSU and a bearer channel is seized and prepared for routing of the call data.
- TCC—Terminating Call Control state machine. The TCC changes the call data into a protocol-specific protocol data unit (PDU) and passes the PDU to the terminating IOCC for routing to the outgoing interface.

Alternatives to Call Tracing

Performing call traces to identify problems can be difficult due to the large amount of data the trace may gather before the error occurs, and the negative impact performing call traces has on system performance. The Cisco MGC software has MML commands that can be used to diagnose problems with hung calls and abnormal call termination. The following sections describe those commands.

Diagnosing Hung Calls

You can print the diagnostic information about hung calls to a file using the **prt-call** MML command. The contents of the file include all of the previous states of the call and a history of occurrences leading up to the call being stuck in its current state.

To print diagnostic information on a hung call, complete the following steps:

Step 1 Log in to the active Cisco MGC and enter the following command:

prt-call:*sig_path***:cic=***number* **[,log=***xyz***]**

or

prt-call:*sig_path***:span=***phys***, bc=***bchan* **[,log=***xyz***]**

Where:

- *sig_path*—Corresponding MML name for any of the following component types:
  - Signaling path of in-band TDM up to MUX and then time switched to TDM media and sent to Cisco MGC.
  - Signaling path of in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
  - Signaling path of in-band TDM signaling up to NAS and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->NAS<-NI2/IP->Cisco MGC).
  - Signaling path or routeset associated with SS7 destination point code.
  - Signaling path for EISUP.

Note This command allows for the use of wildcards for the *sig_path* parameter.

- *number*—A numeric value that identifies the ISUP circuit identification code (CIC) number.
- *phys*—A 16-bit value that identifies an ISDN/PRI physical cable.
- *bchan*—A numeric value that identifies the non-ISUP bearer channel number. BC is used for non-ISUP trunks.; otherwise use CIC.
- *xyz*—The name of an ASCII log file to which the output of this command is written. The name given in this parameter is used as a prefix to the actual name of the file, which includes the *sig_path* name, date, and time. If no log file name is provided, a default name consisting of the *sig_path* name, date, and time is created. The extension of these log files is .prt, and they are located in the $BASEDIR/var/trace directory.

For example, the following MML command prints call data for a signaling path called dms100-pc using a CIC of 124:

```
prt-call:dms100-pc:cic=124
```

The output for this command is stored in a file called pc_*timestamp*.prt, where *timestamp* is the time of the file's creation.

Step 2 To change directories, enter the following command:

```
cd /opt/CiscoMGC/var/trace
```

Step 3 Use a text file viewer, such as vi, to view the contents of the log file.

Performing an Abnormal Call Termination Trace

You can print the global variable information from the state machine and external event information for a call to a file using the **sta-abn-trc** MML command. To print this information, complete the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and enter the following command:

sta-abn-trc:*sig_path*|**all[,log=***xyz***] [,prd=***n***],confirm**

Where:

- *sig_path*—Corresponding MML name for any of the following component types:
  - Signaling path of in-band TDM up to MUX and then time switched to TDM media and sent to Cisco MGC.
  - Signaling path of in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco MGC.
  - Signaling path of in-band TDM signaling up to NAS and then converted to NI2 and sent to the Cisco MGC over IP (that is, FE box<-sig/tdm->NAS<-NI2/IP->Cisco MGC).
  - Signaling path or routeset associated with SS7 DPC.
  - Signaling path for EISUP.

Note This command allows for the use of wildcards for the *sig_path* parameter.

- **all**—Indicates that the start trace command needs to be applied to the whole Cisco MGC, in which case only one trace file is generated.
- *xyz*—The name of an ASCII log file to which the output of this command is written. The name given in this parameter is used as a prefix to the actual name of the file, which includes the *sig_path* name, date, and time. If no log file name is provided, a default name consisting of the *sig_path* name, date, and time is created. The extension of these log files is .prt, and they are located in the $BASEDIR/var/trace directory.
- *n*—The period, in seconds, for which this trace is enabled, during which time any abnormal calls are traced. If this optional parameter is not used, the period defaults to 30 seconds.

For example, the following MML command prints call data for a signaling path called dms100-pc to a file named trace1 (since the period parameter, *n*, is not entered, the trace lasts for the default period, 30 seconds):

```
sta-abn-trc:dms100-pc,log=trace1,confirm
```

Step 2 To change directories, enter the following UNIX command:

```
cd /opt/CiscoMGC/var/trace
```

Step 3 Use a text file viewer, such as vi, to view the contents of the log file.

Stopping an Abnormal Call Termination Trace

You can stop an in-progress abnormal call termination trace using the **stp-abn-trc** MML command. To do this, log in to the active Cisco MGC, start an MML session, and enter the following command:

stp-abn-trc:*sig_srv*

Where *sig_srv* is the MML name for a signaling service on which an abnormal call termination trace is being run.

For example, to stop an abnormal call termination trace being run on a signaling service called ss7srv1, you would enter the following command:

stp-abn-trc:ss7srv1

The system responds with a response similar to the following:

```
Media Gateway Controller 2000-05-26 07:02:11
M  COMPLD
"Trace stopped for the following file:

../var/trace/_20000526070211.abn
"
```

To stop all in-progress abnormal call termination traces, log in to the active Cisco MGC, start an MML session, and enter the following command:

stp-abn-trc:all

The system returns a response similar to the following:

```
Media Gateway Controller 2000-05-26 07:02:11
M  COMPLD
   "ALL:Trace stopped for the following files:

   ../var/trace/_20000526070211.abn
   "
```

Performing a TCAP Trace

To run a TCAP trace on your system, perform the following steps:

Step 1 Start the TCAP trace by logging in to the active Cisco MGC, starting an MML session, and entering the following command:

sta-tcap-trc

The system begins sending TCAP trace messages to the active system logs file.

Step 2 View the active system logs file, as described in the "Viewing System Logs" section on page 8-4. Make note of any TCAP trace messages, such as hex dumps of messages sent to the SCCP layer.

Step 3 When your TCAP trace is complete, enter the following command to stop the TCAP trace:

stp-tcap-trc

Platform Troubleshooting

The following sections contain procedures related to resolving problems with the Cisco MGC platform:

Deleting Unnecessary Files to Increase Available Disk Space

You may need to delete call trace files, archived log files, or configurations from your system to create more available disk space on your Cisco MGC.

The following procedure steps you through the process of deleting all three file types.

Step 1 Log in to the active Cisco MGC and enter the following UNIX commands to determine whether the affected disk drive contains any call trace files in the /opt/CiscoMGC/var/trace directory:

```
cd /opt/CiscoMGC/var/trace

ls
```

The system responds with a list of files in the directory. If the command response indicates that there are *.btr and *.trc files stored in this directory, then proceed to Step 2. Otherwise, proceed to Step 4.

Note Do not delete any call trace files related to troubleshooting any current system problems.

Step 2 Delete the identified call trace files using the following UNIX command:

```
rm -i filename
```

Where *filename* is the name of the call trace file (either *.btr or *.trc) you have identified for deletion.

Step 3 Repeat Step 2 for each additional call trace file identified for deletion.

Step 4 Enter the following UNIX commands to view the archived logs in the /opt/CiscoMGC/var/spool directory on the affected disk drive:

```
cd /opt/CiscoMGC/var/spool

ls
```

The system responds with a list of files in the directory. Review the listed files. If there are archived log files listed that are no longer required, proceed to Step 5. Otherwise, proceed to Step 7.

Note If you are backing up your system software on a regular basis, you can retrieve any files that you choose to delete from your backup files, if the need arises. For more information on backing up your system software, refer to the "Backing Up System Software" section on page 3-28.

Step 5 Delete the identified archived log files using the following UNIX command:

rm -i *filename*

Where *filename* is the name of the archived log file you have identified for deletion.

Step 6 Repeat Step 5 for each additional identified archived log file.

Step 7 Use the config-lib viewer to view the contents of the configuration library, using the information in the "Using the Config-Lib Viewer" section on page 3-113. Determine whether any of the configurations listed are no longer necessary for the operation of your system. If any of the configurations can be deleted, delete them using the information in the "Using the Config-Lib Viewer" section on page 3-113.

Recovering from a Switchover Failure

Use the procedure in this section to recover from a failed switchover operation. You would typically use this procedure when the standby Cisco MGC is unavailable to process calls and a critical alarm occurs on the active Cisco MGC.

To recover from a switchover failure, complete the following steps:

Step 1 Log in to the active Cisco MGC, start an MML session, and view the current alarms, as described in the "Retrieving All Active Alarms" section on page 8-3.

Step 2 Identify the critical alarm that caused the switchover attempt. To do this, review the alarm(s) that are listed in the response. There should be at least one critical alarm, and an alarm indicating that a switchover began and another alarm indicating that the switchover failed.

If there is only one critical alarm listed, that alarm caused the switchover attempt.

If there is more than one critical alarm listed, compare the timestamp of the critical alarms with the timestamp of the alarm indicating that a switchover began. The critical alarm that occurred before the switchover was begun is the alarm that caused the switchover attempt.

Step 3 Refer to the "Alarm Troubleshooting Procedures" section on page 8-8 for descriptions of the steps necessary to resolve the critical alarm that caused the switchover attempt.

Step 4 Log in to the standby Cisco MGC, start an MML session, and view the current alarms, as described in the "Retrieving All Active Alarms" section on page 8-3.

Step 5 Resolve the listed alarm(s). Refer to the "Alarm Troubleshooting Procedures" section on page 8-8 for descriptions of the steps necessary to resolve the alarm(s).

If resolving the alarms does not stabilize the standby Cisco MGC, proceed to Step 6.

Step 6 Generate a ping from the active Cisco MGC to the standby Cisco MGC by entering the following UNIX command at the active Cisco MGC:

ping *standby_addr*

Where *standby_addr* is the IP address of the standby Cisco MGC.

If the ping fails, proceed to Step 7. Otherwise, proceed to Step 8.

Step 7 Verify the Ethernet interfaces between the active Cisco MGC and the standby Cisco MGC. Refer to the Sun Microsystems documentation that came with your system for more information.

If an element of the Ethernet interfaces between the active Cisco MGC and the standby Cisco MGC is found to be faulty, replace it. Otherwise, proceed to Step 8. Refer to the Sun Microsystems documentation that came with your system for more information.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 8.

Step 8 Verify that the host name for each Cisco MGC host is unique. To do this, log on as root to each Cisco MGC host and view the contents of the host file in the /etc directory. If a Cisco MGC host does not have a unique host name, enter the following UNIX command:

```
# echo host_name > /etc/host
```

Where *host_name* is a unique name for the Cisco MGC host.

Step 9 Verify that the IP address parameters in the XECfgParm.dat file, which are listed below, are set correctly on each host.

- *.ipAddrLocalA
- *.ipAddrLocalB
- *.ipAddrPeerB
- *.IP_Addr1
- *.IP_Addr2
- *.IP_Addr3
- *.IP_Addr4

If the IP address settings are correct, proceed to Step 10. Otherwise, update the IP address parameters for each host , using the procedure in the "Rebooting Software to Modify Configuration Parameters" section on page 8-125.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 10.

Step 10 Verify that the settings for the foverd parameters are set correctly in the XECfgParm.dat file, which are listed below, on each host.

```
foverd.conn1Type         = socket
foverd.ipLocalPortA      = 1051
foverd.ipPeerPortA       = 1052
foverd.conn2Type         = socket
foverd.ipLocalPortB      = 1053
foverd.ipPeerPortB       = 1054
foverd.conn3Type         = serial
foverd.conn3Addr         = /dev/null
foverd.abswitchPort      = (/dev/null)
foverd.heartbeatInterval = 4000
```

If the foverd settings are correct, proceed to Step 11. Otherwise, update the foverd settings in the XECfgParm.dat files using the procedure in the "Rebooting Software to Modify Configuration Parameters" section on page 8-125.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 11.

Step 11 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

Recovering from Cisco MGC Host(s) Failure

There are situations, such as a replacement of a failed disk drive, natural or man-made disaster, or software corruption, that make it necessary for you to recover the software configuration data for a failed Cisco MGC host or hosts. (for example, if the Cisco MGC software has become corrupted or you have replaced a failed disk drive).

Note In these procedures, it is assumed that backup operations have been performed regularly on your Cisco MGC. For more information on backing up your Cisco MGC, refer to the "Backing Up System Software" section on page 3-28.

Note Successful recovery from a natural or man-made disaster depends upon your planning in advance for a possible disaster. Refer to the "Creating a Disaster Recovery Plan" section on page 3-27 for more information.

The following sections contain the procedures that describe how to recover from Cisco MGC host(s) failure:

Recovering from a Cisco MGC Host Failure in a Simplex System

To recover from a Cisco MGC host failure in a system equipped with only one Cisco MGC, perform the following steps:

Step 1 Reload the Solaris 2.6 operating system on the Cisco MGC host, as described in the *Installing the Operating System Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 2 Reload the Cisco MGC software on the Cisco MGC host, as described in the *Installing the Cisco Media Gateway Controller Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 3 Restore the configuration of your Cisco MGC from your latest backup file, as described in the "Restoring Stored Configuration Data" section on page 8-117.

Note If your backup files are stored on a remote server, have your network administrator re-establish the path between the Cisco MGC and the server that stores your backups.

Note Any changes you made to the Cisco MGC system subsequent to your last backup are lost.

Step 4 Start the Cisco MGC software, as described in the "Starting the Cisco MGC Software" section on page 2-2.

Recovering from a Single Cisco MGC Host Failure in a Continuous Service System

To recover from a single Cisco MGC host failure in a system equipped with two Cisco MGCs, perform the following steps:

Step 1 Reload the Solaris 2.6 operating system on the affected Cisco MGC host, as described in the *Installing the Operating System Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 2 Reload the Cisco MGC software on the affected Cisco MGC host, as described in the *Installing the Cisco Media Gateway Controller Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 3 Restore the configuration of the affected Cisco MGC from your latest backup file, as described in the "Restoring Stored Configuration Data" section on page 8-117.

Note If your backup files are stored on a remote server, have your network administrator re-establish the path between the affected Cisco MGC and the server that stores your backups.

Step 4 Open the XECfgParm.dat file on the affected Cisco MGC in a text editor, such as vi.

Step 5 Search for the pom.dataSync property and ensure that it is set to *true*.

Step 6 Save the file and exit the text editor.

Step 7 Start the Cisco MGC software, as described in the "Starting the Cisco MGC Software" section on page 2-2.

Step 8 Contact the Cisco TAC for assistance in synchronizing the databases of the active and standby Cisco MGCs. Refer to the "Obtaining Technical Assistance" section on page xviii for more information on contacting the Cisco TAC.h

Recovering from a Dual Cisco MGC Host Failure in a Continuous Service System

To recover from a dual Cisco MGC host failure in a system equipped with two Cisco MGCs, perform the following steps:

Step 1 Select one of the Cisco MGC hosts to be your active system, and the other to be your standby system.

Step 2 Reload the Solaris 2.6 operating system on the active Cisco MGC host, as described in the *Installing the Operating System Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 3 Reload the Cisco MGC software on the active Cisco MGC host, as described in the *Installing the Cisco Media Gateway Controller Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 4 Restore the configuration of the active Cisco MGC from your latest backup file, as described in the "Restoring Stored Configuration Data" section on page 8-117.

> **Note** If your backup files are stored on a remote server, have your network administrator re-establish the path between the active Cisco MGC and the server that stores your backups.

Step 5 Open the XECfgParm.dat file on the active Cisco MGC in a text editor, such as vi.

Step 6 Search for the pom.dataSync property and ensure that it is set to *true*.

Step 7 Save the file and exit the text editor.

Step 8 Start the Cisco MGC software on the active Cisco MGC, as described in the "Starting the Cisco MGC Software" section on page 2-2.

Step 9 Reload the Solaris 2.6 operating system on the standby Cisco MGC host, as described in the *Installing the Operating System Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 10 Reload the Cisco MGC software on the standby Cisco MGC host, as described in the *Installing the Cisco Media Gateway Controller Software* chapter of the *Cisco Media Gateway Controller Software Release 7 Installation and Configuration Guide*.

Step 11 Restore the configuration of the standby Cisco MGC from your latest backup file, as described in the "Restoring Stored Configuration Data" section on page 8-117.

> **Note** If your backup files are stored on a remote server, have your network administrator re-establish the path between the standby Cisco MGC and the server that stores your backups.

Step 12 Open the XECfgParm.dat file on the standby Cisco MGC in a text editor, such as vi.

Step 13 Search for the pom.dataSync property and ensure that it is set to *true*.

Step 14 Save the file and exit the text editor.

Step 15 Start the Cisco MGC software, as described in the "Starting the Cisco MGC Software" section on page 2-2.

Step 16 Contact the Cisco TAC for assistance in synchronizing the databases of the active and standby Cisco MGCs. Refer to the "Obtaining Technical Assistance" section on page xviii section for more information on contacting the Cisco TAC.

Restoring Stored Configuration Data

Typically, restoration of stored configuration data is performed in severe troubleshooting situations where the Cisco MGC is not functioning properly, due to hardware failure, natural disaster, or software corruption. The procedures in this section describe how to restore the Cisco MGC configuration data stored either on a tape drive or on a remote network server.

There are two restoration methods available for the Cisco MGC software, one for software releases up to 7.4(10), and another for software releases from 7.4(11) and above. These restoration procedures are mutually exclusive. You cannot use the restoration procedures for one software release to restore files backed up using the procedures specific to the other release.

These restoration methods are described in the following sections:

- Restoring Procedures for Cisco MGC Software up to Release 7.4(10), page 8-118
- Restoring Procedures for Cisco MGC Software Release 7.4(11) and up, page 8-121

Restoring Procedures for Cisco MGC Software up to Release 7.4(10)

This restoration method uses a script to restore the configuration data for the Cisco MGC software from either a local tape drive or on to a remote machine. Restoration of the Main Memory Database (MMDB) is performed by a separate script.

The following sections provide the restoration procedures:

- Restoring Data from a Local Tape Drive, page 8-118
- Restoring Data from a Remote Machine over the Network, page 8-119
- Restoring Data to the Main Memory Database, page 8-121

Note These procedures assume that you have backed up your system configuration data regularly. The procedures for system configuration backup can be found in the "Backup Procedures for Cisco MGC Software up to Release 7.4(10)" section on page 3-28.

Restoring Data from a Local Tape Drive

This procedure restores everything on a tape in a local tape drive to the Cisco MGC base directory.

Caution This procedure overwrites existing files under the Cisco MGC base directory. Current content in the overwritten files will be lost!

To restore the contents of the entire Cisco MGC software directory from a local tape, complete the following steps:

Step 1 Enter the following UNIX command at the affected Cisco MGC to run the restore script:

```
./restore.sh
```

The system returns a response similar to the following:

```
MGC restore utility
-----------------------------
Source currently set to Local tape (/dev/rmt/0h)
Enter:
    <N> set source to remote NFS server
    <L> set source to Local tape (/dev/rmt/0h)
    <R> for Restore
    <Q> to quit
Select restore mode:
```

Step 2 Select **R** and press **Enter** to start the restore. The system then prompts you as listed below:

```
Are you sure you want to restore a backup.
```

```
Current data in the MGC directory will be overwritten and lost.

Answer(Y/N):
```

Step 3 Select **y** and press **Enter** if you are sure you want to restore from the tape. The system begins the restoration and returns a response similar to the following:

```
Answer(Y/N): y
x ., 0 bytes, 0 tape blocks
x ./var, 0 bytes, 0 tape blocks
x ./var/log, 0 bytes, 0 tape blocks
x ./var/log/platform.log, 117 bytes, 1 tape blocks
x ./var/log/mml.log, 187 bytes, 1 tape blocks.
.
.
.
#
```

Step 4 When the restore has finished, remove the tape from the tape drive.

Step 5 If you have performed any partial backups since the creation of the full backup tape you have just restored, retrieve the most recent partial backup tape and repeat steps 1 to 4 with that tape in the tape drive.

Step 6 If your system does not have a dial plan configured, the procedure is complete. Otherwise, restore the contents of your dial plan as described in the "Restoring Data to the Main Memory Database" section on page 8-121.

Restoring Data from a Remote Machine over the Network

This procedure restores files to the Cisco MGC software base directory from a file on an NFS mountable directory on a remote machine. The remote machine must be set up with an NFS mountable directory that can be written to by the machine being backed up. The NFS setup of the remote machine is beyond the scope of this procedure.

To restore the contents of the Cisco MGC software directory from a remote machine, complete the following steps:

Step 1 Enter the following UNIX command on the affected Cisco MGC to run the restore script:

```
./restore.sh
```

The system returns a response similar to the following:

```
MGC restore utility
-----------------------------
Source currently set to Local tape (/dev/rmt/0h)
Enter:
    <N> set source to remote NFS server
    <L> set source to Local tape (/dev/rmt/0h)
    <R> for Restore
    <Q> to quit
Select restore mode:
```

Step 2 Select **N** and press **Enter** to define the remote NFS server. The system then prompts you to provide the name of the remote server.

Step 3 Enter the name of the remote NFS server:

```
Enter server name: remote_hostname
```

Where: *remote_hostname*—Name of the remote server where the backups are stored.

The system then prompts you to enter the name of the associated directory on the remote server.

Step 4 Enter the directory name on the remote NFS server:

```
Enter remote directory : remote_directory_name
```

Where: *remote_directory_name*—Name of the directory path on the remote server where the backups are stored.

The system returns a response similar to the following:

```
Enter server name: va-panthers
Enter remote directory : /backup

MGC restore utility
-----------------------------

Source currently set to remote NFS server (va-panthers:/backup)
Enter:

    <N> set source to remote NFS server
    <L> set source to Local tape (/dev/rmt/0h)
    <R> for Restore
    <Q> to quit
```

The system then prompts you to select the restore mode.

```
Select restore mode:
```

Step 5 Select **R** and press **Enter** to start the restore. The system returns a response similar to the following:

```
mount -F nfs -o retry=3 va-panthers:/backup /mnt

Available files:
va-blade20000317105201P.tar
va-blade20000317105337.tar
```

The system then prompts you to enter the filename to be restored.

```
Enter filename to restore from:
```

Step 6 Enter the filename for the most recent full backup performed on your system.

Note Full backups have a file name consisting of the name of the host and the timestamp with a .tar designation. Partial backups have a file name consisting of the name of the host, timestamp, and the letter “P” with a .tar designation.

The system then asks you if you really want to restore a backup:

```
Are you sure you want to restore a backup.
Current data in the MGC directory will be overwritten and lost.

Answer(Y/N):
```

Step 7 Enter **y** and press **Enter** if you are sure that you want to restore the Cisco MGC directory. The system returns a response similar to the following:

```
x etc, 0 bytes, 0 tape blocks
x etc/Copyright, 545 bytes, 2 tape blocks
x etc/CONFIG_LIB, 0 bytes, 0 tape blocks
x etc/CONFIG_LIB/new, 0 bytes, 0 tape blocks
```

```
.
.
restore from va-panthers:/backup/va-blade20000317105337.tar complete
#
```

Step 8 If you have performed any partial backups since the creation of the full backup you have just restored, repeat Steps 1 to 7 and restore the most recent partial backup.

Step 9 If your system does not have a dial plan configured, the procedures is complete. Otherwise, restore the contents of your dial plan as described in the "Restoring Data to the Main Memory Database" section on page 8-121.

Restoring Data to the Main Memory Database

Use this procedure to restore dial plan data, which was stored in the MMDB, in a single file as described in the "Performing a Backup Operation on the Main Memory Database" section on page 3-32.

Step 1 Log in to the active Cisco MGC and change directories to a local subdirectory under the base directory. For example, enter the following UNIX command to change to the /opt/CiscoMGC/local directory:

cd /opt/CiscoMGC/local

Step 2 Stop the MMDB by entering the following UNIX command:

ttreplic

Step 3 Run the MMDB restore script by entering the following UNIX command:

./restoreDb.sh *filename*

Where *filename* is the name of the database backup file.

For example, to restore the contents of a file called dplan to the MMDB, you would enter the following command:

./restoreDb.sh dplan

The system returns a response similar to the following:

```
Restoring database contents for DSN=howdydb into dplan
The Restore process is being initiated for the datastore howdydb
Files for /opt/TimesTen32/datastore/howdydb are being restored up onto standard output
Restore Complete
```

Step 4 Restore the MMDB by entering the following UNIX command:

ttreplic

Restoring Procedures for Cisco MGC Software Release 7.4(11) and up

This restoration method uses a script to restore the configuration data for the Cisco MGC software, select UNIX administrative files, and the Main Memory Database (MMDB).

Note This functionality is part of a patch to Release 7.4(11). If you want to use this functionality, you must be upgraded to the proper patch level. For more information on verifying the patch level of your system, refer to "Verifying the Patch Level of the Cisco MGC" section on page 3-104.

The following sections provide the restoration procedures:

- Restoring Data from a Local Tape Drive, page 8-118
- Restoring Data from a Remote Machine over the Network, page 8-119

Note These procedures assume that you have backed up your system configuration data regularly. The procedures for system configuration backup can be found in the "Backup Procedures for Cisco MGC Software from Release 7.4(11) and up" section on page 3-33.

Listing Backup Files

To list the backup files in a particular directory path, enter the following UNIX command on the Cisco MGC:

mgcrestore -d *path* **-l**

Where *path* is the directory path in which you have stored backup files, such as a directory on a remote server or a local tape drive.

The system returns a response similar to the following:

```
Backup files in /var/cisco
--------------------------------------------------
mgc_venus_20011010_153003_backup.tar
mgc_venus_20011011_153003_backup.tar
mgc_venus_20011012_153003_backup.tar
```

Restoring a Backup File

To restore the configuration data stored in a particular backup file, enter the following UNIX command on the affected Cisco MGC to run the restore script:

mgcrestore -d *path* **-f** *filename*

Where:

- *path*—The directory path to the location where your backup files are stored.
- *filename*—The file name of the backup file you want to restore.

For example, to restore a backup file called mgc_venus_20011012_153003_backup.tar stored in a directory path called /var/cisco, you would enter the following command:

mgcrestore -d /var/cisco -f mgc_venus_20011012_153003_backup.tar

Verifying Proper Configuration of Replication

If calls are not being preserved when your system performs a switchover, you should verify that your system is properly configured for replication of call data. To do this, verify that the value of the parameters in the XECfgParm.dat file on each host match the settings listed below, using the procedure in the "Rebooting Software to Modify Configuration Parameters" section on page 8-125.

```
*.SyscheckpointEnabled = true
replicator.portDataChannelSend = 2968
replicator.portDataChannelRecv = 2970
replicator.portCommChannelSend = 2972
replicator.portCommChannelRecv = 2974
replicator.reconnectInterval = 15
replicator.numberReadThreads = 1
```

Measurements Are Not Being Generated

If your Cisco MGC is not generating system measurements, perform the following procedure:

Step 1 Verify that the amdmpr process is running, as described in the "Verifying That Processes Are Running" section on page 3-3.

If the amdmpr process is not running, proceed to Step 2. Otherwise, proceed to Step 3.

Step 2 Verify that the *.disableMeas parameter in the XECfgParm.dat file is set to *false* on each host, using the procedure in the "Rebooting Software to Modify Configuration Parameters" section on page 8-125.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

Call Detail Records Are Not Being Generated

If call detail records are not being generated on your Cisco MGC, perform the following steps:

Step 1 Verify that the dmpr-01 process is running, as described in the "Verifying That Processes Are Running" section on page 3-3.

If the dmpr-01 process is not running, proceed to Step 2. Otherwise, proceed to Step 4.

Step 2 Verify that the settings for the dmprSink.dat file are correct, using the procedure in the "Configuring the Data Dumper" section on page A-2.

If that clears the alarm, the procedure is finished. Otherwise, proceed to Step 3.

Step 3 Verify that the settings for the CDR parameters in the XECfgParm.dat file on each host match those listed below, using the procedure in the "Rebooting Software to Modify Configuration Parameters" section on page 8-125.

```
cdrDmpr.openCDR         = true
cdrDmpr.callDetail      = /opt/CiscoMGC/local/cdbscript.sh
cdrDmpr.seqFile         = ../var/.cdr.seq
diskmonitor.CdrRmFinished = 0     # remove "finished" cdrs after X days (0 = immediate)
engine.CDRencodingFormat  = AnsiCDB
engine.CDRtimeStamp   = S
```

```
engine.CDRmessageTypes   = "1010,1020,1030,1040,1050,1060,1070"
```

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

Rebooting Your System to Modify Properties

When you are modifying certain properties on the Cisco MGC, it is required that you reboot your system as part of the modification process. To reboot your system as part of a property modification process, perform the following steps:

Step 1 Log in to your active Cisco MGC and change directories to the /opt/CiscoMGC/etc directory using the following UNIX command:

```
cd /opt/CiscoMGC/etc
```

Step 2 Open the XECfgParm.dat file in a text editor, such as vi.

Step 3 Search for the pom.dataSync property and ensure that it is set to *false*.

Step 4 Save the file and exit the text editor.

Step 5 Shut down the Cisco MGC software on your active Cisco MGC, as described in the "Shutting Down the Cisco MGC Software Manually" section on page 2-4. This causes the currently standby Cisco MGC to become the active Cisco MGC.

Step 6 Start the Cisco MGC software on the Cisco MGC, as described in the "Starting the Cisco MGC Software" section on page 2-2.

Step 7 Once the Cisco MGC software is fully activated, log in to the active Cisco MGC and perform a manual switchover, as described in the "Performing a Manual Switchover" section on page 3-80.

Step 8 Once the manual switchover is complete, log in to the newly active Cisco MGC, start an MML session and enter the following command to synchronize the Cisco MGCs:

```
prov-sync
```

Step 9 Once the synchronization is complete, perform a manual switchover, as described in the "Performing a Manual Switchover" section on page 3-80.

Step 10 Once the manual switchover is complete, log in to your newly standby Cisco MGC and change directories to the /opt/CiscoMGC/etc directory using the following UNIX command:

```
cd /opt/CiscoMGC/etc
```

Step 11 Open the XECfgParm.dat file in a text editor, such as vi.

Step 12 Search for the pom.dataSync property and ensure that it is set to *true*.

Step 13 Save the file and exit the text editor.

Step 14 Shut down the Cisco MGC software on your standby Cisco MGC, as described in the "Shutting Down the Cisco MGC Software Manually" section on page 2-4.

Step 15 Start the Cisco MGC software on your standby Cisco MGC, as described in the "Starting the Cisco MGC Software" section on page 2-2.

Rebooting Software to Modify Configuration Parameters

Sometimes you may need to change your configuration settings in the XECfgParm.dat file while the system is in-service. To do this, perform the following procedure:

Caution Performing this procedure stops the functioning of the Cisco MGC software. Perform this step only while in contact with Cisco Technical Assistance Center (TAC) personnel. Refer to the "Obtaining Technical Assistance" section on page xviii for information on contacting the Cisco TAC.

Step 1 Log in to the active Cisco MGC and change directories to the etc subdirectory by entering the following UNIX command:

```
cd /opt/CiscoMGC/etc
```

Step 2 Open the XECfgParm.dat using a text editor, such as vi.

Step 3 Search for the parameters specified in the referring procedure and verify that it is set to the correct value. If they are set correctly, proceed to Step 10. Otherwise, proceed to Step 4 to begin the process of correcting your configuration.

Step 4 Stop the Cisco MGC software on your active Cisco MGC, as described in the "Shutting Down the Cisco MGC Software Manually" section on page 2-4.

Step 5 Modify the incorrect parameters identified in Step 3 to match their correct values.

Step 6 Save your changes and close the text editor.

Step 7 Restart the Cisco MGC software on your active Cisco MGC, as described in the "Starting up the Cisco MGC software manually" section on page 2-2.

Step 8 Perform a manual switchover from the newly active Cisco MGC, as described in the "Performing a Manual Switchover" section on page 3-80.

Step 9 Repeat steps 2 through 8 for the newly active Cisco MGC.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 10.

Step 10 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.

Resolving a Failed Connection to a Peer

If you have lost connection to a peer component in your network, perform the following procedure to resolve the problem:

Step 1 Verify that the path to the affected peer is out-of-service, as described in the "Verifying the Status of all Destinations" section on page 3-8.

If the destination is in-service, or there is no destination associated with the peer, proceed to Step 2.

If the destination associated with the peer is out-of-service, bring the destination back into service, as described in the "SS7 Destination is Out of Service" section on page 8-57.

Note If the out-of-service destination is IP destination, perform the procedure described in "Media Gateway IP Destination/Link Out-of-Service" section on page 8-98.

If that resolves the problem, this procedure is complete. Otherwise, proceed to Step 2.

Step 2 Trace the route to the peer by entering the following UNIX command on your active Cisco MGC:

```
traceroute ip_addr
```

Where *ip_addr* is the IP address of the affected peer.

The system responds with a listing of the peers that are passed through on route to the identified peer.

If the system response indicates that the identified peer was reached with no problems, proceed to Step 4.

If the system response indicates that you were unable to reach the identified peer, proceed to Step 3.

Step 3 Log in to the peer identified in Step 2 and verify that the Ethernet interfaces for this peer are working correctly. Refer to the documentation for the peer for more information.

If the Ethernet interfaces are working properly, proceed to Step 4.

If the Ethernet interfaces are not working properly, replace the element that is not working properly. Refer to the documentation of the peer for more information. If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 4.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, refer to the "Obtaining Technical Assistance" section on page xviii.