CHAPTER 8

Troubleshooting the Cisco PGW 2200 Softswitch Platform

Revised: December 3, 2009, OL-0800-12

This chapter describes troubleshooting methods for the Cisco PGW 2200 Softswitch platform. It includes the following sections to help you isolate system problems:

- Troubleshooting Overview, page 8-1
- Troubleshooting Using Cisco PGW 2200 Softswitch Alarms, page 8-3
- Troubleshooting with System Logs, page 8-83
- Resolving SS7 Network Related Problems, page 8-88
- Resolving Bearer Channel Connection Problems, page 8-117
- Resolving SIP Communication Problems, page 8-150
- Tracing, page 8-150
- Platform Troubleshooting, page 8-164

Troubleshooting Overview

This chapter uses the alarms and logs that appear at the Cisco PGW 2200 Softswitch as the basis for isolating problems within the system. You can find a complete listing of alarms and logs in the Cisco PGW 2200 Softswitch Release 9 Messages Reference.

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 PGW 2200 Softswitch software, the Cisco WAN Manager, the Cisco Media Gateway Controller Node Manager (CMNM), 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 PGW 2200 Softswitch platform 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.
Troubleshooting Overview

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

- Cisco ITP-L Failure
- Cisco PGW 2200 Softswitch Failure
- Operating System Failure

Cisco ITP-L Failure

Each Cisco IP Transfer Point LinkExtender (ITP-L) has an Reliable User Datagram Protocol (RUDP)/User Datagram Protocol (UDP)/IP connection to each Cisco PGW 2200 Softswitch for the transfer of Message Transfer Part (MTP) Level 3 (MTP3), ISDN User Part (ISUP), and Transaction Capabilities Application Part (TCAP) information. A Cisco ITP-L platform failure results in the surviving Cisco ITP-L platforms taking over the distribution of messages to the active Cisco PGW 2200 Softswitch. Cisco ITP-L platforms should be provisioned so that half of the platforms can support the entire signaling load. The result is that a Cisco ITP-L platform failure has no significant effect on call processing.

There are several Cisco ITP-L failure scenarios to consider:

- An IP link failure between the Cisco ITP-L and the Cisco PGW 2200 Softswitch, 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 ITP-L.
- In the case where MTP2 failed (equivalent to a Cisco ITP-L 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 PGW 2200 Softswitch fault is detected by a Cisco ITP-L timer, a coordination mechanism causes SS7 messaging to flow to the newly active (formerly standby) Cisco PGW 2200 Softswitch. The standby Cisco PGW 2200 Softswitch assumes control for all calls in progress and all new calls.

Cisco PGW 2200 Softswitch Failure

Cisco PGW 2200 Softswitches run in active-standby mode. The call-processing application is active on only one Cisco PGW 2200 Softswitch at a time, and the application switches to the standby platform when a critical alarm occurs. The result is that Cisco PGW 2200 Softswitch failure and switchover events are invisible to the SS7 signaling network.

Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch should fail, there is a disconnection from the process manager and a switchover to the standby Cisco PGW 2200 Softswitch.

Operating System Failure

An operating system (OS) or hardware failure in the active Cisco PGW 2200 Softswitch can also cause a switchover to the standby Cisco PGW 2200 Softswitch. The failover daemon in the standby Cisco PGW 2200 Softswitch detects the failure of the active Cisco PGW 2200 Softswitch and instructs the process manager to initiate a switchover. The standby Cisco PGW 2200 Softswitch then takes over all call-processing functions. The switchover is transparent to all the Cisco ITP-Ls.
Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

The Cisco PGW 2200 Softswitch generates alarms to indicate problems with processes, routes, linksets, signaling links, and bearer channels. The Cisco PGW 2200 Softswitch Release 9 Messages Reference lists all of the Cisco PGW 2200 Softswitch 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 8-4.

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, see the “Configuring the Data Dumper” section on page A-2.

Troubleshooting using Cisco PGW 2200 Softswitch alarms is described in the following sections:

- Retrieving All Active Alarms, page 8-3
- Acknowledging Alarms, page 8-3
- Alarm Troubleshooting Procedures, page 8-4

Retrieving All Active Alarms

To retrieve all active alarms, log in to the active Cisco PGW 2200 Softswitch, 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"
"TOCM-01: 2000-02-26 09:17:00.690,"
"TOCM-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: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 PGW 2200 Softswitch, start an MML session, and enter the following command:

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

Where:
Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

- **comp**—The MML name of the component. A complete list of components can be found in the *Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide*. You can retrieve a list of select provisioned components by entering the `prov-rtrv:all` 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"
```  

### 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 PGW 2200 Softswitch Release 9 Messages Reference*.

### All Conn Cntl Links Fail

This alarm occurs when the MGCP 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** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Verify that the Ethernet interfaces between the Cisco PGW 2200 Softswitch and the associated media gateway are working properly.

**Note** Information on verifying the proper operation of an Ethernet interface on the Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch 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 MGCP sessions are operating normally. See the documentation for the affected media gateway for more information on verifying the functioning of the MGCP sessions.

If the MGCP sessions are not operating normally, return the MGCP sessions to normal operations, as described in the documentation for the affected media gateway. Otherwise, proceed to Step 3.
Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**All C7 IP Links Fail**

This alarm occurs when communication is lost to all Cisco ITP-Ls of every configured protocol family. This defaults to a critical alarm, and causes an automatic switchover, if a standby Cisco PGW 2200 Softswitch is present.

*Note*

Generation of this alarm is now controlled by an XECfgParm.dat parameter, *AllLinksFailCausesFailover*. When this parameter is set to *false* (the default value), this alarm is not generated when the alarm condition occurs. If you want this alarm to be generated, you must set the parameter to *true*, using the procedure defined in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.

If your Cisco PGW 2200 Softswitches are in separate geographic locations, we recommend that you set the value of *AllLinksFailCausesFailover to true.*

**Corrective Action**

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

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** If your system is provisioned with destinations that use more than one version of SS7, ensure that this alarm is configured correctly, as described in the “Verifying Configuration to Support Multiple Versions of SS7” section on page 8-115.

**Step 3** Verify that the Cisco ITP-Ls are operating normally, as described in the “Checking Equipment Status” section on page 6-2 and the “Using the Cisco ITP-L Operating System to Check Status” section on page 6-5.

**Step 4** Verify that the Ethernet interfaces between the Cisco PGW 2200 Softswitch and the Cisco ITP-Ls are working properly.

*Note* Information on verifying the proper operation of an Ethernet interface on the Cisco PGW 2200 Softswitch 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 5.

*Note* Information on removing and replacing an Ethernet interface card on the Cisco PGW 2200 Softswitch can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing an interface card on the Cisco ITP-L can be found in the “Replacing a Cisco ITP-L” section on page 6-6.
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Step 5  Verify that the configuration for your system is correct. To verify the provisioning data for your Cisco PGW 2200 Softswitch, use the `prov-rtrv` MML command, as described in the “Retrieving Provisioning Data” section on page 3-68. To verify the provisioning data for the Cisco ITP-Ls, use show commands, as described in the “Using the Cisco ITP-L Operating System to Check Status” section on page 6-5.

If the configuration of your Cisco PGW 2200 Softswitch is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

If the configuration of your Cisco ITP-Ls is incorrect, modify the provisioning data for your system. See the Cisco Signaling Link Terminal document for more information.

If the configuration of both the Cisco PGW 2200 Softswitch and the Cisco ITP-Ls are correct, then 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

### All ISDN BRI IP Conn Fail

This alarm occurs when all IP connections supporting an ISDN BRI data pathway has failed.

**Corrective Action**

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

**Step 1**  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**  Determine the health of the associated media gateway using the procedures in the user documentation for the media gateway.

If the media gateway is working correctly, proceed to Step 3.

If the media gateway is not healthy, restore it using the procedures in the user documentation for the media gateway. If those procedures restore the media gateway and this alarm clears, the procedure is complete. Otherwise, proceed to Step 3.

**Step 3**  Verify the functioning of the cabling between the Cisco PGW 2200 Softswitch and the switch.

If the cables are functioning properly, proceed to Step 4.

If you find bad cable(s), replace them. If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 4.

**Step 4**  Verify the functioning of the associated switch. See the documentation for your switch for the necessary steps.

If the switch is functioning properly, proceed to Step 5.

If the switch is not functioning properly, see the appropriate troubleshooting procedures in the documentation for the switch. If that corrects the problem, the procedure is complete. Otherwise, proceed to Step 7.

**Step 5**  Check the IP connectivity between the Cisco PGW 2200 Softswitch and the associated Cisco BRI voice gateway.

If the IP connectivity is good, proceed to Step 6.
If the IP connectivity is bad, restore the IP connectivity. If the alarm clears after the IP connectivity is restored, the procedure is complete. Otherwise, proceed to Step 6.

**Step 6**

Verify that the provisioning data for your ISDN BRI backhaul connect is correct. To verify the provisioning data, use the `prov-rtrv` MML command, as described in the “Retrieving Provisioning Data” section on page 3-68.

If the provisioning data is correct, proceed to Step 7.

If the provisioning data is not correct, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

**Step 7**

Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**All ISDN IP Conn Fail**

This alarm occurs when communication is lost to all ISDN IP connections. The severity of this alarm is Critical, which causes an automatic switchover if a standby Cisco PGW 2200 Softswitch is present.

**Note**

The ability to change the severity level of this alarm is implemented in a patch (CSCOgs059) for Release 9.5(2). The severity level of this alarm is now controlled by an XECfgParm.dat parameter, `*.AllISDNLinksFailCausesFailover`. When this parameter is set to `false` (the default value), this alarm has a severity level of Major. If you set this parameter to `true`, this alarm has a severity level of Critical.

This property should be set to `true` if your Cisco PGW 2200 Softswitches are in separate geographic locations. You can also set this parameter to `true` if your system is not processing SS7 calls and you want your system to perform an automatic switchover should all of the ISDN IP connections fail. To change the value of this parameter, use the procedure defined in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.

**Corrective Action**

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

**Step 1**

Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**

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

**Step 3**

Verify that the Ethernet interfaces between the Cisco PGW 2200 Softswitch and the media gateways are working properly.

**Note**

Information on verifying the proper operation of an Ethernet interface on the Cisco PGW 2200 Softswitch 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.
Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

Note
Information on removing and replacing an Ethernet interface card on the Cisco PGW 2200 Softswitch 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
Verify that the configuration for your system is correct. To verify the provisioning data for your Cisco PGW 2200 Softswitch, use the `prov-rtrv` MML command, as described in the “Retrieving Provisioning Data” section on page 3-68. To verify the provisioning data for the media gateways, use show commands, as described in the associated documentation.

If the configuration of your Cisco PGW 2200 Softswitch is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

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

If the configuration of the Cisco PGW 2200 Softswitch and the media gateways are correct, then proceed to Step 5.

Step 5
Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

All M3UAKEY Ack Pending
This alarm occurs when the Cisco PGW 2200 Softswitch cannot send or receive traffic for the identified SS7 signaling service associated with a Cisco ITP.

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

Step 1
Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2
Determine the AS definitions on the associated Cisco ITP. See the documentation for your Cisco ITP for more information.

Step 3
Retrieve the settings for the affected M3UA routing keys using the `prov-rtrv` MML command, as described in the “Retrieving Provisioning Data” section on page 3-68.

Step 4
The AS definitions should match the routing contexts of the M3UA routing keys. If they match, proceed to Step 6. Otherwise, proceed to Step 5.

Step 5
Open a dynamic reconfiguration session to modify the routing contexts of the M3UA routing keys, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

If this corrects the problem, the procedure is complete. Otherwise, proceed to Step 6.

Step 6
Verify that the AS is not shutdown on the Cisco ITP. See the documentation for your Cisco ITP for more information. If the AS is shutdown, restart it. Otherwise, proceed to Step 7.

If this corrects 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**All M3UA Assoc Fail**

This alarm occurs when all M3UA associations transporting SS7 signaling have failed.

---

**Note**

Generation of this alarm is now controlled by an XECfgParm.dat parameter, *.AllLinksFailCausesFailover. When this parameter is set to false (the default value), this alarm is not generated when the alarm condition occurs. If you want this alarm to be generated, you must set the parameter to true, using the procedure defined in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.

If your Cisco PGW 2200 Softswitches are in separate geographic locations, we recommend that you set the value of *.AllLinksFailCausesFailover to true.

---

**Corrective Action**

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

---

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Verify that the Cisco ITPs are operating normally. See the documentation for your Cisco ITP for more information.

If you find that the Cisco ITPs are operating normally, proceed to Step 3. Otherwise, correct the problems.

If this corrects the problem, the procedure is complete. Otherwise, proceed to Step 3.

**Step 3** Verify that the Ethernet interfaces between the Cisco PGW 2200 Softswitch and the Cisco ITPs are working properly.

---

**Note**

Information on verifying the proper operation of an Ethernet interface on the Cisco PGW 2200 Softswitch 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 Cisco ITP 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 PGW 2200 Softswitch 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 ITP can be found in its associated documentation.

**Step 4** Verify that the M3UA provisioning data on your Cisco PGW 2200 Softswitch is correct.

If the provisioning data is correct, proceed to Step 6. Otherwise, proceed to Step 5.
**All SUAKEY Ack Pending**

This alarm occurs when the Cisco PGW 2200 Softswitch cannot send or receive traffic for the identified SS7 subsystem.

**Corrective Action**

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

- **Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
- **Step 2** Determine the AS definitions on the associated Cisco ITP. See the documentation for your Cisco ITP for more information.
- **Step 3** Retrieve the settings for the affected SUA routing keys using the `prov-rtrv` MML command, as described in the “Retrieving Provisioning Data” section on page 3-68.
- **Step 4** The AS definitions should match the routing contexts of the SUA routing keys. If they match, proceed to Step 6. Otherwise, proceed to Step 5.
- **Step 5** Open a dynamic reconfiguration session to modify the routing contexts of the M3UA routing keys, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.
  
  If this corrects the problem, the procedure is complete. Otherwise, proceed to Step 6.
- **Step 6** Verify that the AS is not shutdown on the Cisco ITP. See the documentation for your Cisco ITP for more information. If the AS is shutdown, restart it. Otherwise, proceed to Step 7.
  
  If this corrects 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**All SUA Assoc Fail**

This alarm occurs when all SUA associations transporting SS7 signaling have failed.

**Note**

Generation of this alarm is now controlled by an XECfgParm.dat parameter, `*.AllLinksFailCausesFailover`. When this parameter is set to `false` (the default value), this alarm is not generated when the alarm condition occurs. If you want this alarm to be generated, you must set the parameter to `true`, using the procedure defined in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.
If your Cisco PGW 2200 Softswitches are in separate geographic locations, we recommend that you set the value of *AllLinksFailCausesFailover to true.

**Corrective Action**

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

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Verify that the Cisco ITPs are operating normally. See the documentation for your Cisco ITP for more information.

If you find that the Cisco ITPs are operating normally, proceed to Step 3. Otherwise, correct the problems.

If this corrects the problem, the procedure is complete. Otherwise, proceed to Step 3.

**Step 3** Verify that the Ethernet interfaces between the Cisco PGW 2200 Softswitch and the Cisco ITPs are working properly.

**Note** Information on verifying the proper operation of an Ethernet interface on the Cisco PGW 2200 Softswitch 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 Cisco ITP 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 PGW 2200 Softswitch 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 ITP can be found in its associated documentation.

**Step 4** Verify that the SUA provisioning data on your Cisco PGW 2200 Softswitch is correct.

If the provisioning data is correct, proceed to Step 6. Otherwise, proceed to Step 5.

**Step 5** Open a dynamic reconfiguration session to modify the SUA provisioning data, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

If this corrects the problem, the procedure is complete. Otherwise, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**ANAL: ALoopCtExceeded**

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**
Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**
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 3-135.

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. See the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65.

If there are no infinite loops in your A-number dial plan, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**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 8-114.

---

**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 8-114.

---

**ANAL: ATableFlt_DgtRangeError**

This alarm occurs when the A-number analysis digit tree has been accessed with a digit that is out of range for the digit tree table. This alarm could occur if the system was incorrectly configured to support a base 10 dial plan, and an overdecadic digit was received from the line and passed to analysis.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:
Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Verify that the parameter, *.OverdecadicDigitsEnabled, is set correctly in the XECfgParm.dat file on each host.

Note The setting of this parameter should reflect the dial plan restrictions for the protocol in use. If the configured protocol supports the use of overdecadic digits, the parameter should be set to true, and vice versa.

If the setting for the parameter is correct, proceed to Step 3. Otherwise, reboot your software using the procedure described in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.

Step 3 If the setting for the parameter is false, check the received digit string for presence of an overdecadic digit. If the digit string does not have an overdecadic digit, proceed to Step 5. If the digit string does have an overdecadic digit, proceed to Step 4.

If the setting for the parameter is true, proceed to Step 5.

Step 4 Check the compliancy documentation for the configured protocol.

If the documentation indicates that overdecadic digits are supported, change the setting for the *.OverdecadicDigitsEnabled XECfgParm.dat parameter to true on both hosts, using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.

If the documentation indicates that overdecadic digits are not supported, proceed to Step 5.

Step 5 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Validate that there are no infinite loops in the B-number dial plan, as described in the “Verifying a Dial Plan Translation” section on page 3-135.

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. See the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65.

If there are no infinite loops in your B-number dial plan, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**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 8-114.

**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**  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
- **Step 2**  Verify that all of the configured announcement IDs are within the range 0 through 9999, using the `numan-rtrv` MML command. See the Cisco PGW 2200 Softswitch Release 9.8 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. See the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65. Otherwise, proceed to Step 3.

- **Step 3**  Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114.

---

**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 8-114.
Chapter 8      Troubleshooting the Cisco PGW 2200 Softswitch Platform

Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

Chapter 8

Troubleshooting the Cisco PGW 2200 Softswitch Platform

Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

**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 8-114.

**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 8-114.

**ANAL: BTableFlt_DgtRangeError**

This alarm occurs when the B-number analysis digit tree has been accessed with a digit that is out of range for the digit tree table. This alarm could occur if the system was incorrectly configured to support a base 10 dial plan, and an overdecadic digit was received from the line and passed to analysis.

**Corrective Action**

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

---

**Step 1**

Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**

Verify that the parameter, *.OverdecadicDigitsEnabled, is set correctly in the XECfgParm.dat file on each host.

**Note**

The setting of this parameter should reflect the dial plan restrictions for the protocol in use. If the configured protocol supports the use of overdecadic digits, the parameter should be set to true, and vice versa.

If the setting for the parameter is correct, proceed to Step 3. Otherwise, update the parameter settings in the XECfgParm.dat files using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.

**Step 3**

If the setting for the parameter is false, check the received digit string for presence of an overdecadic digit. If the digit string does not have an overdecadic digit, proceed to Step 5. If the digit string does have an overdecadic digit, proceed to Step 4.

If the setting for the parameter is true, proceed to Step 5.

**Step 4**

Check the compliance documentation for the configured protocol.
If the documentation indicates that overdecadic digits are supported, change the setting for the *OverdecadicDigitsEnabled XECfgParm.dat parameter to true on each host using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.

If the documentation indicates that overdecadic digits are not supported, proceed to Step 5.

**Step 5** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

### 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** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Verify that the associated cause table contains all of the existing call context cause values, using the `numan-rtrv` MML command. See the *Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide* for more information.

If the cause table is incomplete, modify its value using the `numan-ed` MML command. See the *Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide* for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65. Otherwise, proceed to Step 3.

**Step 3** Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114.

---

### 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** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Verify that the associated B-number digit modification table is correct, using the `numan-rtrv` MML command. See the *Cisco PGW 2200 Softswitch Release 9.8 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. See the *Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide* for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65. Otherwise, proceed to Step 3.
Step 3 Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114.

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 8-114.

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 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Verify that the associated location table contains all of the possible references from the cause table, using the `numan-rtrv` MML command. See the Cisco PGW 2200 Softswitch Release 9.8 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. See the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65. Otherwise, proceed to Step 3.

Step 3 Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114.

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 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Verify that the associated result table contains all of the possible references from the cause and location tables, using the `numan-rtrv` MML command. See the Cisco PGW 2200 Softswitch Release 9.8 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. See the *Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide* for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65. Otherwise, proceed to Step 3.

**Step 3**

Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114.

---

**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 8-114.

**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**
Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**
Verify that the affected announcement ID is within the range 0 through 9999, using the `numan-rtrv` MML command. See the *Cisco PGW 2200 Softswitch Release 9.8 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 3. See the *Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide* for more information. Otherwise, proceed to Step 3.

**Step 3**
Verify that the affected B-number is at least 4 digits long, using the `numan-rtrv` MML command. See the *Cisco PGW 2200 Softswitch Release 9.8 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. *Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide* for more information. Otherwise, proceed to Step 4.

**Step 4**
If you modified your dial plan, save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65. Otherwise, proceed to Step 5.
Step 5  Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114.

**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** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Verify that the specified application points in the result data is correct, using the `numan-rtrv` MML command. See the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide for more information.

If any of the application points are incorrect, modify their value using the `numan-ed` MML command. See the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65. Otherwise, proceed to Step 3.

**Step 3** Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114.

**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 8-114.

**ANAL: CustId/StartIdx Missing**

This alarm occurs when the property CustGrpId is not present on the identified trunk group. This is 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** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2 Verify that the value of the CustGrpId property for the associated trunk group is correct by logging in to the active Cisco PGW 2200 Softswitch, starting an MML session, and entering the following command:

```
prov-rtrv:trnkgrpprop:name="comp_name"
```

Where `comp_name` is the MML name for the affected trunk group.

For example, if you wanted to verify the properties for an trunk group called `1001`, you would enter the following command:

```
prov-rtrv:trnkgrpprop:name="1001"
```

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:trnkgrpprop"
/*
...
CustGrpId=2222
...
```

Step 3 If you need to modify your settings, start a provisioning session as described in the “Starting a Provisioning Session” section on page 3-64.

Step 4 If the CustGrpId property is missing from the affected 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 8-118. Once you have entered the CustGrpId value, you can return the SS7 signaling service to the in-service administrative state.
```

```
prov-ed:trnkgrp:name="comp_name", CustGrpId=number
```

Where:

- `comp_name`—MML name for the affected trunk group.
- `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 3-65.

If the alarm clears, the procedure is complete. Otherwise, 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, See the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**ANAL:DataBaseAccessFail**

This alarm occurs when certain functions in generic analysis has failed. Failure of any of the following general analysis functions causes this alarm to be triggered:
• ReadANumDpSelection()—Alarm is found in the Analysis MDL log.
• CheckEPortedHandling(VAR BNumRecd : BNumberElem, B_DgtBuff : Dgtbuff, VAR ResultsFromBnoForUpdate : AnalyseBnoResults): GeneralActionRslts—Alarm is found in the B_Analysis MDL log.
• CheckERouteNumHandling(B_DgtBuff : Dgtbuff, VAR ResultsFromBnoForUpdate : AnalyseBnoResults): GeneralActionRslts—Alarm is found in the B_Analysis MDL log.
• ANumberHandling()—Alarm is found in either the B_Analysis or A_Analysis MDL log.
• BNumberHandling()—Alarm is found in the MDL log as B_Analysis.

Corrective Action

| Step 1 | Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87. |
| Step 2 | Verify that the parameter, engine.SysConnectDataAccess, is set to true in the XECfgParm.dat file on the active Cisco PGW 2200 Softswitch. If the setting is correct, proceed to Step 4. Otherwise, update the value of the parameter for each host, using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178. If correcting the setting does not clear the alarm, proceed to Step 4. |
| Step 3 | Perform a call trace, as described in “Performing a Call Trace” section on page 8-151. |
| Step 4 | Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx. |

**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 8-114.

**ANAL:dpselection_table_fail**

This alarm occurs when the correct dial plan selection could not be determined.

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 8-114.

**ANAL:getDialplanBase_fail**

This alarm occurs when the Cisco PGW 2200 Softswitch could not load or generate the dial plan.
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 8-114.

**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** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Display the valid trunk group types using the `prov-rtrv` MML command as described in the “Retrieving Provisioning Data” section on page 3-68.

**Step 3** Correct the invalid trunk group type in the route analysis table using the `numan-ed` MML command. See the *Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide* for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65.

If the alarm clears, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**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 8-114.

**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 8-114.
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:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Verify that the NOA table uses all of the existing call context NOA values using the <code>numan-rtrv</code> MML command. See the <em>Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide</em> for more information. If the NOA table is missing any of the existing call context NOA values, add them using the <code>numan-ed</code> MML command. See the <em>Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide</em> for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65. Otherwise, proceed to Step 3.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114.</td>
</tr>
</tbody>
</table>

ANAL: Prof_GetFail_NOATbl_A

This alarm occurs during profile analysis when the NOA table is unreadable. This can be due either to the NOA table being corrupted, or to a failure in the underlying software.

Corrective Action

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.</td>
</tr>
</tbody>
</table>

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:
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Verify that the NPI table uses all of the possible references from the NOA table using the `numan-rtrv` MML command. See the *Cisco PGW 2200 Softswitch Release 9.8 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. See the *Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide* for more information.

Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65. Otherwise, proceed to Step 3.

**Step 3** Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114.

---

**ANAL: Prof_GetFail_NPITbl_A**

This alarm occurs during profile analysis when the NPI table is unreadable. This can be due either to the NOA table being corrupted, or to a failure in the underlying software.

**Corrective Action**

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

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.

**Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**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** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Verify that the result table uses all of the possible references from the NOA and NPI tables using the `numan-rtrv` MML command. See the *Cisco PGW 2200 Softswitch Release 9.8 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. See the *Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide* for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65. Otherwise, proceed to Step 3.
Step 3 Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114.

**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** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Verify that the NPA values have been properly provisioned for the trunk group using the `numan-rtrv` MML command. See the *Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide* for more information. If the NPA values are incorrect, modify them using the `numan-ed` MML command. See the *Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide* for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65. Otherwise, proceed to Step 3.

**Step 3** Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114.

**ANAL: Prof_InvlRslts_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 8-114.

**ANAL: Prof_InvlRslts_NOATbl_A**

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. The immediate result index indicates that analysis should start reading results now but the NPI index indicates that another table read is required to find the correct result table index. These results are logically incompatible. Most likely, this alarm 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, perform the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Verify that the specified application points in the result data is correct, using the <strong>numan-rtrv</strong> MML command. See the <em>Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide</em> for more information. If any of the application points are incorrect, modify their value using the <strong>numan-ed</strong> MML command. See the <em>Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide</em> for more information. Save and activate your dial plan changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65. Otherwise, proceed to Step 2.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Verify that the data for the provisioned route lists is correct by logging in to the active Cisco PGW 2200 Softswitch, starting an MML session, and entering the following command: prov-rtrv:rtlist:<em>all</em></td>
</tr>
</tbody>
</table>

---

[Note: The original text contains various hyperlinks and commands, which are not displayed in this natural text representation.]
Step 3  If there is incorrect data for the route lists, correct it by using the prov-ed MML command. Otherwise, proceed to Step 4. See the Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide for more information on provisioning route lists.

Step 4  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

ANAL: Rte_TableHopCtrExceeded

This alarm occurs when generic analysis fails due to excessive number of routing table changes.

Corrective Action

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

Step 1  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Test for a loop in the routing configuration using the following steps:
   a. Export the routing configuration to a file, as described in the “Exporting Provisioning Data” section on page 3-75.
   b. Import the routing configuration file created in Step 2a, as described in the “Importing Provisioning Data” section on page 3-74.
      If the import fails, proceed to Step 3. Otherwise, proceed to Step 4.

Step 3  Perform a call trace, as described in the “Performing a Call Trace” section on page 8-151.

Step 4  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 8-114.

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 8-114.

**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 8-114.

**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 8-114.

**ANAL: TableFail_BearerCapTable**

This alarm occurs when the bearer capability table could not be read during generic analysis.

Corrective Action

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

---

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.

**Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**ANAL: TableFail_CondRouteDescTable**

This alarm occurs when the conditional route description table could not be read during generic analysis.

Corrective Action

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

---

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
Step 3  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**ANAL: TableFail_CondRouteTable**

This alarm occurs when the conditional routing table could not be read during generic analysis.

**Corrective Action**

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

- **Step 1**  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
- **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 8-114.
  
  If that procedure resolves the problem, the procedure is finished. Otherwise, proceed to Step 2.
- **Step 3**  Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
- **Step 4**  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**ANAL: TableFail_CPCTable**

This alarm occurs when the calling party category (CPC) table could not be read during generic analysis.

**Corrective Action**

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

- **Step 1**  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
- **Step 2**  Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
- **Step 3**  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**ANAL: TableFail_RouteHolTable**

This alarm occurs when route holiday table could not be read during generic analysis.

**Corrective Action**

To correct the problem identified by this alarm, perform the following steps:
Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

Step 1  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
Step 3  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

ANAL: TableFail_PercRouteTable

This alarm occurs when the percentage route holiday table could not be read during generic analysis.

Corrective Action

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

Step 1  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
Step 3  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

ANAL: TableFail_TMRTable

This alarm occurs when the transmission medium requirements (TMR) table could not be read during generic analysis.

Corrective Action

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

Step 1  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
Step 3  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

ANAL: TableFail_TNSTable

This alarm occurs when the transit network selection (TNS) table could not be read during generic analysis.
Corrective Action

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.</td>
</tr>
</tbody>
</table>

**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 8-114.

**Association Degraded**

This alarm occurs when one of the destination addresses for an SCTP association has failed, but the association is still in-service (IS).

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the “Resolving an Association Alarm” section on page 8-115.

**Association Fail**

This alarm occurs when an SCTP association has failed due to an IP connectivity failure or an out-of-service (OOS) destination.

Corrective Action

To correct the problem identified by this alarm, perform the procedure in the “Resolving an Association Alarm” section on page 8-115.

**C7LNK ALGNMT LOST**

This alarm occurs when the MTP2 for the C7 link between a Cisco ITP-L and an associated APC has lost alignment.
Corrective Action

To correct the problem identified by this alarm, use the diagnostics on the affected Cisco ITP-L 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 PGW 2200 Softswitch.

Corrective Action

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

- **Step 1**: Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
- **Step 2**: Verify the status of the links associated with the affected DPC, as described in the “Retrieving Service State of C7/SS7 Links or Linksets” section on page 3-44.
  
  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 3**: Return the out-of-service links to service, as described in the “Setting the Service State of a C7/SS7 Link or Linkset” section on page 8-98.
  
  If that does not resolve the problem, proceed to Step 3.
  
- **Step 4**: Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

C7LNK CONGESTION

This alarm occurs when an SS7 MTP2 link becomes congested and it cannot receive any more messages.

Corrective Action

If this alarm occurs repeatedly, perform the following steps to correct the problem:

- **Step 1**: Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
- **Step 2**: Reduce the amount of traffic from the far-end associated with the affected link.
  
  If that clears the alarm, the procedure is complete. Otherwise, proceed to Step 2.
  
- **Step 3**: Add additional links to the linkset associated with the affected link. See the Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide for more information about adding links.
  
  If that does not resolve the problem, proceed to Step 3.
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Step 4  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 C7/SS7 Link or Linkset” section on page 8-98, when the maintenance is complete.

C7SLTLinkCong

This alarm occurs when an SS7 link on a 4-link Cisco ITP-L is congested.

Corrective Action

If this alarm occurs repeatedly, perform the following steps to correct the problem:

Step 1  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Reroute the SS7 traffic to other links to reduce the congestion. See the Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide for more information about adding links. 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Call Back Feature Insertion Failure

This alarm occurs when an attempt to insert a call back feature entry in the main memory database fails. When this insertion fails, the call back feature does not work.

Corrective Action

Contact the Cisco TAC to analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Call Back Feature Deletion Failure

This alarm occurs when an attempt to delete a call back feature entry from the main memory database fails. When this deletion fails, the call back feature does not work.
Corrective Action

Contact the Cisco TAC to analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Charge Table Access Failure

This alarm occurs when the Cisco PGW 2200 Softswitch could not access the charge table.

Corrective Action

To correct the problem identified by this alarm, check for the presence of the Charge Table Load Failure alarm, using the procedure in “Retrieving All Active Alarms” section on page 8-3. If this alarm is present, perform the corrective action for that alarm. Otherwise, the procedure is complete.

Charge Table Load Failure

This alarm occurs when a Cisco PGW 2200 Softswitch process is unable to load the charge table.

Corrective Action

Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Verify whether a charge table is present on your system by logging in to your active Cisco PGW 2200 Softswitch, starting an MML session, and entering the following command:

```
prov-rtrv:charge:"all"
```

The system responds with a list of elements in the charge table, or with an error indicating that a charge table does not exist.

If a charge table is not present, provision a charge table, as described in the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide.

If a charge table is present, verify that the information returned is correct. If the information is correct, proceed to Step 3. Otherwise, correct the contents of the charge table, as described in the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide.

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Comm Srvc Creation Error

This alarm occurs when an error occurred while creating or opening a communication service.

Corrective Action

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

Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  Shutdown the Cisco PGW 2200 Softswitch software on the standby Cisco PGW 2200 Softswitch, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

Step 3  Restart the Cisco PGW 2200 Softswitch software on the standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

Step 4  Perform a manual switchover operation, as described in the “Performing a Manual Switchover” section on page 3-95.

**Warning** Switchover operations cause the loss of all SS7 messages transmitted to the Cisco PGW 2200 Softswitch for approximately three seconds. This affects unstable in-progress calls as well as new calls. Stable in-progress calls are not affected.

Step 5  Shutdown the Cisco PGW 2200 Softswitch software on the newly standby Cisco PGW 2200 Softswitch, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

Step 6  Restart the Cisco PGW 2200 Softswitch software on the newly standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

Step 7  Perform a manual switchover operation, as described in the “Performing a Manual Switchover” section on page 3-95.

**Warning** Switchover operations cause the loss of all SS7 messages transmitted to the Cisco PGW 2200 Softswitch for approximately three seconds. This affects unstable in-progress calls as well as new calls. Stable in-progress calls are not affected.

Step 8  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**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  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Search the active system log file, as described in the “Viewing System Logs” section on page 8-83, 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 3.

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 3-66.

If that corrects the problem, the procedure is complete. Otherwise, proceed to Step 3.
CTI Connection Failed

This alarm occurs when the CTI connection to the Cisco CallManager cluster has failed.

Corrective Action

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

Step 1 Collect diagnostic information from your system.

Step 2 Verify that the Ethernet interfaces between the Cisco PGW 2200 Softswitch and the Cisco CallManager cluster are working properly.

You can determine the status of the Ethernet interfaces on the Cisco PGW 2200 Softswitch using the Cisco IPT Platform Administration application. See the on-line help topic for this subject for more information. You can find information on verifying the proper functioning of an Ethernet interface on the Cisco CallManager cluster in the associated documentation.

If the Ethernet connections are working correctly, proceed to Step 4. Otherwise, proceed to Step 3.

Step 3 If an element of the Ethernet connection (such as a cable or an Ethernet interface card) is not working properly, replace it. Once the replacement is complete, return to Step 2.

Information on removing and replacing an Ethernet interface card on either platform can be found in the documentation that came with the platform.

Step 4 Verify that the MGCP sessions are operating normally. See the documentation for the affected media gateway for more information on verifying the functioning of the MGCP sessions.

If the MGCP sessions are not operating normally, return the MGCP sessions to normal operations, as described in the documentation for the affected Cisco CallManager cluster. Otherwise, proceed to Step 5.

Step 5 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

CTI Version Mismatch

This alarm occurs when the CTI version of the CTI Manager component configured on Cisco PGW 2200 Softswitch is not compatible with the version on the CTI Manager.

Corrective Action

Check the version of CTI Manager and install appropriate patches on the Cisco PGW 2200 Softswitch to make it compatible with the version on CTI Manager.
Dial Plan Loading Failed

This alarm occurs when a dial plan has not loaded properly.

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 8-114.

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 PGW 2200 Softswitch, as described in the “Deleting Unnecessary Files to Increase Available Disk Space” section on page 8-165.

EISUP: Unexpected Msg/Par

This alarm occurs when the EISUP module has received an unsupported message or parameter. This alarm is most likely to occur when the local EISUP version is older than the EISUP version used by the Cisco PGW 2200 Softswitch or Cisco H.323 Signaling Interface (HSI) on the other end.

Corrective Action

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

---

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** To upgrade the version of EISUP locally, you must either upgrade the Cisco PGW 2200 Softswitch software to same release as the other Cisco PGW 2200 Softswitch, or to the release supported by your current version of the Cisco HSI software.

The steps required to upgrade your Cisco PGW 2200 Softswitch software are found in the *Cisco PGW 2200 Softswitch Release 9 Software Installation and Configuration Guide*. If upgrading the Cisco PGW 2200 Softswitch software clears the alarm, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

ENGINE CONFIG FAIL

This alarm occurs when a component in the engine configuration has failed.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

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 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Search the active system log file for log messages indicating which component is raising this alarm, using the procedure described in the “Viewing System Logs” section on page 8-83.

If there are logs that indicate a failed component, proceed to Step 2.

If there are no logs that indicate a failed component, proceed to Step 3.

Step 3 Begin a dynamic reconfiguration session to reprovision the failed component, using the procedure described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 3.

Step 4 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

Warning

Switchover operations cause the loss of all SS7 messages transmitted to the Cisco PGW 2200 Softswitch for approximately three seconds. This affects unstable in-progress calls as well as new calls. Stable in-progress calls are not affected.

---

Step 5 Perform a manual switchover, as described in the “Performing a Manual Switchover” section on page 3-95.

Step 6 Shut down the Cisco PGW 2200 Softswitch software on your newly standby Cisco PGW 2200 Softswitch, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

Step 7 Restart the Cisco PGW 2200 Softswitch software on your newly standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.
If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 8.

**Step 8**
Replace the component identified in the alarm text. Procedures for replacing Cisco PGW 2200 Softswitch hardware can be found in the associated Sun Microsystems documentation. Procedures for replacing Cisco ITP-L hardware can be found in “Replacing a Cisco ITP-L” section on page 6-6.

Procedures for replacing Cisco switch can be found in the documentation for your switch.

**Step 9**
Contact the Cisco TAC to further analyze the problem and “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**FailoverPeerLost**

This alarm occurs when the failover daemon on the standby Cisco PGW 2200 Softswitch is not reachable.

**Corrective Action**

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

**Step 1**
Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**
Verify that the Ethernet interfaces between the active and standby Cisco PGW 2200 Softswitches and the Cisco switches are working properly.

*Note*  Information on verifying the proper operation of an Ethernet interface on the Cisco PGW 2200 Softswitch 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 switches can be found in the documentation for your switch.

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 PGW 2200 Softswitch 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 switch can be found in the documentation for your switch.

**Step 3**
Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**FailoverPeerOOS**

This alarm occurs when the failover daemon goes out-of-service in the standby Cisco PGW 2200 Softswitch.
Corrective Action

To correct the problem identified by this alarm, check the alarms on the standby Cisco PGW 2200 Softswitch, using the procedure in the “Retrieving All Active Alarms” section on page 8-3, and resolve those alarms.

FAIL REMOTE STANDBY

This alarm occurs on the active Cisco PGW 2200 Softswitch when a synchronization operation between the active and standby Cisco PGW 2200 Softswitches fails. This alarm is automatically cleared if a successful synchronization operation occurs after the failure. As a result, the Standby Warm Start alarm is triggered. See the “Standby Warm Start” section on page 8-70 for more information.

Corrective Action

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

Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Verify that the standby Cisco PGW 2200 Softswitch is in the standby platform state, using the procedure defined in the “Verifying the Platform State of the Cisco PGW 2200 Softswitches” section on page 3-2.
If the standby Cisco PGW 2200 Softswitch is in the standby platform state, proceed to Step 3. Otherwise, proceed to Step 4.

Step 3 Synchronize the standby Cisco PGW 2200 Softswitch with the active Cisco PGW 2200 Softswitch by entering the prov-sync MML command.

Step 4 Shut down the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

Step 5 Restart the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.
If that resolves the problem, the procedure is complete. Otherwise, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

FORCE NODE RESTART

This alarm occurs on the standby Cisco PGW 2200 Softswitch when a new SS7 IOCC is added to the configuration of the system. This alarm causes the Cisco PGW 2200 Softswitch software on the standby Cisco PGW 2200 Softswitch to be rebooted. This alarm does not affect the active Cisco PGW 2200 Softswitch.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:
Step 1  Once the Cisco PGW 2200 Softswitch software has restarted on the standby Cisco PGW 2200 Softswitch, collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Verify that the standby Cisco PGW 2200 Softswitch is in the standby platform state, using the procedure defined in the “Verifying the Platform State of the Cisco PGW 2200 Softswitches” section on page 3-2. If the standby Cisco PGW 2200 Softswitch is in the standby platform state, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Search the active system log file, as described in the “Viewing System Logs” section on page 8-83, 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 3.

Step 3  Shut down the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

Step 4  Restart the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

Step 5  Perform a manual switchover, as described in the “Performing a Manual Switchover” section on page 3-95.
Warning

Switchover operations cause the loss of all SS7 messages transmitted to the Cisco PGW 2200 Softswitch for approximately three seconds. This affects unstable in-progress calls as well as new calls. Stable in-progress calls are not affected.

---

**Step 6**
Shut down the Cisco PGW 2200 Softswitch software on your newly standby Cisco PGW 2200 Softswitch, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

**Step 7**
Restart the Cisco PGW 2200 Softswitch software on your newly standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2. If that resolves the problem, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**Holiday Table Access Failure**

This alarm occurs when the Cisco PGW 2200 Softswitch could not access the holiday table.

**Corrective Action**

To correct the problem identified by this alarm, check for the presence of the Holiday Table Load Failure alarm, using the procedure in “Retrieving All Active Alarms” section on page 8-3. If this alarm is present, perform the corrective action for that alarm. Otherwise, the procedure is complete.

**Holiday Table Load Failure**

This alarm occurs when a Cisco PGW 2200 Softswitch process is unable to load the holiday table.

**Corrective Action**

**Step 1**
Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**
Verify whether a holiday table is present on your system by logging in to your active Cisco PGW 2200 Softswitch, starting an MML session, and entering the following command:

```
prov-rtrv:holiday:*all*
```

The system responds with a list of elements in the holiday table, or with an error indicating that a holiday table does not exist.

If a holiday table is not present, provision a holiday table, as described in the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide.

If a holiday table is present, verify that the information returned is correct. If the information is correct, proceed to Step 2. Otherwise, correct the contents of the holiday table, as described in the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide.
Chapter 8 Troubleshooting the Cisco PGW 2200 Softswitch Platform

Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

INVALID M3UA RC

This alarm occurs when an M3UA message is received from the identified Cisco ITP with a routing context that has not been provisioned on the Cisco PGW 2200 Softswitch.

Corrective Action

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

Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Determine the AS definitions on the associated Cisco ITP. See the documentation for your Cisco ITP for more information.

Step 3 Retrieve the settings for the affected M3UA routing keys using the prov-rtrv MML command, as described in the “Retrieving Provisioning Data” section on page 3-68.

Step 4 Identify the AS defined on the Cisco ITP that is not provisioned as a routing context on the Cisco PGW 2200 Softswitch.

Step 5 Open a dynamic reconfiguration session to add the routing context to the M3UA routing keys, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

If this corrects the problem, the procedure is complete. Otherwise, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

INVALID SUA RC

This alarm occurs when there is a mismatch between SUA routing keys defined on the Cisco PGW 2200 Softswitch and the signaling gateway.

Corrective Action

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

Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Determine the AS definitions on the associated Cisco ITP. See the documentation for your Cisco ITP for more information.

Step 3 Retrieve the settings for the affected SUA routing keys using the prov-rtrv MML command, as described in the “Retrieving Provisioning Data” section on page 3-68.

Step 4 Identify the AS defined on the Cisco ITP that is not provisioned as a routing context on the Cisco PGW 2200 Softswitch.
Step 5  Open a dynamic reconfiguration session to add the routing context to the SUA routing keys, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

If this corrects the problem, the procedure is complete. Otherwise, proceed to Step 5.

Step 6  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Invalid Virtual IP.Addr

This alarm occurs when the configured virtual IP address is not part of the networks associated with the IP addresses set for the IP.Addr1 or IP.Addr2 parameters in the XECfgParm.dat file.

Corrective Action

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

Step 1  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Verify that the IP address defined for the XECfgParm.dat parameter, *.Virtual_IP.Addr, is set correctly in the XECfgParm.dat file on each host.

Note  The IP address defined for this parameter should be a part of the networks associated with the IP addresses defined for the XECfgParm.dat parameters IP.Addr1 or IP.Addr2.

If the setting for the parameter is correct, proceed to Step 3. Otherwise, reboot your software using the procedure described in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.

Step 3  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

IP CONNECTION FAILED

This alarm occurs when the Cisco PGW 2200 Softswitch loses network (IP) connectivity to a Cisco ITP-L. This alarm is generated for each SS7 link associated with the affected Cisco ITP-L.

Corrective Action

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

Step 1  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Verify that the affected Cisco ITP-L is up and running by performing the procedures in the “Checking Equipment Status” section on page 6-2.
If the affected Cisco ITP-L is not up and running, start it using the procedure in the “Cisco SS7 Interface Startup Procedure” section on page 2-3. If this does not resolve the problem, replace the affected Cisco ITP-L as described in the “Replacing a Cisco ITP-L” section on page 6-6.

If the affected Cisco ITP-L is up and running, proceed to Step 3.

**Step 3**

Verify that the Ethernet interfaces between the Cisco PGW 2200 Softswitch and the affected Cisco ITP-L are working properly.

*Note*

Information on verifying the proper operation of an Ethernet interface on the Cisco PGW 2200 Softswitch 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 ITP-L 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 4.

*Note*

Information on removing and replacing an Ethernet interface card on the Cisco PGW 2200 Softswitch can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing components on the Cisco ITP-L can be found in the “Replacing Hardware Components” section on page 6-15.

**Step 4**

Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**IP RTE CONF FAIL**

This alarm occurs when an IP route cannot access the local interface defined by its IP address parameter.

**Corrective Action**

Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87 and contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**IP RTE FAIL**

This alarm occurs when an IP route is in the OOS state with a cause other than off-duty or commanded out-of-service.

**Corrective Action**

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

**Step 1**

Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  Verify the IP addresses of the local interfaces on the standby Cisco PGW 2200 Softswitch using the following UNIX command:

```
ifconfig -a
```

The system returns a response indicating the IP addresses of your local interfaces.

Step 3  Verify that the IP addresses obtained in Step 2 match the values set for the IP_Addr1 through IP_Addr4 parameters in the XECfgParm.dat file.

If the settings for the local IP addresses are not the same, proceed to Step 4.

If the settings for the local IP addresses are the same, proceed to Step 12.

Step 4  Log in to your active Cisco PGW 2200 Softswitch and change directories to the /opt/CiscoMGC/etc directory using the following UNIX command:

```
cd /opt/CiscoMGC/etc
```

Step 5  Open the XECfgParm.dat file in a text editor, such as vi.

Step 6  Search for the IP_Addr properties and change those that are not configured correctly.

Step 7  Save the file and exit the text editor.

Step 8  Shut down the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch by entering the following UNIX command:

```
/etc/init.d/CiscoMGC stop
```

**Note**  Shutting down the Cisco PGW 2200 Softswitch software on the active Cisco PGW 2200 Softswitch causes the currently standby Cisco PGW 2200 Softswitch to become the active Cisco PGW 2200 Softswitch.

Step 9  Restart the Cisco PGW 2200 Softswitch software on this Cisco PGW 2200 Softswitch by entering the following command:

```
/etc/init.d/CiscoMGC start
```

Step 10  Once the Cisco PGW 2200 Softswitch software is fully activated, log in to the active Cisco PGW 2200 Softswitch and perform a manual switchover, using the following MML command:

```
sw-over::confirm
```

Step 11  Repeat steps 2 through 9 on the newly standby Cisco PGW 2200 Softswitch.

If the problem has not been resolved after you have completed those steps, proceed to Step 12.

Step 12  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**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 8-144.

License server unreachable

This alarm appears if the license server is unavailable. The Cisco PGW 2200 Softswitch looks at the local license files to retrieve the configuration time TDM ports/runtimetype license information. At the same time, a timer is started.

If the license server is still unreachable after 1 week, the license number will be half of the license number in license files.

If the license server is still unreachable after 8 weeks, the license number will be the number of demo licenses.

Corrective Action

If you see the license server unreachable alarm, you can use the rtrv-lics output to determine how many days license server has been unreachable.

Follow these steps to resolve this problem.

Step 1

Go to the machine where the license server is running (see the first line of the license file for the server hostname).

Step 2

Enter ps -ef |grep lmgrd to see whether the license server daemon is running.

a. If the license server is not running, enter /opt/CiscoMGC/local/reload_lics.sh to restart the license server.

b. If the license server still fails to start, check the /opt/CiscoMGC/var/log/flexlm_server.log for detailed information or contact Cisco TAC.

c. If the license server is running, but the active Cisco PGW 2200 Softswitch is running on a separate machine, ensure that the Cisco PGW 2200 Softswitch machine can reach the IP address of the license server machine.

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 a local Ethernet interface has failed.
Corrective Action

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

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Use the Log viewer in the MGC Viewer toolkit to search the system log file from the same time period as this alarm for a GEN_ERR_IPINTF_FAIL log message.

**Note** For more information on using the Log viewer, see the Cisco PGW 2200 Softswitch Release 9 Operations, Maintenance, and Troubleshooting Guide.

If a GEN_ERR_IPINTF_FAIL log message is found, proceed to Step 3. Otherwise, proceed to Step 7.

**Step 3** Identify the cause of the failure from the information in the log message.

If the cause in the log message is “Admin Down”, the interface was taken down using an administrative command. Proceed to Step 4.

If the cause in the log message is “Link Down”, the Ethernet path has failed. Proceed to Step 5.

**Step 4** Enter the following UNIX command to restore the link to service:

```
ifconfig interface up
```

Where `interface` is the IP address of the affected interface.

If the interface is restored and is working fine, the procedure is complete. Otherwise, proceed to Step 7.

**Step 5** Verify that the cable connected between the interface and the associated Ethernet switch is working properly.

If the cable is working correctly, proceed to Step 6.

If the cable is not working correctly, replace it. If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 6.

**Step 6** Verify that the associated Ethernet switch is working properly.

If the Ethernet switch is working correctly, proceed to Step 7.

If the Ethernet switch is not working correctly, trouble shoot the problem as indicated in the documentation for your switch. 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**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** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** 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 3. If the alarm does not clear, proceed to Step 3.

**Step 3** Change the line build-out setting. If the alarm does not clear, proceed to Step 4.

**Step 4** 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 5. Once you have isolated the problem, resolve as necessary. If the alarm does not clear, proceed to Step 5.

**Step 5** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**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** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** 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 3.

**Step 3** 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 3.

**Step 4** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.
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 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2 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 3.
Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2 Connect an external loopback cable to the affected port.
   If no alarms are produced, proceed to Step 3.
   If alarms are produced, the port is causing the error. Replace the hardware component associated with the port. See the associated media gateway documentation for more information on replacing the component.
Step 3 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 4.
   If you do not find a wiring problem, then proceed to Step 4.
Step 4 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 5.
Step 5  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

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  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  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 3.

If you do not find a problem with the V.35 cables, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

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  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  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 3.

If you do not find a problem with the V.35 cables, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.
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 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 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 3.
   If you do not find a problem with the V.35 cables, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

M3UAKEY Ack Pending

This alarm occurs when the Cisco PGW 2200 Softswitch cannot send or receive traffic for the identified SS7 signaling service via the Cisco ITP that has not acknowledged the M3UAKEY.

Corrective Action

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

Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Determine the AS definitions on the associated Cisco ITP. See the documentation for your Cisco ITP for more information.

Step 3 Retrieve the settings for the affected M3UA routing keys using the prov-rtrv MML command, as described in the “Retrieving Provisioning Data” section on page 3-68.

Step 4 The AS definitions should match the routing contexts of the M3UA routing keys. If they match, proceed to Step 6. Otherwise, proceed to Step 5.

Step 5 Open a dynamic reconfiguration session to modify the routing contexts of the M3UA routing keys, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.
   If this corrects the problem, the procedure is complete. Otherwise, proceed to Step 6.

Step 6 Verify that the AS is not shutdown on the Cisco ITP. See the documentation for your Cisco ITP for more information. If the AS is shutdown, restart it. Otherwise, proceed to Step 7.
   If this corrects 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.
MeterPulseTariff Table Load Failure

This alarm occurs when the Cisco PGW 2200 Softswitch failed to load the meter pulse tariff table.

Corrective Action

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Verify whether a tariff table is present on your system by logging in to your active Cisco PGW 2200 Softswitch, starting an MML session, and entering the following command:

```
prov-rtrv:metertariff:*all*
```

The system responds with a list of elements in the meter pulse tariff table, or with an error indicating that the meter pulse tariff table does not exist.

If the meter pulse tariff table is not present, provision a meter pulse tariff table, as described in the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide.

If a meter pulse tariff table is present, verify that the information returned is correct. If the information is correct, proceed to Step 3. Otherwise, correct the contents of the meter pulse tariff table, as described in the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide.

**Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 PGW 2200 Softswitch, as described in the “Deleting Unnecessary Files to Increase Available Disk Space” section on page 8-165.

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 PGW 2200 Softswitch, as described in the “Deleting Unnecessary Files to Increase Available Disk Space” section on page 8-165.
**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 PGW 2200 Softswitch, as described in the “Deleting Unnecessary Files to Increase Available Disk Space” section on page 8-165.

**NAS: AuditResponse Failure**

This alarm occurs when the identified media gateway fails to send a RESYNC RESP message back to the Cisco PGW 2200 Softswitch within the audit time interval.

**Corrective Action**

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</td>
</tr>
</tbody>
</table>
| **Step 2** | Verify that the affected media gateway is in the in-service state, as described in the “Verifying the Status of all Signaling Services” section on page 3-9.  
If the affected media gateway is in-service, proceed to Step 3. Otherwise, proceed to Step 4. |
| **Step 3** | Verify that the configuration of the affected media gateway is correct. See the documentation for the media gateway for more information.  
If that does not resolve the problem, proceed to Step 4. |
| **Step 4** | Verify that the Ethernet interfaces between the Cisco PGW 2200 Softswitch and the associated media gateway are working properly. |

**Note**

Information on verifying the proper operation of an Ethernet interface on the Cisco PGW 2200 Softswitch 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 5.

**Note**

Information on removing and replacing an Ethernet interface card on the Cisco PGW 2200 Softswitch 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 5** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.
NAS: CommsFailure

This alarm occurs when the Cisco PGW 2200 Softswitch cannot communicate with the identified media gateway.

Corrective Action

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

- **Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

- **Step 2** Determine whether the affected media gateway is up and running. See the documentation for the media gateway for more information.
  - If the affected media gateway is not up and running, restore it to service. See the documentation for the media gateway for more information.
  - If the affected media gateway is up and running, proceed to Step 3.

- **Step 3** Verify that the IP configuration parameters for the Cisco PGW 2200 Softswitch and the affected media gateway are correct.

  Note: Use the `prov-rtrv` MML command, as described in the “Retrieving Provisioning Data” section on page 3-68, to retrieve the IP configuration information for the Cisco PGW 2200 Softswitch. See the documentation for the media gateway for information on retrieving the IP configuration data.

  If the configuration of your Cisco PGW 2200 Softswitch is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

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

  If the configuration of both the Cisco PGW 2200 Softswitch and the affected media gateway are correct, then proceed to Step 3.

- **Step 4** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 8-144.
OLC: Leg1chanSeizedUnpackError

This alarm occurs when an Seized Channel (CRCX) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.</td>
</tr>
</tbody>
</table>

OLC: Leg1chanModifiedUnpackError

This alarm occurs when an Modify Channel (MDCX) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.</td>
</tr>
</tbody>
</table>

OLC: Leg1chanDeletedUnpackError

This alarm occurs when a Delete Channel (DLCX) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.</td>
</tr>
</tbody>
</table>
Step 3  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**OLC: Leg1notifyUnpackError**

This alarm occurs when a Notify (NTFY) message received from the media gateway could not be unpacked.

**Corrective Action**

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

- **Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
- **Step 2** Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
- **Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**OLC: Leg1deleteChanUnpackError**

This alarm occurs when a Delete Channel (DLCX) message received from the media gateway could not be unpacked.

**Corrective Action**

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

- **Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
- **Step 2** Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
- **Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**OLC: Leg1notifyRequestAckUnpackError**

This alarm occurs when an Request Notify (RQNT) acknowledge message received from the media gateway could not be unpacked.

**Corrective Action**

To correct the problem identified by this alarm, perform the following steps:
Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

Step 1  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
Step 3  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

OLC: Leg1chanOpsFailed

This alarm occurs when the Cisco PGW 2200 Softswitch has detected an internal error or a media gateway related problem.

Corrective Action

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

Step 1  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
Step 3  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

OOS TRAFFIC RE-ROUTE

This alarm occurs when the traffic channels (bearer channels, IP network) on one side of the Cisco PGW 2200 Softswitch have been lost, causing the Cisco PGW 2200 Softswitch 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  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  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 3.
Step 3  Verify that the traffic channel provisioning settings for the Cisco PGW 2200 Softswitch and the affected media gateway are correct.

Note  Use the prov-rtrv MML command, as described in the “Retrieving Provisioning Data” section on page 3-68, to retrieve the traffic channel provisioning data for the Cisco PGW 2200 Softswitch. See the documentation for the media gateway for information on retrieving the traffic channel data.
If the configuration of your Cisco PGW 2200 Softswitch is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

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

If the configuration of both the Cisco PGW 2200 Softswitch and the affected media gateway 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**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, see the “Managing Automatic Congestion Control” section on page 3-76.

**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 8-90, and re-route some of your traffic to other Cisco PGW 2200 Softswitches.

**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, see the “Provisioning your Cisco PGW 2200 Softswitch” section on page 3-64.

---

**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, see the “Managing Automatic Congestion Control” section on page 3-76.

**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 8-90, and re-route some of your traffic to other Cisco PGW 2200 Softswitches.
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, see the “Provisioning your Cisco PGW 2200 Softswitch” section on page 3-64.

**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, see the “Managing Automatic Congestion Control” section on page 3-76.

**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 8-90, and re-route some of your traffic to other Cisco PGW 2200 Softswitches.

**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, see the “Provisioning your Cisco PGW 2200 Softswitch” section on page 3-64.

**OverResIncomingThreshold**

This alarm occurs when the percentage of idle CICs in a trunk group is less than or equal to the configured threshold.

**Corrective Action**

This alarm may occur occasionally during periods of congestion. However, if this alarm occurs repeatedly, you may need to adjust the value of the parameter that controls the percentage of idle CICs for the affected trunk group. To do this, perform the following steps:

**Step 1**

Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**

Retrieve the current settings for the affected trunk group using the following MML command:

```
prov-rtrv:rttrnkgrp:name="trnkgrp_name"
```

Where `trnkgrp_name` is the name of the affected trunk group.

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 2002-09-20 15:38:02.892 EST
M RTRV
"session=NOA_SPAIN:rttrnkgrp"
/*

<table>
<thead>
<tr>
<th>name</th>
<th>type</th>
<th>reattempts</th>
<th>queuing</th>
<th>cutThrough</th>
<th>resIncomingPerc</th>
</tr>
</thead>
<tbody>
<tr>
<td>111</td>
<td>1</td>
<td>2</td>
<td>120</td>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>
```
Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

The parameter, ResIncomingPerc, controls the percentage of idle CICs for the trunk group. In the above example the value is 0.

Step 3 Start a provisioning session, as described in the “Starting a Provisioning Session” section on page 3-64.

Step 4 Use the prov-ed MML command to modify the setting of the resIncomingPerc parameter. For example, to change the percentage of idle CICs to 30 percent in a trunk group called 1000, you would enter the following command:

prov-ed:rttrnkgrp:name="1000", resIncomingPerc="30"

Note The new value for resIncomingPerc takes effect after your provisioning session is activated. Once the new value is activated, the OverResIncomingThreshold alarm is set or cleared after an outgoing call routed is over the affected trunk group.

Step 5 Save and activate your provisioning session, as described in the “Saving and Activating your Provisioning Changes” section on page 3-65.

If the alarm clears, the procedure is complete. Otherwise, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 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 3.

Step 3 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 3-68.

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 3-66.

If the configuration data associated with the DPC is 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.
Peer IP Links Failure

This alarm occurs when the IP links to the peer Cisco PGW 2200 Softswitch are removed or down.

Corrective Action

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

1. Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
2. Verify that the Ethernet interfaces for the active and standby Cisco PGW 2200 Softswitches are working properly.

   Note Information on verifying the proper operation of an Ethernet interface on the Cisco PGW 2200 Softswitch 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 3.

   Note Information on removing and replacing an Ethernet interface card on the Cisco PGW 2200 Softswitch can be found in the Sun Microsystems documentation that came with your system.

3. Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 8-177.

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 8-177.
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

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 8-177.

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 3-65. For more information about provisioning your Cisco PGW 2200 Softswitch, see the Cisco PGW 2200 Softswitch Release 9.8 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 3-64, 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. See the “Invoking Dynamic Reconfiguration” section on page 3-66 for more information.

Corrective Action

If necessary, you can complete the dynamic reconfiguration procedure, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

POM: PEER_SYNC_ERR

This alarm occurs when the standby Cisco PGW 2200 Softswitch attempts to synchronize the contents of its configuration library while a provisioning session is in progress on the active Cisco PGW 2200 Softswitch.
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 3-66, or save and activate your changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65.

PRI: B-Channel not available

This alarm occurs when the Cisco PGW 2200 Softswitch 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 save and activate your provisioning session, as described in the “Saving and Activating your Provisioning Changes” section on page 3-65.

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 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2 Stop the Cisco PGW 2200 Softswitch software on the standby Cisco PGW 2200 Softswitch, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.
Step 3 Restart the Cisco PGW 2200 Softswitch software on the standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.
Step 4 Perform a manual switchover, as described in the “Performing a Manual Switchover” section on page 3-95.

Warning Switchover operations cause the loss of all SS7 messages transmitted to the Cisco PGW 2200 Softswitch for approximately three seconds. This affects unstable in-progress calls as well as new calls. Stable in-progress calls are not affected.

Step 5 Stop the Cisco PGW 2200 Softswitch software on the newly standby Cisco PGW 2200 Softswitch, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.
Step 6 Restart the Cisco PGW 2200 Softswitch software on the newly standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

If this does not resolve the problem, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.
ProtocolFileMissing

This alarm occurs when the protocol file(s) associated with your system configuration have not been installed.

Corrective Action

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

Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2 Search the active system log file, as described in the “Viewing System Logs” section on page 8-83, for logs that indicate that a *.mdo or *.so file cannot be found.
   If there are logs that indicate that a *.mdo or *.so file cannot be found, proceed to Step 3.
   If there are no logs that indicate that an IPC file cannot be opened, proceed to Step 5.
Step 3 Determine which protocol patch contains the missing file. To do this, consult the Release Notes for your particular release of the Cisco PGW 2200 Softswitch software.
Step 4 Once you have determined the protocol patch that contains your missing file(s), go to the following URL to download this patch for your version of the Cisco PGW 2200 Softswitch software:
Step 5 Install the patch as instructed in its associated text file.
Step 6 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

REPL: all connections failure

This alarm occurs when the Cisco PGW 2200 Softswitch cannot establish communication to the peer Cisco PGW 2200 Softswitch.

Corrective Action

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

Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2 Verify that the Ethernet interfaces for the Cisco PGW 2200 Softswitch are working properly.
   Note Information on verifying the proper operation of an Ethernet interface on the Cisco PGW 2200 Softswitch 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 3.
   Note Information on removing and replacing an Ethernet interface card on the Cisco PGW 2200 Softswitch can be found in the Sun Microsystems documentation that came with your system.
Step 3  Verify the replicator configuration on the Cisco PGW 2200 Softswitches, as described in the “Restoring a Backup File from a Device” section on page 8-174.
If that does not resolve 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  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 3-68.
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 3-66.
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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  Place the affected signaling channel in the out-of-service state.
Step 3  Start a provisioning session, as described in the “Starting a Provisioning Session” section on page 3-64.
Step 4  Remove the affected signaling channel from your configuration using the prov-dlt MML command. See the Cisco PGW 2200 Softswitch Release 9 MML Command Reference for more information.
Step 5 Referring to your local provisioning parameters, re-provision the signaling channel using the prov-add MML command. See the Cisco PGW 2200 Softswitch Release 9 MML Command Reference for more information.

Step 6 Save and activate your provisioning session, as described in the “Saving and Activating your Provisioning Changes” section on page 3-65.

Step 7 Place the signaling channel in the in-service state.

If that does not resolve the problem, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

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 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 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 3.

Step 3 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 3-68.

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 3-66.

If the configuration data for the signaling channel is 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

SC M-OOS

This alarm occurs when a signaling channel has been manually taken out of service.
Corrective Action

To correct the problem identified by this alarm, restore the affected signaling channel to the in-service state, using the appropriate procedure. Procedure for modifying the state of signaling channels are described in the “Setting the Service State of a C7/SS7 Link or Linkset” section on page 8-98, the “Setting the Service State of an IP Link” section on page 8-98, and the “Setting the Service State of a D-channel” section on page 8-100.

SIP: DNS CACHE NEARLY FULL

This alarm occurs when the domain name service (DNS) cache is nearly full.

Corrective Action

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

Step 1: Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2: Retrieve the current DNS properties by logging in to the active Cisco PGW 2200 Softswitch, starting an MML session, and entering the following command:

`prov-rtrv:dnsparam:`

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 1999-12-30 14:27:48
M RTRV
"session=test:dnsparam"
/*
*DnsCacheSize = 500
*DnsKeepAlive = 30
*DnsPolicy = HIERARCHY
*DnsQueryTimeout = 1000
*DnsServer1 = 172.22.1.1
*DnsServer2 = 143.83.1.1
*DnsTTL = 3600
*/
```

Make note of the value of the *DnsCacheSize parameter.

Step 3: Begin a dynamic reconfiguration session to increase the value of the *DnsCacheSize parameter, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

If this alarm occurs repeatedly despite increasing the size of the cache, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

SIP: DNS SERVICE OOS

This alarm occurs when the DNS servers are not responding to queries. The DNS servers may be out of service or the access to them is lost.
Corrective Action

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

---

**Step 1**
Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**
Retrieve the current DNS properties by logging in to the active Cisco PGW 2200 Softswitch, starting an MML session, and entering the following command:

```
prov-rtrv:dnsparam:*all*
```

The system returns a response similar to the following:

```
MGC-01 - Media Gateway Controller 1999-12-30 14:27:48
M  RTRV
"session=test:dnsparam"

/*
*.DnsCacheSize = 500
*.DnsKeepAlive = 30
*.DnsPolicy = HIERARCHY
*.DnsQueryTimeout = 1000
*.DnsServer1 = 172.22.1.1
*.DnsServer2 = 143.83.1.1
*DnsTTL = 3600
*/
```

Make note of the value of the *.DnsServer1 and *.DnsServer2 parameters.

**Step 3**
Begin a dynamic reconfiguration session to select new DNS servers for your system, entering their IP addresses in the *.DnsServer1 and *.DnsServer2 parameters, using the procedure described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

If this alarm occurs repeatedly despite selecting new DNS servers, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**SIP: OOS**

This alarm occurs when an IP link used by the SIP is out of service.

Corrective Action

To correct the problem identified by this alarm, attempt to restore the IP link to service using the procedure described in the “Setting the Service State of an IP Link” section on page 8-98.

**SIP Service Fail Over**

This alarm is caused by the failure of switch interfaces, due to either physical failure or administrative shut down.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:
Step 1  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Determine whether the failure is caused by a physical failure or an administrative shutdown.

If the failure is caused by a physical failure, proceed to Step 2.

If the failure is caused by an administrative shutdown, check for this alarm again once the interface has been restored. If this alarm is still active, proceed to Step 3.

Step 3  Verify that the switch interfaces between the Cisco PGW 2200 Softswitch and the affected SIP element are working properly.

Note  Information on verifying the proper operation of a switch interface on the Cisco PGW 2200 Softswitch can be found in the Sun Microsystems documentation that came with your system. Information on verifying the proper functioning of a switch interface on other devices can be found in the user documentation that came with that device.

If an element of the switch 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 PGW 2200 Softswitch can be found in the Sun Microsystems documentation that came with your system. Information on removing and replacing components on other devices can be found in the user documentation that came with that device.

Step 4  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Standby Warm Start

This alarm occurs on the active Cisco PGW 2200 Softswitch when a synchronization operation between the active and standby Cisco PGW 2200 Softswitches begins. This alarm clears automatically when the synchronization operation is completed. This alarm also occurs on the standby Cisco PGW 2200 Softswitch when the prov-sync MML command is entered on the active Cisco PGW 2200 Softswitch. In that case, the alarm clears automatically when the synchronization of provisioning data is complete. If a synchronization operation should fail, this alarm is automatically cleared and a FAIL REMOTE STANDBY alarm is generated. See the “FAIL REMOTE STANDBY” section on page 8-40 for more information.

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 8-178.
**SS7 RTE KEY FAIL**

This alarm occurs when one or more routing keys for an SS7 signaling service associated with an SG has failed; the signaling service cannot receive some ISUP messages. The maximum number of routing keys supported by the associated SG might have been exceeded.

**Corrective Action**

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

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Ensure that the provisioning settings for the bearer channels associated with this SG are correct, using the procedure described in the “Retrieving Provisioning Data” section on page 3-68.

If the configuration data associated with the bearer channels is incorrect, begin a dynamic reconfiguration session, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

If this clears the alarm, the procedure is complete. Otherwise, proceed to Step 3.

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

**Step 3** Determine the maximum number of dynamic routing keys that are allowed on the associated SG.

**Step 4** Determine how many routing keys are being used by the Cisco PGW 2200 Softswitch by adding the number of CICs associated with the SS7 signaling service(s) (ss7sgpath).

For example, if 990 CICs and 10 SS7 subsystems were associated with the SG, then 1000 routing keys would be in use by the Cisco PGW 2200 Softswitch.

**Step 5** Compare the maximum number of routing keys allowed to the number of routing keys being used. If the number of routing keys being used is greater, proceed to Step 6. Otherwise, proceed to Step 7.

**Step 6** Begin a dynamic reconfiguration session to delete the excess routing keys by removing either CICs or SS7 subsystems from your configuration, using the procedure described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

If this clears the alarm, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**SS7 SIG SRVC CONFIG FAIL**

This alarm occurs when the identified SS7 signaling service associated with an SG is not configured correctly.

**Corrective Action**

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

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Retrieve the current DNS properties by logging in to the active Cisco PGW 2200 Softswitch, starting an MML session, and entering the following command:

```bash
prov-rtrv:SS7SGPath:name="sig_srv"
```
Where *sig_serv* is the MML name of the identified SS7 signaling service.

The system returns a response that lists all of the properties associated with the selected SS7 signaling service.

**Step 3** Verify that the information displayed for the SS7 signaling service is correct.
If it is correct, proceed to Step 5. Otherwise, proceed to Step 4.

**Step 4** Begin a dynamic reconfiguration session to correct the settings for the SS7 signaling service, using the procedure described in the “Invoking Dynamic Reconfiguration” section on page 3-66.
If this clears the alarm, the procedure is complete. Otherwise, proceed to Step 5.

**Step 5** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**SS7 SIG SRVC UNAVAIL**

The identified SS7 signaling service is unavailable.

**Corrective Action**

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

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Perform the MML command `rtrv-dest` on the SS7PATH or SS7SUBSYS object.
If the state is OOS,FLD, the signaling service is out of service due to failure of the MTP3 transport. Perform a `prov-rtrv:SS7PATH` or a `prov-rtrv:SS7SUBSYS` on the signaling service object.

a. If the object has an OPC attribute defined, the signaling service is using Cisco ITP-Ls for SS7 communication. The MTP3 layer is on the Cisco PGW 2200 Softswitch. The SS7ROUTEs and LINKSETs need to be examined to determine the cause of the failure.

b. If the object doesn't have an OPC attribute defined, the signaling service is using ITPs for SS7 communication. The MTP3 layer is one the ITPs. Examine the M3UAROUTEs that have the same OPC and DPC as SS7PATH or the SUAROUTEs that have the same OPC, APC, and REMOTE SSN to determine which ITP EXTNODEs are being used by the signaling service. Consult the ITP documentation and debug the problem on the ITPs.

If the state is OOS,FLD&UPU, the signaling service is out of service due to failure of the user part layer at the destination. This remote destination should be examined to determine the cause of the failure.

**Step 3** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**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** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** 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 3-68.

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 3-66.

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

**Step 3** 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 3-66, 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 4.

**Step 4** Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**SUAKEY Ack Pending**

This alarm occurs when the Cisco PGW 2200 Softswitch cannot send or receive traffic for the identified SS7 subsystem via the Cisco ITP that has not acknowledged the SUAKEY.

Corrective Action

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

---

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Determine the AS definitions on the associated Cisco ITP. See the documentation for your Cisco ITP for more information.

**Step 3** Retrieve the settings for the affected SUA routing keys using the `prov-rtrv` MML command, as described in the “Retrieving Provisioning Data” section on page 3-68.

**Step 4** The AS definitions should match the routing contexts of the SUA routing keys. If they match, proceed to Step 6. Otherwise, proceed to Step 5.

**Step 5** Open a dynamic reconfiguration session to modify the routing contexts of the M3UA routing keys, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

If this corrects the problem, the procedure is complete. Otherwise, proceed to Step 6.

**Step 6** Verify that the AS is not shutdown on the Cisco ITP. See the documentation for your Cisco ITP for more information. If the AS is shutdown, restart it. Otherwise, proceed to Step 7.

If this corrects 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  Check for other alarms, as described in the “Retrieving All Active Alarms” section on page 8-3, that further identify the failed entity.
Step 3  Once you have identified the failed entity, replace it and restore it to service. If the entity is hardware, see 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 4.
Step 4  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

SwitchoverFail

This alarm occurs when a switchover operation from the active Cisco PGW 2200 Softswitch to the standby Cisco PGW 2200 Softswitch 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 8-166.

Tariff Table Access Failure

This alarm occurs when the Cisco PGW 2200 Softswitch could not access the tariff table.

Corrective Action

To correct the problem identified by this alarm, check for the presence of the Tariff Table Load Failure alarm, using the procedure in “Retrieving All Active Alarms” section on page 8-3. If this alarm is present, perform the corrective action for that alarm. Otherwise, the procedure is complete.
Tariff Table Load Failure

This alarm occurs when a Cisco PGW 2200 Softswitch process is unable to load the tariff table.

Corrective Action

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Verify whether a tariff table is present on your system by logging in to your active Cisco PGW 2200 Softswitch, starting an MML session, and entering the following command: prov-rtrv:tariff:<em>all</em></td>
</tr>
</tbody>
</table>

The system responds with a list of elements in the tariff table, or with an error indicating that a tariff table does not exist.

If a tariff table is not present, provision a tariff table, as described in the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide.

If a tariff table is present, verify that the information returned is correct. If the information is correct, proceed to Step 3. Otherwise, correct the contents of the tariff table, as described in the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide.

| Step 3 | Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx. |

TLC: Leg2chanSeizedUnpackError

This alarm occurs when a Seize Channel (CRCX) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.</td>
</tr>
</tbody>
</table>

TLC: Leg2chanModifiedUnpackError

This alarm occurs when a Modify Channel (MDCX) acknowledge message received from the media gateway could not be unpacked.

Corrective Action

To correct the problem identified by this alarm, perform the following steps:
Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Troubleshooting Using Cisco PGW 2200 Softswitch Alarms

Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2 Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**TLC: Leg2chanDeletedUnpackError**

This alarm occurs when a Delete Channel (DLCX) acknowledge message received from the media gateway could not be unpacked.

**Corrective Action**

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

Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2 Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**TLC: Leg2notifyUnpackError**

This alarm occurs when a Notify (NTFY) message received from the media gateway could not be unpacked.

**Corrective Action**

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

Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2 Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

**TLC: Leg2deleteChanUnpackError**

This alarm occurs when a Delete Channel (DLCX) message received from the media gateway could not be unpacked.

**Corrective Action**

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

Step 1 Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2 Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.
Step 3 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.
**Corrective Action**

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.</td>
</tr>
</tbody>
</table>

**TLC: Leg2notifyRequestAckUnpackError**

This alarm occurs when an Request Notify (RQNT) acknowledge message received from the media gateway could not be unpacked.

**Corrective Action**

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.</td>
</tr>
</tbody>
</table>

**TLC: Leg2chanOpFailed**

This alarm occurs when the Cisco PGW 2200 Softswitch has detected an internal error or a media gateway related problem.

**Corrective Action**

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.</td>
</tr>
</tbody>
</table>

**UCM: CCodeModfailed**

This alarm occurs when the country code prefix could not be applied or removed.
Corrective Action

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

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Determine whether the country code prefix could not be applied or removed by viewing the active system log file, using the procedure described in the “Viewing System Logs” section on page 8-83. There should be a log present that uses the same text as the alarm. That log indicates whether the country code prefix could not be applied or removed and lists the affected B-number.

**Step 3** Determine whether country code prefix application or removal should be performed for the affected B-number.
- If country code prefix processing should not be performed, proceed to Step 4.
- If country code prefix processing should be performed, proceed to Step 8.

**Step 4** Verify whether the result set associated with the affected B-number has a result type of CC_DIG configured, using the **numan-rtrv** MML command. For example:

```
numan-rtrv:.resulttable:custgrpid=T002
```

If the result set does have a result type of CC_DIG configured, use the **numan-dlt** MML command to remove the CC_DIG result set. For example:

```
numan-dlt:.resulttable:custgrpid="T002", name="result46", resulttype="CC_DIG"
```

Otherwise, proceed to Step 5.

**Step 5** Verify that the BDigitCCPrefix property for the associated trunk group is set to 0 (disabled) using the **prov-rtrv** MML command. For example:

```
prov-rtrv:trnkgrpprop:name="trnkgrp1"
```

If the BDigitCCPrefix property in the associated trunk group is not set to 0, use the **prov-ed** MML command to modify the value of the property. For example:

```
prov-ed:trnkgrp:name="trnkgrp1", BDigitCCPrefix=0
```

Otherwise, proceed to Step 6.

**Step 6** Verify that the BDigitCCrm property for the associated trunk group is set to NULL (disabled) using the **prov-rtrv** MML command. For example:

```
prov-rtrv:trnkgrpprop:name="trnkgrp1"
```

If the BDigitCCrm property in the associated trunk group is not set to NULL, use the **prov-ed** MML command to modify the value of the property. For example:

```
prov-ed:trnkgrp:name="trnkgrp1", BDigitCCrm=null
```

Otherwise, proceed to Step 7.

**Step 7** Verify that the associated B-number analysis configuration does not allow for country code digit removal using the **numan-rtrv** MML command. For example:

```
numan-rtrv:digmodstring:custgrpid="T002"
```

If the associated B-number analysis configuration allows country code digit removal, use the **numan-dlt** MML command to remove the digit string. For example:

```
numan-dlt:digmodstring:custgrpid="T002", name="ccspain"
```

Otherwise, proceed to Step 13.
Step 8 Select a step based on the country code prefix information found in the log identified in Step 2. If the log indicates that the country code prefix could not be applied, proceed to Step 9. If the log indicates that the country code prefix could not be removed, proceed to Step 11.

Step 9 Verify whether the result set associated with the affected B-number has a result type of CC_DIG configured, using the `numan-rtrv` MML command. If the result set does not have a result type of CC_DIG configured, use the `numan-ed` MML command to add the CC_DIG result set. For example:

```
numan-ed:resulstable:custgrpid="T002", name="result46", resulttype="CC_DIG", dw1=ccspain, setname="setname1"
```

Otherwise, proceed to Step 10.

Step 10 Verify that the BDigitCCPrefix property for the associated trunk group is set to 1 (enabled) using the `prov-rtrv` MML command. For example:

```
prov-rtrv:trnkgrpprop:name="trnkgrp1"
```

If the BDigitCCPrefix property in the associated trunk group is not set to 1, use the `prov-ed` MML command to modify the value of the property. For example:

```
prov-ed:trnkgrp:name="trnkgrp1", BDigitCCPrefix=1
```

Otherwise, proceed to Step 13.

Step 11 Verify that the BDigitCCrm property for the associated trunk group is set to the correct number string using the `prov-rtrv` MML command. For example:

```
prov-rtrv:trnkgrpprop:name="trnkgrp1"
```

If the BDigitCCrm property in the associated trunk group is not set to the correct number string, use the `prov-ed` MML command to modify the value of the property. For example:

```
prov-ed:trnkgrp:name="trnkgrp1", BDigitCCrm=34
```

Otherwise, proceed to Step 12.

Step 12 Verify that the associated B-number analysis configuration allows for country code digit removal using the `numan-rtrv` MML command. For example:

```
uman-rtrv:digmodstring:custgrpid="T002"
```

If the associated B-number analysis configuration does not allow for country code digit removal, use the `numan-ed` MML command to modify the setting. For example:

```
numan-ed:digmodstring:custgrpid="T002", name="ccspain", digstring="34"
```

Otherwise, proceed to Step 13.

Step 13 Verify that the dial plan file was loaded correctly, using the procedure described in “Verifying Proper Loading of a Dial Plan” section on page 8-114. If that procedure resolves the problem, the procedure is finished. Otherwise, proceed to Step 13.

Step 14 Perform a call trace, as described in “Performing a Call Trace” section on page 8-151.

Step 15 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.
UCM: MGCPDIALAuthFail

This alarm occurs when an MGCP dial call fails after an automatic switchover takes place, due to the expiration of a timer waiting for a Notify message from the associated media gateway.

Note

This alarm is valid as of Release 9.3(1). There is a patch for Release 9.3(2) that retires this alarm.

Corrective Action

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

- **Step 1**: Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
- **Step 2**: Verify the configuration of the associated media gateway. If there are no configuration problems, proceed to Step 2. Otherwise, fix the identified configuration problems.
- **Step 3**: Verify that the IP path between the media gateway and the Cisco PGW 2200 Softswitch is working properly. If you find no problems in the IP path between the media gateway and the Cisco PGW 2200 Softswitch, proceed to Step 4. Otherwise, fix the identified IP path problems.
- **Step 4**: Verify that the IP path between the media gateway and the authentication server is working properly. If you find no problems in the IP path between the media gateway and the authentication server, proceed to Step 5. Otherwise, fix the identified IP path problems.
- **Step 5**: Verify that the authentication server is working properly. If you find no problems in the authentication server, proceed to Step 6. Otherwise, fix the identified problems in the authentication server.
- **Step 6**: Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Virtual_IP_Addr Mismatch

This alarm occurs when the virtual IP addresses configured in XECfgParm.dat files on the active and the standby Cisco PGW 2200 Softswitches do not match.

Corrective Action

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

- **Step 1**: Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
- **Step 2**: Verify the value set for the XECfgParm.dat parameter, *.Virtual_IP_Addr, on the active Cisco PGW 2200 Softswitch.
- **Step 3**: Verify the value set for the XECfgParm.dat parameter, *.Virtual_IP_Addr, on the standby Cisco PGW 2200 Softswitch.
  
  If the parameter values match, proceed to Step 10. Otherwise, proceed to Step 4.
- **Step 4**: Log in to the standby Cisco PGW 2200 Softswitch and change directories to the etc subdirectory by entering the following UNIX command:
  ```
  cd /opt/CiscoMGC/etc
  ```
Step 5  Open the XECfgParm.dat using a text editor, such as vi.

Step 6  Set the value of the *.Virtual_IP_Addr parameter to match the value on the active Cisco PGW 2200 Softswitch.

Step 7  Save your changes and close the text editor.

Step 8  Stop the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

Step 9  Restart the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Wrong IP Path

This alarm occurs when an IP route or local interface associated with the identified component cannot be used. This can happen when one of the following occurs:

- A route has been overridden by another route in the operating system routing table.
- A route configured on your system has been deleted by someone using the UNIX command route delete.
- An IP link or route has been provisioned incorrectly.
- This alarm can also occur if an IP signaling channel has been misconfigured. Use the netstat -rnv UNIX command to retrieve the current operating system routing table.

Corrective Action

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

Step 1  Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Log in to the active Cisco PGW 2200 Softswitch and retrieve the current operating system routing table using the following UNIX command:

```
netstat -rnv
```

The system returns a response similar to the following:

```
IRE Table: IPv4
Destination          Mask             Gateway          Device  Flags
------------------- ---------- ---------- ---------- ------- -----
10.82.80.0           255.255.255.0  10.82.82.1       UGH
10.82.81.0           255.255.255.0  10.82.83.1       UGH
10.82.82.0           255.255.255.0  10.82.82.112      hme0    U
10.82.83.0           255.255.255.0  10.82.83.112      hme1    U
default              0.0.0.0         10.82.82.1       UG
224.0.0.0            240.0.0.0       10.82.82.112      hme0    U
127.0.0.1            255.255.255.255 127.0.0.1       lo0     UN
```
Step 3 If the response does not contain the route identified in the alarm, open the operating system routing table file using a text editor such as vi. Otherwise, proceed to Step 6.

Step 4 Add the route to the routing table using the appropriate text editor command.

Step 5 Save the file and exit the editing session. If this resolves the problem, the procedure is complete. Otherwise, proceed to Step 6.

Step 6 Verify that the provisioned settings for the identified IP link are correct, using the prov-rtrv MML command, as described in the “Retrieving Provisioning Data” section on page 3-68.

If the provisioned settings for your IP link are correct, proceed to Step 8.

If the provisioned settings for your IP link are incorrect, proceed to Step 7.

Step 7 Start a dynamic reconfiguration session to change the settings, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66. If this resolves the problem, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**XE Rsnc Fail**

This alarm occurs when memory resources have been exhausted on the active Cisco PGW 2200 Softswitch. If this alarm occurs frequently you may need to add additional memory to your Cisco PGW 2200 Softswitch. See the Sun Microsystems documentation for your Cisco PGW 2200 Softswitch for more information about adding additional memory.

**Corrective Action**

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

**Step 1** Collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Perform a manual switchover, as described in the “Performing a Manual Switchover” section on page 3-95.

**Warning** Switchover operations cause the loss of all SS7 messages transmitted to the Cisco PGW 2200 Softswitch for approximately three seconds. This affects unstable in-progress calls as well as new calls. Stable in-progress calls are not affected.

**Step 3** Stop the Cisco PGW 2200 Softswitch software on the newly standby Cisco PGW 2200 Softswitch, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

**Step 4** Restart the Cisco PGW 2200 Softswitch software on the newly standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

If this resolves the problem, the procedure is complete. Otherwise, proceed to Step 5.
Step 5  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 PGW 2200 Softswitch Release 9 Messages Reference.

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, see 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. See the Cisco PGW 2200 Softswitch Release 9.8 Software 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, see the “Using the Log Viewer” section on page 3-128.

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 PGW 2200 Softswitch. Then 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 EST | 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 EST | 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 EST | 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 13:35:32:923 2001 EST | 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 EST | unknown (PID 15663) <Info>
/tmp/almM_input: installed time handler, hdlrId = 1

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 EST”. 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 PGW 2200 Softswitch 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 PGW 2200 Softswitch software processes.

Table 8-1 lists the logging levels that can be selected for the Cisco PGW 2200 Softswitch software processes without severely degrading system performance.

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

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 PGW 2200 Softswitch, 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 3-5.
- `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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch:

```
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.

---

**Collecting System Data for Cisco TAC**

Cisco PGW 2200 Softswitch software has a data collection script. When you run this script, a data snapshot of your system is saved into a log file. You should run this script shortly after you discover a problem, and prior to taking any corrective action.

This script collects the following information in the log file:

- System name
- System boot messages
- Operating system patch level
- System patch level
- Processor information
- Disk usage
- Processor tables
- CPU utilization
- Number of users logged in
- Statistics for the Ethernet interfaces
- IP routing
- System setup
- Swap space
- Date and time of last system reboot
- Permissions for the configuration library (CONFIG_LIB)
- File permissions for the /opt/CiscoMGC/etc and /opt/CiscoMGC/bin directories
- Copy of the XECfgParm.dat file

To collect your system data snapshot, perform the following steps:

**Step 1** Log in to your active Cisco PGW 2200 Softswitch, and enter the following UNIX command to change directories:

```
cd /opt/CiscoMGC/local
```

**Step 2** Enter the following to run the system data snapshot script:
Resolving SS7 Network Related Problems

The Cisco PGW 2200 Softswitch platform 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 8-89**
- **Signaling Destination Problems, page 8-93**
- **Signaling Channel Troubleshooting Procedures, page 8-96**
Signaling Channel Problems

The Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch uses to transfer signaling information among itself, the Cisco ITP-Ls, and the Signal Transfer Points (STPs). Signaling links provide the necessary delivery reliability for higher-layer SS7 signaling protocols.

You can use the Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch Platform Operations,” for detailed information.

Note
For more information on MML commands, see the Cisco PGW 2200 Softswitch Release 9 MML Reference.

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, page 8-89
- SS7 Load Sharing Malfunction, page 8-90
- Physical Layer Failures, page 8-92
- Configuration Errors, page 8-92
- Supporting Entity Failures, page 8-92
- Incomplete Signaling, page 8-92
- Changing Service States, page 8-93

SS7 Link is Out-of-Service

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

Step 1
If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Resolving SS7 Network Related Problems

Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

SS7 Load Sharing Malfunction

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

**Step 1** If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** Log in to the active Cisco PGW 2200 Softswitch, 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 PRI   SLC     TIMESLOT SESSIONSET
---- ---- --- ------ -------- ---------
ls1link1 ls1 1    0       0          c7-slct1
```
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Resolving SS7 Network Related Problems

Step 3  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
route2                opc1                  dpc2                  ls2 1
rt3                   opc2                  scp2                  ls-itu 1
rt1                   opc2                  stpl                   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 4  Start a provisioning session, as described in “Starting a Provisioning Session” section on page 3-64.

Step 5  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 C7/SS7 Link or Linkset” section on page 8-98.

Step 6  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 7  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 an SS7 Signaling Service” section on page 8-97.

Step 8  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 9  Save and activate your provisioning changes, as described in the “Saving and Activating your Provisioning Changes” section on page 3-65.

If the conditions clears, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.
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 ITP-L 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 ITP-L and the Cisco PGW 2200 Softswitch can be caused by

- Ethernet card failure on the Cisco ITP-L
- Ethernet card failure on the Cisco switch
- Cisco switch failure
- Fast Ethernet interface card failure on the Cisco PGW 2200 Softswitch

In each of the above cases, it is impossible to transfer MTP3 signaling messages from the Cisco ITP-L to the Cisco PGW 2200 Softswitch. Cisco ITP-L platform failure (which is equivalent to MTP2 failure) causes signaling messages to be unable to go to MTP3. The MTP2 layer on the Cisco ITP-L is supposed to transmit SIOO messages to the STP mated pair to initiate the changeover procedure. Cisco ITP-L 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 8-92. 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 PGW 2200 Softswitch 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 PGW 2200 Softswitch 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 PGW 2200 Softswitch Alarms” section on page 8-3.

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 PGW 2200 Softswitch 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 PGW 2200 Softswitch. 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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch 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, page 8-94**
- **Configuration Errors, page 8-95**
- **Traffic Restart, page 8-95**
- **SS7 Destination is Out of Service, page 8-95**
- **SS7 Route is Out of Service, page 8-95**
- **SS7 Destination is Unavailable, page 8-96**

**Bouncing SS7 Links**

Usually, this condition is caused by mismatched signaling link codes (SLCs) or DPCs/OPCs between the Cisco PGW 2200 Softswitch and the far end. To resolve a bouncing SS7 condition, perform the following steps:

**Step 1** If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2** 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 3-68, 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 3. Otherwise, modify the settings to match with those used on the far end. See the “Invoking Dynamic Reconfiguration” section on page 3-66 for more information about modifying the settings of a provisioned component. If that clears the problem, the procedure is complete. Otherwise, proceed to Step 3.

**Step 3** Ensure that the local MTP3 timer settings match the network defaults by performing the “Verifying MTP3 Timers” section on page 8-102.

If the local MTP3 timer settings match the network defaults, proceed to Step 4. 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 4.

**Step 4** View the system logs, as described in the “Viewing System Logs” section on page 8-83, looking for excessive alignment error monitoring (AERM) logs. If large numbers of AERM logs are present, proceed to Step 5.

If no AERM logs are present, proceed to Step 6.

**Step 5** Determine why the link is not aligning properly by checking the alignment status on the Cisco ITP-L associated with the affected link, as described in the “Verifying the Link Alignment Status” section on page B-6.

If the conditions clears, the procedure is complete. Otherwise, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 PGW 2200 Softswitch 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 PGW 2200 Softswitch 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 If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Contact your SS7 provider and have them verify the links from the DPC to the associated STP.

Step 3 Verify the state of the signaling channels, as described in the “Verifying the Status of all Signaling Services” section on page 3-9.

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 8-89. 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 8-95.

If the conditions clear, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

SS7 Route is Out of Service

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

Step 1 If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Resolving SS7 Network Related Problems

Step 2  Change the service state of the destination to in-service, as described in the “Setting the Service State of a Signaling Service” section on page 8-97.

If the destination goes into service, the procedure is complete. Otherwise, proceed to Step 3.

Step 3  Verify the state of the signaling channels, as described in the “Verifying the Status of all Signaling Services” section on page 3-9.

If none of the SS7 links are in-service, proceed to Step 4. 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 4  Determine why the link is not aligning properly by checking the alignment status on the Cisco ITP-L associated with the affected link, as described in the “Verifying the Link Alignment Status” section on page B-6.

If the conditions clears, the procedure is complete. Otherwise, proceed to Step 5.

Step 5  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 8-95.

Signaling Channel Troubleshooting Procedures

The following sections are procedures used to resolve problems associated with the Cisco PGW 2200 Softswitch platform signaling connections to other networks:

- Setting the Service State of a Signaling Service, page 8-97
- Setting the Service State of an SS7 Signaling Service, page 8-97
- Setting the Service State of a C7/SS7 Link or Linkset, page 8-98
- Setting the Service State of an IP Link, page 8-98
- Setting the Service State of an IP Route, page 8-99
- Setting the Service State of a D-channel, page 8-100
- Setting the Service State of a Local Subsystem Number, page 8-100
- Setting the Service State of an Association, page 8-101
- Verifying MTP Timer Settings, page 8-101
- Modifying Configurable Timers, page 8-103
- Managing Japanese SS7 Signaling Link Tests, page 8-112
- Managing Japanese SS7 Signaling Route Tests, page 8-113
- Verifying Proper Loading of a Dial Plan, page 8-114
- Verifying Configuration to Support Multiple Versions of SS7, page 8-115
- Resolving an Association Alarm, page 8-115
Setting the Service State of a Signaling Service

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

⚠️ **Caution**

The `set-dest` command should only be used while you are dynamically reconfiguring the system. Do not use the `set-dest` 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 PGW 2200 Softswitch, start an MML session, and enter the following command:

```
set-dest: sig_srv: serv_state
```

Where:

- `sig_srv`—The MML name of the desired signaling service.
- `serv_state`—The desired service state. The valid states are listed below:
  - IS—Places a signaling service in service.
  - OOS—Places a signaling service 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. See the documentation for the media gateway for more information on shutting down D-channels.

For example, to set the service state of a signaling service called sigsrv1 to IS, enter the following command:

```
set-dest: sigsrv1: IS
```

**Step 2**

Verify that the state of the destination has changed by entering the `rtrv-dest` command, as described in the Retrieving Signaling Service States, page 3-43.

---

Setting the Service State of an SS7 Signaling Service

To set the service state of an SS7 signaling service, perform the following steps:

⚠️ **Caution**

The `set-spc` command should only be used while you are dynamically reconfiguring the system. Do not use the `set-spc` 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 PGW 2200 Softswitch, start an MML session, and enter the following command:

```
set-spc:ss7_srv:serv_state
```

Where:
- `ss7_srv` — The MML name of the desired SS7 signaling service.
- `serv_state` — The desired service state. The valid states are listed below:
  - IS — Places the SS7 signaling service in service.
  - OOS — Takes the SS7 signaling service out of service.

For example, to set the service state of an SS7 signaling service called `ss7srv1` to IS, enter the following command:

```
set-spc:ss7srv1:IS
```

Step 2 Verify that the state of the SS7 signaling service has changed by entering the `rtrv-spc` command, as described in the Retrieving the State of SS7 Signaling Services, page 3-47.

---

Setting the Service State of a C7/SS7 Link or Linkset

To change the service state of an SS7 link, log in to the active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command:

```
set-c7lnk:c7link_name:serv_state
```

Where:
- `c7link_name` — MML name of the SS7 link you want to modify.
- `serv_state` — Service state to which you want to change. Valid values for SS7 links are IS, OOS, FOOS, INH, and UNH.

**Note** To set the last link in a linkset out of service, you must enter the FOOS service state in the command.

For example, to set the service state of the SS7 link, `c7link1`, to IS, enter the following command:

```
set-c7lnk:c7link1:IS
```

You can verify that the selected SS7 link is in the proper service state by performing the procedure in the Retrieving Service State of C7/SS7 Links or Linksets, page 3-44.

**Note** To modify the service state of the backhaul link for the Cisco ITP-L, you must set the state of all link types associated with that Cisco ITP-L. The possible link types are S77 links (`c7lnk`), D-channels (`dchan`), and IP links (`iplnk`).

---

Setting the Service State of an IP Link

To change the service state of an IP link, log in to the active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command:
Resolving SS7 Network Related Problems

set-iplink:iplink_name:serv_state[:confirm]

Where:
- *iplink_name*—MML name of the IP link you want to modify.
- *serv_state*—Service state to which you want to change. Valid values for IP links are IS, OOS, and FOOS.
- *confirm*—This parameter is required when you are setting the service state of an MGCP link. Other types of IP links do not require this parameter.

For example, to set the service state of the IP link, *iplink1*, to IS, enter the following command:
```mml
set-iplink:iplink1:IS
```

In another example, you would enter the following command to set the service state of an MGCP link called *mgcplnk1* to IS:
```mml
set-iplink:mgcplnk1:IS::confirm
```

You can verify that the selected IP link is in the proper service state by performing the procedure in the “Retrieving the Service State for IP Links” section on page 3-44.

**Note**
To modify the service state of the backhaul link for the Cisco ITP-L, you must set the state of all link types associated with that Cisco ITP-L. The possible link types are S77 links (c7lnk), D-channels, (dchan), and IP links (iplnk).

Setting the Service State of an IP Route

To change the service state of an IP route, log in to the active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command:
```mml
set-iproute:iproute_name:serv_state[,confirm]
```

Where:
- *iproute_name*—MML name of the IP route you want to modify.
- *serv_state*—Service state to which you want to change. Valid values for IP links are IS, OOS, and FOOS.
- *confirm*—This parameter is required when you are setting the service state to OOS or FOOS.

**Note**
This command cannot be used on the standby Cisco PGW 2200 Softswitch.

An IP route in any of the following combinations of primary and secondary service states can be set to OOS or FOOS:
- IS
- OOS, CONF
- OOS, OFF_DUTY
- OOS, STDBY

For an IP route to be set to IS, it must have a primary service state of OOS and secondary service state of COOS.
Resolving SS7 Network Related Problems

For example, you would enter the following command to set the service state of an IP route called iprte1 to OOS:

```
set-iproute:iprte1:OOS,confirm
```

Note
You can verify that the selected IP route is in the proper service state by performing the procedure in the “Retrieving the Service State for IP Routes” section on page 3-45.

Setting the Service State of a D-channel

To change the service state of a D-channel, log in to the active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command:

```
set-dchan:dchan_name:serv_state
```

Where:
- `dchan_name`—MML name of the D-channel you want to modify.
- `serv_state`—service state to which you want to change. Valid values for D-channels are IS and OOS.

For example, to set the service state of the D-channel, `dchan-1`, to IS, enter the following command:

```
set-dchan:dchan-1:IS
```

You can verify that the selected D-channel is in the proper service state by performing the procedure in the “Retrieving the Service State of D-Channels” section on page 3-46.

Note
To modify the service state of the backhaul link for the Cisco ITP-L, you must set the state of all link types associated with that Cisco ITP-L. The possible link types are S77 links (c7lnk), D-channels, (dchan), and IP links (iplnk).

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 PGW 2200 Softswitch, 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
```
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Resolving SS7 Network Related Problems

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 3-48.

Setting the Service State of an Association

To change the service state of an association, log in to the active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command:

\[
\text{set-association:assoc\_name:serv\_state[\text{,confirm}]} \\
\]

Where:

- \text{assoc\_name}—MML name of the association you want to modify.
- \text{serv\_state}—Service state to which you want to change. Valid values for IP links are IS, OOS, and FOOS.
- \text{confirm}—This parameter is required when you are setting the service state to OOS or FOOS.

Note  This command cannot be used on the standby Cisco PGW 2200 Softswitch.

For example, to set the service state of the association, assoc1, to OOS, enter the following command:

\[
\text{set-association:assoc1:OOS,confirm} \\
\]

You can verify that the selected association is in the proper service state by performing the procedure in the “Retrieving the Service State for Associations” section on page 3-49.

Verifying MTP Timer Settings

When resolving signaling problems between the Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch 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 PGW 2200 Softswitch. The following subsections describe methods for verifying the MTP timer settings on the Cisco PGW 2200 Softswitch.

Note  See the Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide for more information on the MTP timers.

Verifying MTP2 Timers

To verify the values used for the MTP2 timers on the Cisco ITP-Ls, complete the following steps:

Step 1  Enter the following command at the Cisco ITP-L to display the settings for the MTP2 timers:

\[
\text{Router \#show SS7 mtp2 timer channel} \\
\]

Where: \text{channel} specifies a channel, 0 through 3.

The system returns a message similar to the following:

SS7 MTP2 Timers for channel 0 in milliseconds
Resolving SS7 Network Related Problems

Step 2 Verify the MTP2 timers settings listed for the Cisco ITP-Ls 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” section on page 8-103.

Verifying MTP3 Timers

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

Step 1 Log on to active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command to display the settings for the MTP3 timers:

```
prov-rtrv:lnksetprop:name="MML_name"
```

Where `MML_name` is the MML name for the linkset associated with the MTP3 timers you want to verify.

The system returns a message similar to the following:

```
MGC-01 - Media Gateway Controller 2000-07-27 18:33:56
M RTRV
"session=nsite04:sigsvcprop"
/*
   mtp3ApcMtpRstrtT28 = 50
   mtp3DlnkConnAckT7 = 10
   mtp3PrcUnhT13 = 10
   mtp3InhAckT14 = 20
   mtp3LocInhTstT20 = 900
   mtp3MaxSltTries = 2
   mtp3MsgPriority = 2
   mtp3MtpRstrtT24 = 60
   mtp3RepeatRstrtT26 = 150
   mtp3FtrUsed = false
   mtp3TrsSmT29 = 600
   mtp3TstSlitmT1 = 60
   mtp3TstSlitmT2 = 600
   mtp3UnhAckT12 = 10
   reference = ANSI96
*/
```

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.

---

### Modifying Configurable Timers

In prior releases of the Cisco PGW 2200 Softswitch software, you could not modify the settings of the message transfer part level 3 (MTP3) and redundant link manager (RLM) timers. You can modify the settings of these timers. The procedures for verifying and modifying these timers are described in the following sections:

- Modifying MTP2 Timers, page 8-103
- Verifying and Modifying MTP3 Timer Settings, page 8-104
- Verifying and Modifying RLM Timers, page 8-105
- Verifying and Modifying ISUP Timer Settings, page 8-107
- Rebooting Your System to Modify Properties, page 8-111

#### Modifying MTP2 Timers

Use the following MML commands at the Cisco ITP-L 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

See 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, see the procedure in the “Verifying MTP2 Timers” section on page 8-101.
Resolving SS7 Network Related Problems

Verifying and Modifying MTP3 Timer Settings

When resolving signaling problems between the Cisco PGW 2200 Softswitch and an associated SS7 network element (such as an STP), you may need to verify that the MTP3 timer settings used by the Cisco PGW 2200 Softswitch conform to settings used by the associated SS7 network element. If the settings do not match, you need to modify the settings for the MTP3 timers.

Note

See the Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide for more information on the MTP timers.

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

Step 1
Log on to active Cisco PGW 2200 Softswitch, 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"
/*
mt2AermEmgThr = 1
mt2AermNrmThr = 4
mt2CongDiscard = false
mt2LsSuLen = 1
mt2MaxAlignRetries = 5
mt2MaxMuFrmLen = 272
mt2MaxOutsFrames = 127
mt2ProvingEmgt4 = 6
mt2ProvingNormalT4 = 23
mt2SuermThr = 64
mt2T1 = 130
mt2T2 = 115
mt2T3 = 115
mt2T5 = 1
mt2T6 = 30
mt2T7 = 10
mt3ApcMtpRstrtT28 = 30
mt3DlnkConnAckT7 = 10
mt3FrcUnhT13 = 10
mt3InhAckT14 = 20
mt3LocInhTstT20 = 900
mt3MaxSltTries = 2
mt3MsgPriority = 2
mt3MtpRstrtT24 = 100
mt3RepeatRstrtT26 = 150
mt3TfrUsed = false
mt3TraSntT29 = 600
mt3tstSltmT1 = 60
mt3tstSltmT2 = 600
mt3UnhAckT12 = 10
reference = ANSI92
rudpAck = enable
rudpKeepAlives = enable
rudpNumRetx = 2
```

Note

See the Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide for more information on the MTP timers.

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

Step 1
Log on to active Cisco PGW 2200 Softswitch, 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"
/*
mt2AermEmgThr = 1
mt2AermNrmThr = 4
mt2CongDiscard = false
mt2LsSuLen = 1
mt2MaxAlignRetries = 5
mt2MaxMuFrmLen = 272
mt2MaxOutsFrames = 127
mt2ProvingEmgt4 = 6
mt2ProvingNormalT4 = 23
mt2SuermThr = 64
mt2T1 = 130
mt2T2 = 115
mt2T3 = 115
mt2T5 = 1
mt2T6 = 30
mt2T7 = 10
mt3ApcMtpRstrtT28 = 30
mt3DlnkConnAckT7 = 10
mt3FrcUnhT13 = 10
mt3InhAckT14 = 20
mt3LocInhTstT20 = 900
mt3MaxSltTries = 2
mt3MsgPriority = 2
mt3MtpRstrtT24 = 100
mt3RepeatRstrtT26 = 150
mt3TfrUsed = false
mt3TraSntT29 = 600
mt3tstSltmT1 = 60
mt3tstSltmT2 = 600
mt3UnhAckT12 = 10
reference = ANSI92
rudpAck = enable
rudpKeepAlives = enable
rudpNumRetx = 2
```
Verifying and Modifying RLM Timers

If you want to change the values for these timers, you must change them on the Cisco PGW 2200 Softswitch and on the associated media gateway(s). See the documentation for your media gateway for more information on changing the RLM timers on the media gateway. To change the RLM timers on the Cisco PGW 2200 Softswitch, perform the following steps:

Verifying and Modifying RLM Timers

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 keepalives are sent by the media gateway to the Cisco PGW 2200 Softswitch. If the RLM keepalive timer on the Cisco PGW 2200 Softswitch 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.
**Resolving SS7 Network Related Problems**

**Step 1** Verify the current settings of your RLM timers on the Cisco PGW 2200 Softswitch by logging in to the standby Cisco PGW 2200 Softswitch, starting an MML session, and entering the following command:

```
prov-rtrv:lnksetprop:name="protocol_fam"
```

Where `protocol_fam` is the MML name for the associated protocol family.

For example, to retrieve the values of RLM timers for an ANSI signaling environment, you would enter the following command:

```
prov-rtrv:lnksetprop:name="SS7-ANSI"
```

The system returns a response similar to the following:

```
MGW-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, using the procedure in the “Starting a Provisioning Session” section on page 3-64.

**Step 3** Modify the RLM timer properties, as needed, using the following command:

```
prov-ed:lnksetprop:name="protocol_fam",prop_name="value",prop_name="value",...
```

Where:

- `protocol_fam`—The MML name of the associated protocol family.
- `prop_name`—The name of the RLM timer property you want to modify.
- `value`—The value you want for the specified RLM timer property.

For example, to change the values of RLM timers for an ANSI signaling environment, you would enter the following command:

```
prov-ed:lnksetprop:name="SS7-ANSI",timerLinkDownMin="120",timerLinkEcho="15"
```

**Step 4** Save and activate your provisioning session, using the procedure in the “Saving and Activating your Provisioning Changes” section on page 3-65.

**Step 5** Reboot your system as described in the “Rebooting Your System to Modify Properties” section on page 8-111.
Verifying and Modifying ISUP Timer Settings

When resolving signaling problems you may need to verify that the ISUP timer settings used by the Cisco PGW 2200 Softswitch conform to settings used by the associated network elements. If the settings do not match, you need to modify the settings for the ISUP timers. You can modify the settings of the local ISUP timers. The configurable ISUP timers are listed in the table below, grouped according to the associated ISUP protocol(s) for each. Other ISUP timers cannot be changed.

Table 8-2 Configurable ISUP Timer Protocol Listings

<table>
<thead>
<tr>
<th>Timers</th>
<th>Associated Protocol Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>• ANSISS7_STANDARD</td>
</tr>
<tr>
<td></td>
<td>• Q761_BASE</td>
</tr>
<tr>
<td></td>
<td>• Q767_BASE</td>
</tr>
<tr>
<td></td>
<td>• Q761_SINGAPORE</td>
</tr>
<tr>
<td></td>
<td>• Q761_ARGENTINA</td>
</tr>
<tr>
<td></td>
<td>• ISUPV2_FINNISH96</td>
</tr>
<tr>
<td></td>
<td>• ISUPV2_FRENCH</td>
</tr>
<tr>
<td></td>
<td>• Q761_THAILAND</td>
</tr>
<tr>
<td></td>
<td>• Q761_PERU</td>
</tr>
<tr>
<td></td>
<td>• Q761_BELG_C2</td>
</tr>
<tr>
<td></td>
<td>• ISUPV2_JAPAN</td>
</tr>
<tr>
<td>T2, T5, T6</td>
<td>• ANSISS7_STANDARD</td>
</tr>
<tr>
<td>T7, T8, T9</td>
<td>• Q761_BASE</td>
</tr>
<tr>
<td>T12, T13, T14</td>
<td>• Q767_BASE</td>
</tr>
<tr>
<td>T15, T16, T17</td>
<td>• Q761_SINGAPORE</td>
</tr>
<tr>
<td>T18, T19, T20</td>
<td>• Q761_ARGENTINA</td>
</tr>
<tr>
<td>T21, T22, T23</td>
<td>• ISUPV2_SPANISH</td>
</tr>
<tr>
<td>T24, T25, T26</td>
<td>• ISUPV2_FINNISH96</td>
</tr>
<tr>
<td>T27, T33, T36</td>
<td>• ISUPV2_FRENCH</td>
</tr>
<tr>
<td></td>
<td>• Q761_THAILAND</td>
</tr>
<tr>
<td></td>
<td>• Q761_PERU</td>
</tr>
<tr>
<td></td>
<td>• Q761_BELG_C2</td>
</tr>
<tr>
<td></td>
<td>• ISUPV2_JAPAN</td>
</tr>
<tr>
<td>Timers</td>
<td>Associated Protocol Files</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>T28</td>
<td>ANSIS7_STANDARD</td>
</tr>
<tr>
<td></td>
<td>Q761_BASE</td>
</tr>
<tr>
<td></td>
<td>Q761_SINGAPORE</td>
</tr>
<tr>
<td></td>
<td>Q761_ARGENTINA</td>
</tr>
<tr>
<td></td>
<td>ISUPV2_SPANISH</td>
</tr>
<tr>
<td></td>
<td>ISUPV2_FINNISH96</td>
</tr>
<tr>
<td></td>
<td>ISUPV2_FRENCH</td>
</tr>
<tr>
<td></td>
<td>Q761_THAILAND</td>
</tr>
<tr>
<td></td>
<td>Q761_PERU</td>
</tr>
<tr>
<td></td>
<td>Q761_BELG_C2</td>
</tr>
<tr>
<td></td>
<td>ISUPV2_JAPAN</td>
</tr>
<tr>
<td>T34</td>
<td></td>
</tr>
<tr>
<td>T35</td>
<td>Q761_BASE</td>
</tr>
<tr>
<td></td>
<td>Q767_BASE</td>
</tr>
<tr>
<td></td>
<td>Q761_SINGAPORE</td>
</tr>
<tr>
<td></td>
<td>Q761_ARGENTINA</td>
</tr>
<tr>
<td></td>
<td>ISUPV2_SPANISH</td>
</tr>
<tr>
<td></td>
<td>ISUPV2_FINNISH96</td>
</tr>
<tr>
<td></td>
<td>ISUPV2_FRENCH</td>
</tr>
<tr>
<td></td>
<td>Q761_THAILAND</td>
</tr>
<tr>
<td></td>
<td>Q761_PERU</td>
</tr>
<tr>
<td></td>
<td>Q761_BELG_C2</td>
</tr>
<tr>
<td></td>
<td>ISUPV2_JAPAN</td>
</tr>
</tbody>
</table>

Table 8-2 Configurable ISUP Timer Protocol Listings
Table 8-2  Configurable ISUP Timer Protocol Listings

<table>
<thead>
<tr>
<th>Timers</th>
<th>Associated Protocol Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>T38</td>
<td>• Q761_BASE&lt;br&gt;• Q761_SINGAPORE&lt;br&gt;• Q761ARGINETINA&lt;br&gt;• ISUPV2_SPANISH&lt;br&gt;• ISUPV2_FINNISH96&lt;br&gt;• ISUPV2_FRENCH&lt;br&gt;• Q761_THAILAND&lt;br&gt;• Q761_BELG_C2&lt;br&gt;• ISUPV2_JAPAN</td>
</tr>
<tr>
<td></td>
<td>• T_CCR&lt;br&gt;• T_CCCR&lt;br&gt;• T_CGB&lt;br&gt;• T_CGBA&lt;br&gt;• T_CRA&lt;br&gt;• T_GRS&lt;br&gt;• T_CVT</td>
</tr>
</tbody>
</table>

Note: The default values and valid ranges for each of these timers within the supported protocols can be found in the Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide.

To verify and modify the values used for the ISUP timers, complete the following steps:

Step 1: Unless you have previously created a profile for the associated signaling service or trunk group with modified values for these ISUP timers, the values for these eight timers match the default values listed in the tables above. If you have previously created a profile with modified ISUP timer values for the associated signaling service or trunk group, proceed to Step 2 to retrieve the current values set in the profile. Otherwise, proceed to Step 3.

Step 2: Log on to active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command to display the settings for the modified ISUP timers:

```
prov-rtrv:profile:name="profile_name"
```

Where `profile_name` is the MML name for the profile that contains the modified values for the configurable ISUP timers.

The system returns a message similar to the following:

```
MGC-01 - Media Gateway Controller 2002-10-07 15:47:39.928 EST
M RTRV
"session=NOA_SPAIN:profile"
/*
ProfileType PropertyName ProfileValue
-------------- -------------- -------------
isuptmrprofile T1 5000
```
Resolving SS7 Network Related Problems

Chapter 8      Troubleshooting the Cisco PGW 2200 Softswitch Platform

Resolving SS7 Network Related Problems

Step 3 Verify the ISUP timers settings listed against the ISUP timers used at the associated destination.
If the ISUP timers settings match, your signaling problem has different cause. Check for alarms on your system and resolve them using the procedures in the “Alarm Troubleshooting Procedures” section on page 8-4.
If the ISUP timers settings do not match, proceed to Step 4.

Step 4 Start a provisioning session, using the procedure in the “Starting a Provisioning Session” section on page 3-64.

Step 5 If you have already defined a profile that modifies the configurable ISUP timers, proceed to Step 8. Otherwise, proceed to Step 6.

Step 6 Enter your new ISUP timer values using the following command:
prov-add:profile:name="profile_name",type="isuptmrprofile", timer_number="timer_value",
timer_number="timer_value", timer_number="timer_value"

Where:
- profile_name—MML name for the profile that contains the set of ISUP measurements being used.
- timer_number—number of the timer to be modified.
- timer_value—New value for the selected ISUP timer.

Note See the Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide for more information on the valid ranges for the ISUP timers. If you enter a number outside the valid range, the default value is used.

In the following example, the values of the T6, T8, and T35 ISUP timers are modified:
prov-add:profile:name="set1",type="isuptmrprofile",T6="30000",T8="12000",T35="18000"

Step 7 Create a profile for your new ISUP timer values using the following command:
prov-add:component:name="comp_name",isuptmrprofile="profile_name"

Where:
- component—MML component type name for signaling service or trunk group profiles. Enter one of the following:
  - sigpathprof—Component type for signaling service profiles.
  - trnkgrpprof—Component type for trunk group profiles.
- comp_name—MML name for the signaling service or trunk group profile to be associated with the set of new ISUP timer values, as set in Step 6.
- profile_name—MML name for the profile that contains the customized set of ISUP measurements, as set in Step 6.

Once the new ISUP timer values have been set, proceed to Step 9.

Step 8 Modify the parameters for the desired ISUP timers by entering the following command:
prov-ed:profile:name="profile_name",type="isuptmrprofile", timer_number="timer_value",
timer_number="timer_value", timer_number="timer_value"

Where:
- profile_name—MML name for the profile that contains the set of ISUP measurements being used.
• *timer_number*—number of the timer to be modified.
• *timer_value*—New value for the selected ISUP timer.

**Note**  
See the *Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide* for more information on the valid ranges for the ISUP timers. If you enter a number outside the valid range, the default value is used.

In the following example, the values of the T6, T8, and T33 ISUP timers are modified:

```
```

Once the new ISUP timer values have been set, proceed to Step 9.

**Step 9**  
Save and activate your provisioning session, using the procedure in the “Saving and Activating your Provisioning Changes” section on page 3-65.

---

### Rebooting Your System to Modify Properties

When you are modifying MTP3 and RLM timers on the Cisco PGW 2200 Softswitch, it is required that you reboot your system as part of the modification process. To do this, perform the following steps:

**Step 1**  
Log in to your active Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch software on your active Cisco PGW 2200 Softswitch, using the procedure in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

**Note**  
Shutting down the Cisco PGW 2200 Softswitch software on the active Cisco PGW 2200 Softswitch causes the currently standby Cisco PGW 2200 Softswitch to become the active Cisco PGW 2200 Softswitch.

**Step 6**  
Restart the Cisco PGW 2200 Softswitch software on this Cisco PGW 2200 Softswitch, using the procedure in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

**Step 7**  
Once the Cisco PGW 2200 Softswitch software is fully activated, log in to the active Cisco PGW 2200 Softswitch and perform a manual switchover, using the procedure in the “Performing a Manual Switchover” section on page 3-95.

**Warning**  
Switchover operations cause the loss of all SS7 messages transmitted to the Cisco PGW 2200 Softswitch for approximately three seconds. This affects unstable in-progress calls as well as new calls. Stable in-progress calls are not affected.

**Step 8**  
Once the manual switchover is complete, log in to the newly active Cisco PGW 2200 Softswitch, start an MML session and enter the following command to synchronize the Cisco PGW 2200 Softswitches:
Resolving SS7 Network Related Problems

Step 9

Once the synchronization is complete, perform a manual switchover using the procedure in the “Performing a Manual Switchover” section on page 3-95.

Warning

Switchover operations cause the loss of all SS7 messages transmitted to the Cisco PGW 2200 Softswitch for approximately three seconds. This affects unstable in-progress calls as well as new calls. Stable in-progress calls are not affected.

Step 10

Once the manual switchover is complete, log in to your newly standby Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch by entering the following UNIX command:

/etc/init.d/CiscoMGC stop

Step 15

Restart the Cisco PGW 2200 Softswitch software on this Cisco PGW 2200 Softswitch by entering the following command:

/etc/init.d/CiscoMGC start

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, page 8-112
- Retrieving Results for a Japanese SS7 Signaling Link Test, page 8-112

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 PGW 2200 Softswitch, start an MML session, and enter the following command:

```plaintext
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:

```plaintext
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 PGW 2200 Softswitch, start an MML session, and enter the following command:
resv-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:

```
resv-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
 *ls1-link1: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 8-113
- Retrieving Results for a Japanese SS7 Signaling Route Test, page 8-114

#### 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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch, start an MML session, and enter the following command:

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

Where:

- \textit{pt\_code}—MML name of an adjacent point code (APC) or destination point code (DPC) configured for Japanese SS7.
- \textit{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

\textbf{Step 1}  If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2  Search the active system log file, as described in the “Viewing System Logs” section on page 8-83, for logs that indicate that the dial plan was loaded incorrectly.

If the dial plan was not loaded correctly, reload the dial plan by saving and activate your dial plan again as described in the “Saving and Activating your Provisioning Changes” section on page 3-65.

If there are no logs that indicate that the dial plan was loaded incorrectly, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**Verifying Configuration to Support Multiple Versions of SS7**

Step 1  If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Log in to the active Cisco PGW 2200 Softswitch and change directories to the etc subdirectory by entering the following UNIX command:

```
cd /opt/CiscoMGC/etc
```

Step 3  Open the alarmCats.dat using a text editor, such as vi.

Step 4  The third column in the file indicates the severity level for each alarm. Verify that the severity level for the All C7 IP Links Fail alarm is set to “2”. If it is set correctly, the procedure is complete. Otherwise, proceed to Step 5 to begin the process of correcting your configuration.

Step 5  Set the the severity level of the All C7 IP Links Fail alarm to “2”.

Step 6  Save your changes and close the text editor.

Step 7  Repeat steps 2 through 6 on the standby Cisco PGW 2200 Softswitch.

Step 8  Stop the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

Step 9  Restart the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

Step 10 Perform a manual switchover from the active Cisco PGW 2200 Softswitch, as described in the “Performing a Manual Switchover” section on page 3-95.

**Warning** Switchover operations cause the loss of all SS7 messages transmitted to the Cisco PGW 2200 Softswitch for approximately three seconds. This affects unstable in-progress calls as well as new calls. Stable in-progress calls are not affected.

---

**Resolving an Association Alarm**

When referred here by an alarm indicating a failure on an association, perform the following steps:
Resolving SS7 Network Related Problems

Step 1 If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 If this alarm occurs along with the LIF FAIL alarm on the failed destination address, proceed to Step 3. Otherwise, proceed to Step 5.

Step 3 Verify the functioning of the cabling between the Cisco PGW 2200 Softswitch and the destination address.
   If the cables are functioning properly, proceed to Step 4.
   If bad cable(s) are found, replace them. If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 4.

Step 4 Verify the functioning of the associated Cisco switch.
   If the switch is functioning properly, proceed to Step 5.
   If the switch is not functioning properly, see the documentation for your switch for troubleshooting information. If that corrects the problem, the procedure is complete. Otherwise, proceed to Step 7.

Step 5 Debug the IP connectivity between the Cisco PGW 2200 Softswitch and the associated external node.
   If the IP connectivity is working correctly, proceed to Step 6.
   If the IP connectivity is not working correctly, see the documentation for the external node to determine a method to identify and fix the IP connectivity problem. If that corrects the problem, the procedure is complete. Otherwise, proceed to Step 6.

Step 6 Determine the health of the associated external node.
   If the external node is working correctly, proceed to Step 7.
   If the external node is not healthy, see the documentation for the external node for troubleshooting information. If that corrects 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Converting Stored and Transmitted Point Code Values

If you are troubleshooting signaling problems, you may encounter point code values displayed in hexadecimal or decimal. You must convert these values to understand which point code is affected, or the value being transmitted by the Cisco PGW 2200 Softswitch. You can follow these basic steps:

Step 1 Convert the hexadecimal or decimal value to binary code.
   For example, if you found a log message indicating a problem with a point code in a ITU SS7 connection, identified with a hexadecimal value of 00:00:36:33, the converted binary value is 000000000000000011011000110011.

Step 2 Remove the padding, based upon which point code address type applies to the point code (14, 16, or 24-bit).

Note You can find an explanation of the point code address types in the Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide.
Continuing with the example, since the problem is with an ITU SS7 connection, the address should be 14 bits in length, resulting in a binary value 11011000110011.

**Note** If you are troubleshooting signaling problems for a Japanese ISUP connection, remember that the Cisco PGW 2200 Softswitch transmits the higher order bits first for those point codes. The fields for any transmitted point code value you retrieve for a Japanese ISUP connection must be reversed while in its binary value for you to correctly identify the associated point code on the Cisco PGW 2200 Softswitch.

**Step 3** Convert the binary code into decimal, using the correct point code format.

**Note** You can find an explanation of the point code formats in the *Cisco PGW 2200 Softswitch Release 9.8 Provisioning Guide*.

Concluding the example, since the problem is with an ITU SS7 connection and the value came from a Cisco PGW 2200 Softswitch log message, the address should use the ITU International point code format (3-bits/8-bits/3-bits, or 3-8-3), the resulting point code is 6.198.3.

**Resolving Bearer Channel Connection Problems**

Bearer channels are the focus of everything that the Cisco PGW 2200 Softswitch does. The main function of the Cisco PGW 2200 Softswitch 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 3-15.

The following sections contain procedures that are related to resolving problems associated with the Cisco PGW 2200 Softswitch platform bearer channel connections:

- Setting the Administrative State, page 8-118
- Querying Local and Remote CIC States, page 8-124
- Performing CIC Validation Tests, page 8-126
- Resolving ISDN D-Channel Discrepancies, page 8-131
- Unblocking CICs, page 8-133
- Resetting CICs, page 8-134
- Resolving Stuck CICs, page 8-135
- Auditing Call States, page 8-139
- Stopping Calls, page 8-139
- Auditing an MGCP Media Gateway, page 8-142
- Running a Manual Continuity Test, page 8-144
- Verifying Continuity Test Settings, page 8-144
- Media Gateway IP Destination/Link Out-of-Service, page 8-146
Resolving Bearer Channel Connection Problems

- Calls Fail at the Cisco PGW 2200 Softswitch, page 8-147
- 3.1 KHz (ISDN Category 3) Calls are Failing, page 8-148
- Calls are Misrouting, page 8-149

Setting the Administrative State

You can use the `set-admin-state` MML command to change the administrative state of various components. A log message 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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch, page 8-118
- Setting the Administrative State of a Media Gateway, page 8-119
- Setting the Administrative State of a Trunk Group, page 8-119
- Setting the Administrative State of a Signaling Service, page 8-120
- Setting the Administrative State of Spans, page 8-121
- Setting the Administrative State of CICs, page 8-123

### Setting the Administrative State of a Cisco PGW 2200 Softswitch

To set the administrative state of a Cisco PGW 2200 Softswitch, perform the following steps:

**Step 1**

Log in to the active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command:

```
set-admin-state:mgc:state
```

Where:

- `mgc`—The MML name of the desired Cisco PGW 2200 Softswitch.
- `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 PGW 2200 Softswitch 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 PGW 2200 Softswitch called `mgc1` to unlock, enter the following command:

```
set-admin-state:mgc1:unlock
```
Step 2 Verify that the state of the Cisco PGW 2200 Softswitch has changed by entering the `rtrv-admin-state` MML command, as described in the “Retrieving the Administrative State of a Cisco PGW 2200 Softswitch” section on page 3-55.

---

### 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 PGW 2200 Softswitch, 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 3-56.

---

### 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 PGW 2200 Softswitch, start an MML session, and enter the following command:

```
set-admin-state:trkgrp:state
```

**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 3-56.
Resolving Bearer Channel Connection Problems

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 3-56.

---

**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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco PGW 2200 Softswitch.
  - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco PGW 2200 Softswitch over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP->Cisco PGW 2200 Softswitch).
  - 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 PGW 2200 Softswitch 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 3-56.

---

### 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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco PGW 2200 Softswitch.
  - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco PGW 2200 Softswitch over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP->Cisco PGW 2200 Softswitch).
  - Signaling service or routeset associated with a DPC.
  - EISUP signaling service.

- `x` — A 16-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 3-57.

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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco PGW 2200 Softswitch.
  - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco PGW 2200 Softswitch over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP->Cisco PGW 2200 Softswitch).
  - Signaling service or routeset associated with a DPC.
  - EISUP signaling service.
- `x`—A 16-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
```
Chapter 8      Troubleshooting the Cisco PGW 2200 Softswitch Platform

Resolving Bearer Channel Connection Problems

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 3-57.

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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco PGW 2200 Softswitch.
  - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco PGW 2200 Softswitch over IP (that is, FE box<sig/tdm>media gateway<N2/IP>Cisco PGW 2200 Softswitch).
  - 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 PGW 2200 Softswitch has changed by entering the **rtrv-admin-state** MML command, as described in the “Retrieving the Administrative State of CICs” section on page 3-58.
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 PGW 2200 Softswitch, start an MML session, and enter the following command:

```
query-cic:sig_srv:cic=number[,rng=range]
```

Where:

- `sig_srv`—The MML name for the signaling service 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. See the Cisco PGW 2200 Softswitch Release 9 MML Command Reference for more information on the SABT error code.

**Note**

The Cisco PGW 2200 Softswitch 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 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 query the state of CICs 20 through 24, associated with a signaling service called `ss7svc1`, you would enter the following command:

```
query-cic:ss7svc1: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
"ss7svc1:CIC=20;LPST=IS;LSST=IDLE;RPST=IS;RSST=IDLE"
"ss7svc1:CIC=21;LPST=IS;LSST=IDLE;RPST=IS;RSST=IDLE"
"ss7svc1:CIC=22;LPST=IS;LSST=IDLE;RPST=IS;RSST=IDLE"
"ss7svc1:CIC=23;LPST=IS;LSST=IDLE;RPST=IS;RSST=IDLE"
"ss7svc1: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 8-125. 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 remotely
  - 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, if your CICs are using ANSI SS7 signaling. To do this, log in to the active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command:

```
query-cic: sig_srv: cic=number[,rng=range], rslv
```

Where:
- `sig_srv`—The MML name for the signaling service 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 PGW 2200 Softswitch 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 CIC state mismatches 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, collect system data as described in the “Collecting System Data for Cisco TAC” section on page 8-87 and contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 PGW 2200 Softswitch 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 PGW 2200 Softswitch and validate the properties for a particular circuit identification code (CIC) using the following command:

\[ \text{vld-cic}: \text{dest}\_pc: \text{cic}=\text{number} \]

Where:

- \text{dest}\_pc—The MML name for the DPC associated with the affected CIC.
- \text{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 - MSC-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 - MSC-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 PGW 2200 Softswitch. 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
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Resolving Bearer Channel Connection Problems

- 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 PGW 2200 Softswitch 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 PGW 2200 Softswitch. 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 PGW 2200 Softswitch and the far-end exchange do not match.

- Z_CLLI—CLLI code for either the far-end exchange or the Cisco PGW 2200 Softswitch. 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 PGW 2200 Softswitch 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 PGW 2200 Softswitch) 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 PGW 2200 Softswitch and/or the associated far-end exchange need to be modified to resolve the error.
If the settings on the Cisco PGW 2200 Softswitch 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:
Resolving Bearer Channel Connection Problems

**Step 4**

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
BothwayWorking = 1
CctGrpCarrier = 2
CGBA2 = 0
CircHopCount = 0
CLIPEss = 0
CotInTone = 2010
CotOutTone = 2010
CotPercentage = 0
dialogRange = 0
ExtCCOT = 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
```

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: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 CUSTOMPIDCUSTGRPPTBLSIDE
---- --- --- -----------------------
ss7am401am401a-pcANSISS7_STANDARD00000101network
ss7am702am702b-pcANSISS7_STANDARD00000101network
ss7inet1inetsp1-pcANSISS7_STANDARD00000101network
ss7am408am408a-pcANSISS7_STANDARD00000101network
ss7am408bam408b-pcANSISS7_STANDARD00000101network
ss7inet2inetsp2-pcANSISS7_STANDARD00000101network
ss7dmsdms100-pcANSISS7_STANDARD00000101network
ss7am401bam401b-pcANSISS7_STANDARD00000101network
ss7am608bam608b-pcANSISS7_STANDARD00000101network
ss7sc2200sc2200-pcANSISS7_STANDARD00000101network
```

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: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 CUSTOMPIDCUSTGRPPTBLSIDE
---- --- --- -----------------------
ss7am401am401a-pcANSISS7_STANDARD00000101network
ss7am702am702b-pcANSISS7_STANDARD00000101network
ss7inet1inetsp1-pcANSISS7_STANDARD00000101network
ss7am408am408a-pcANSISS7_STANDARD00000101network
ss7am408bam408b-pcANSISS7_STANDARD00000101network
ss7inet2inetsp2-pcANSISS7_STANDARD00000101network
ss7dmsdms100-pcANSISS7_STANDARD00000101network
ss7am401bam401b-pcANSISS7_STANDARD00000101network
ss7am608bam608b-pcANSISS7_STANDARD00000101network
ss7sc2200sc2200-pcANSISS7_STANDARD00000101network
```

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`.
Normal = 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.
  - CotPercentage is 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 3-64.

**Step 7**  
Modify the appropriate signaling service settings using the following command:
Resolving Bearer Channel Connection Problems

**Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform**

**Resolving Bearer Channel Connection Problems**

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 PGW 2200 Softswitch 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 SVCTYPESELSEQQABLE
---- --- --- -----------------
1003 DMS100CLLI ss7dms TDM_ISUPASCN
```

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"
/*
CarrierIdentity = 0333
CLLI = GR31764KB5
CompressionType = 1
CotPercentage = 1
CustGrpId = V123
EchoCanRequired = 0
ExtCOT = Loop
GLARE = 2
Npa = 919
RingNoAnswer = 100000
SatelliteInd = 0
```
Resolving Bearer Channel Connection Problems

Step 11 Modify the appropriate trunk group settings using the following command:

```
prov-ed:trnkgrp:name="trnk_grp",param_name="param_value",param_value="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 3-65.

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 PGW 2200 Softswitch 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 PGW 2200 Softswitch 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
```
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Resolving Bearer Channel Connection Problems

Where \( d_{num} \) is the D-channel number identified in the alarm message.

The system returns a message similar to the following:

\[
\begin{align*}
\text{sigChanDev.dat:} & \ 001002bd \ 00160002 \ 1 \ 0034015e \ 00030011 \ 00060001 \ \text{2854} \\
\text{sigChanDev.dat:} & \ 001002be \ 00160002 \ 1 \ 0034015e \ 00030011 \ 00060002 \ \text{2854}
\end{align*}
\]

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 \text{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:

\[
\text{grep } \text{comp\_ID} \ \text{components.dat}
\]

Where: \text{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 PGW 2200 Softswitch and enter the following command to determine the MML name for the signaling service associated with the IP link(s) identified in **Step 3**:

\[
\text{prov-rtrv:iplnk:name=} \ \text{ip\_link}
\]

Where: \text{ip\_link} — The MML name for an IP link(s) identified in **Step 3**.

The system returns a message similar to the following:

\[
\begin{align*}
\text{Media Gateway Controller 2000-06-08 13:49:53} \\
\text{M RTRV} \\
\text{ "session=active:iplnk"} \\
\text{/*} \\
\text{NAME = bh531-31} \\
\text{DESC = IP link-backhaul svc mgx8260 EAST} \\
\text{SVC = bh531-3} \\
\text{IP = enif1} \\
\text{IPADDR = IP.Addr1} \\
\text{PORT = 7007} \\
\text{PEERADDR = 10.15.26.20} \\
\text{PEERPORT = 7007} \\
\text{PRI = 1} \\
\text{SIGSLOT = 11} \\
\text{SIGPORT = 38} \\
\text{*/}
\end{align*}
\]

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**:

\[
\text{rtrv-dest:sig\_serv}
\]

Where \text{sig\_serv} is the MML name for a signaling service identified in **Step 5**.
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Resolving Bearer Channel Connection Problems

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. See 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. See 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 3-64.

**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 3-65.

---

**Unblocking CICs**

You may need to unblock a CIC or a range of CICs on your Cisco PGW 2200 Softswitch. 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 PGW 2200 Softswitch, start an MML session and enter the following command:

```
unblk-cic: sig_svc:CIC=number
```

Where:

- `sig_svc`—The MML name of the signaling service 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 signaling service called ss7svc1, you would enter the following command:

```
unblk-cic:ss7svc1:CIC=2
```

To unblock a range of CICs, log in to your active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command:

```
unblk-cic: sig_svc:CIC=number,RNG=range
```

Where:

- `sig_svc`—The MML name of a signaling service 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`—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.

The Cisco PGW 2200 Softswitch 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, use of the `range` option causes individual supervision messages to be issued for each CIC in the range, instead a single group supervision message.

For example, to unblock CIC number 1 through 20, which are associated with a signaling service called ss7svc1, you would enter the following command:

```
unblk-cic:ss7svc1:cic=1,rng=19
```

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 3-15. If the CIC(s) are still blocked, proceed to the “Resetting CICs” section on page 8-134.

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 8-134.

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) using the `reset-cic` MML command.
Resolving Bearer Channel Connection Problems

Note: The \texttt{reset-cic} MML command is not supported for signaling services that use variants of the BTNUP protocol.

To reset a single CIC, log in to your active Cisco PGW 2200 Softswitch, start an MML session and enter the following command:

\texttt{reset-cic:sig\_srv:CIC=number}

Where:
- \textit{sig\_srv}—The MML name of the signaling service associated with the CICs to be reset.
- \textit{number}—The number of the affected CIC.

For example, to reset CIC number 2, which is associated with a signaling service called ss7svc1, you would enter the following command:

\texttt{reset-cic:ss7svc1:CIC=2}

To reset a range of CICs, log in to your active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command:

\texttt{reset-cic:sig\_srv:CIC=number,RNG=range}

Where:
- \textit{sig\_srv}—The MML name of a signaling service associated with the CICs you want to reset.
- \textit{number}—The number of the first CIC in the range of CICs you want to reset.
- \textit{range}—A number such that \textit{number+range} is the number of the last CIC in the range of affected CICs. All CICs between \textit{number} and \textit{number+range} are displayed.

Note: The Cisco PGW 2200 Softswitch 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, use of the \textit{range} option causes individual supervision messages to be issued for each CIC in the range, instead of a single group supervision message.

For example, to reset CICs number 1 through 20, which are associated with a signaling service called ss7svc1, you would enter the following command:

\texttt{reset-cic:ss7svc1:cic=1,rng=19}

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 3-15. If the CIC(s) are still blocked, proceed to the “Resolving Stuck CICs” section on page 8-135.

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 \texttt{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 PGW 2200 Softswitch and the call state for the associated span and bearer channel (also known as timeslot) on the media gateway.
Resolving Bearer Channel Connection Problems

Chapter 8   Troubleshooting the Cisco PGW 2200 Softswitch Platform

The Cisco PGW 2200 Softswitch is capable of automatically detecting and terminating stuck CICs. 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 PGW 2200 Softswitch match the associated states for the spans and bearer channels on the media gateway. If the audit finds that the Cisco PGW 2200 Softswitch 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 8-136.

**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, see the *Cisco PGW 2200 Softswitch Release 9 Software Installation and Configuration Guide*. For more information on CDRs, see the *Cisco PGW 2200 Softswitch Release 9 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 PGW 2200 Softswitch.

**Note**

The audit cron job is not run by the system when the call engine’s CPU load is greater than the limit set in the XECfgParm.dat file. For more information on XECfgParm.dat configuration, see the *Cisco PGW 2200 Softswitch Release 9 Software Installation and Configuration Guide*.

**Manually Resolving Stuck CICs**

If you want to manually resolve stuck CICs, perform the following steps:

**Step 1**

If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**

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 8-85.

**Step 3**

Perform a call state audit, using the procedure described in the “Auditing Call States” section on page 8-139.

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:

```
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 4. Otherwise, proceed to Step 16.
**Step 4**  
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:  

CP_ERR_AUEP:Audit:failed to audit end point nassvc1[00140001]/0/2  

CP_ERR_AUEP:Audit:failed to audit end point sigsrv1[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 (nassvc1 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 signaling service associated with the affected CIC (sigsrv1 in the example).  
- The internal hexadecimal code associated with the identified signaling service (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 5**  
Convert the hexadecimal values for the span, bearer channel, and CIC into decimal values.  

**Step 6**  
Using the information gathered in steps 4 and 5, stop the call on an affected CIC for its associated signaling service, using the procedure described in the “Stopping Calls on CICs” section on page 8-142.  

**Step 7**  
Using the information gathered in steps 4 and 5, 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 8-141.  

**Step 8**  
Reset the affected CIC using the procedure in the “Resetting CICs” section on page 8-134.  

**Step 9**  
Repeat steps 3 through 8, 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 10**  
Repeat steps 3 and 4, 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 11. Otherwise, proceed to Step 14.  

**Step 11**  
Forcefully end the call on the signaling services and CICs identified in Step 4 by entering the following command:  

\[kill-call:sig_srv:cic=num,confirm\]
Chapter 8    Troubleshooting the Cisco PGW 2200 Softswitch Platform

Resolving Bearer Channel Connection Problems

Caution

The kill-call MML command forcibly ends calls locally. It does not send any 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 reset-cic or stp-call MML commands.

Where:

- sig_srv—MML name of the signaling service identified in Step 4.
- num—Number of the stuck CIC identified in Step 4.

For example, to forcefully stop a call on CIC 215, which is associated with a signaling service called sigsrv1, you would enter the following command:

```
kill-call:sigsrv1:cic=215,confirm
```

Repeat this step for each CIC you have identified as being stuck.

**Step 12**

Forcefully end the call on the signaling service, spans, and bearer channels identified in Step 4 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 any 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 reset-cic or stp-call MML commands.

Where:

- sig_srv—MML name of the signaling service identified in Step 4.
- span_num—Number of the span identified in Step 4.
- bear_chan—Number of the stuck bearer channel identified in Step 4.

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 13**

Repeat steps 3 and 4, 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 14. If these CICs are still stuck, proceed to Step 15.

**Step 14**

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 8-85.

**Step 15**

Perform a call trace as described in “Performing a Call Trace” section on page 8-151.

**Step 16**

Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.
Auditing Call States

To run a call state audit, which compares the call states of the CICs on the Cisco PGW 2200 Softswitch with the associated states of the spans and bearer channels on the media gateway, perform the following steps:

Step 1 If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Log in to the active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command:

```
sta-aud
```

Note The Cisco PGW 2200 Softswitch 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.

Step 3 View the active system log file as described in the “Viewing System Logs” section on page 8-83. 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. See the “Obtaining Documentation and Submitting a Service Request” section on page xx for more information about contacting the Cisco TAC.

Step 4 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:

- Stopping Calls on a Cisco PGW 2200 Softswitch, page 8-139
- Stopping Calls on a Media Gateway, page 8-140
- Stopping Calls on a Trunk Group, page 8-140
- Stopping Calls on a Signaling Service, page 8-140
- Stopping Calls on Spans, page 8-141
- Stopping Calls on CICs, page 8-142

Stopping Calls on a Cisco PGW 2200 Softswitch

To stop all active calls on all traffic channels on a Cisco PGW 2200 Softswitch, log in to the active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command:

```
stp-call: mgc,confirm
```

Where `mgc` is the MML name of the desired Cisco PGW 2200 Softswitch.
Resolving Bearer Channel Connection Problems

For example, to stop all active calls on all traffic channels on a Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch, 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,confirm
```

### 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 PGW 2200 Softswitch, 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.

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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch.
- For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco PGW 2200 Softswitch.
For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco PGW 2200 Softswitch over IP (that is, FE box<sig/tdm->media gateway<NI2/IP->Cisco PGW 2200 Softswitch).

- 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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco PGW 2200 Softswitch.
  - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco PGW 2200 Softswitch over IP (that is, FE box<sig/tdm->media gateway<NI2/IP->Cisco PGW 2200 Softswitch).
  - 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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco PGW 2200 Softswitch.
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Resolving Bearer Channel Connection Problems

- For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco PGW 2200 Softswitch over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP->Cisco PGW 2200 Softswitch).
- Signaling service or routeset associated with a DPC.
- EISUP signaling service.

- $x$—A 16-bit value that identifies an ISDN/PRI physical cable.
- $y$—A numeric value that identifies the non-ISUP bearer channel number.
- $\text{range}$—A value such that $y + \text{range}$ is a valid bearer channel number. The administrative state for all bearer channels between $y$ and $y + \text{range}$ 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 PGW 2200 Softswitch, start an MML session, and enter the following command:

stp-call:$\text{sig\_srv}$:cic=$\text{number}$[,rng=$\text{range}$],confirm

Where:

- $\text{sig\_srv}$ 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 PGW 2200 Softswitch.
  - For in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco PGW 2200 Softswitch.
  - For in-band TDM signaling up to the media gateway and then converted to NI2 and sent to the Cisco PGW 2200 Softswitch over IP (that is, FE box<-sig/tdm->media gateway<-NI2/IP->Cisco PGW 2200 Softswitch).
  - Signaling service or routeset associated with a DPC.
  - EISUP signaling service.
- $\text{number}$—A valid CIC number.
- $\text{range}$—A value such that $y + \text{range}$ is a valid bearer channel number. The administrative state for all bearer channels between $y$ and $y + \text{range}$ 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 PGW 2200 Softswitch. The procedure to audit an MGCP media gateway is described in the following sections:
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 PGW 2200 Softswitch 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 8-143.

To run an audit on a single MGCP media gateway, log on to the active Cisco PGW 2200 Softswitch, 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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch, 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
*MCP-MGC1: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
```
Resolving Bearer Channel Connection Problems

The response indicates whether the audit has passed or failed. If the audit has failed, see 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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch, start an MML session, and enter the following command:

```
tst-cot: sig_srv:cic=number
```

Where:
- `sig_srv`—The MML name of the signaling service 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 signaling service named sigsrv1, you would enter the following command:

```
tst-cot: sigsrv1: cic=5
```

If the manual COT test should fail, verify the COT settings for the Cisco PGW 2200 Softswitch and the associated media gateway, as described in the “Verifying Continuity Test Settings” section on page 8-144.

Verifying Continuity Test Settings

**Step 1**
If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**
Verify that the COT properties for the associated SS7 signaling service or trunk group are correct by logging in to the active Cisco PGW 2200 Softswitch, 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
MRTRV
*session=active:sigsvcprop*
/*
adjDestinations = 16
AlarmCarrier = 0
BothwayWorking = 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 3** If your settings for the highlighted properties match what is displayed above, proceed to Step 6. Otherwise, you must modify the COT settings on your Cisco PGW 2200 Softswitch. To begin modifying the COT settings, start a provisioning session as described in the “Starting a Provisioning Session” section on page 3-64.

**Step 4** Enter the following command to modify the COT settings on your Cisco PGW 2200 Softswitch:

```
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 5** Save and activate your changes as described in the “Saving and Activating your Provisioning Changes” section on page 3-65.

**Step 6** 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. See 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 7.
Step 7 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Ping the affected Cisco PGW 2200 Softswitch link from the associated media gateway, using the following UNIX command:

```
ping link_addr
```

Where `link_addr` is the IP address of the affected Cisco PGW 2200 Softswitch link.

Repeat this step if the second link for the destination is also out-of-service.

If the links are unreachable, proceed to Step 10. Otherwise, proceed to Step 3.

Step 3 If the path between the Cisco PGW 2200 Softswitch and the media gateway is defined using an MGCP signaling service, proceed to Step 4. If the path between the Cisco PGW 2200 Softswitch 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. See the documentation associated with the media gateway for more information.

If the MGCP interface on your media gateway is working properly, proceed to Step 10. 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, see 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. See 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. See 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. See 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 PGW 2200 Softswitch using the `debug` command. See the documentation associated with the media gateway for more information.
If RLM messages are being acknowledged by the Cisco PGW 2200 Softswitch, proceed to Step 10. Otherwise, proceed to Step 9.

**Step 9**
Verify that the configuration for RLM on the Cisco PGW 2200 Softswitch matches the configuration on the media gateway. To display the configuration of the IP links on the Cisco PGW 2200 Softswitch, enter the following MML command at the active Cisco PGW 2200 Softswitch:

```
prov-rtrv:iplnk:"all"
```

The system returns a response similar to the following:

```
MGC-02 - Media Gateway Controller 2001-07-26 12:57:48
MRTRV
"session=active:iplnk"
/*

<table>
<thead>
<tr>
<th>NAME</th>
<th>SVC</th>
<th>IF</th>
<th>IF</th>
<th>NEXTHOP</th>
<th>NETMASK</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEERADDR</td>
<td>PEERPORT</td>
<td>PRI</td>
<td>SIGSLOT</td>
<td>SIGPORT</td>
<td>PORT</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
<td>---------</td>
<td>------</td>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>va-5300-202-1</td>
<td>va-5300-202</td>
<td>enif1</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0 255.255.255.255</td>
</tr>
<tr>
<td>172.24.200.19</td>
<td>3001</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0 255.255.255.255</td>
</tr>
<tr>
<td>va-5300-202-2</td>
<td>va-5300-202</td>
<td>enif1</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0 255.255.255.255</td>
</tr>
<tr>
<td>172.24.200.19</td>
<td>3001</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0 255.255.255.255</td>
</tr>
<tr>
<td>va-5300-203-1</td>
<td>va-5300-203</td>
<td>enif1</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0 255.255.255.255</td>
</tr>
<tr>
<td>172.24.200.20</td>
<td>3001</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0 255.255.255.255</td>
</tr>
<tr>
<td>va-5300-203-2</td>
<td>va-5300-203</td>
<td>enif1</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0 255.255.255.255</td>
</tr>
<tr>
<td>172.24.200.20</td>
<td>3001</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0.0.0.0 255.255.255.255</td>
</tr>
</tbody>
</table>

*/
```

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, see the documentation for your media gateway for more information. If the changes need to be made on the Cisco PGW 2200 Softswitch, start a dynamic reconfiguration session to make your changes, as described in the “Invoking Dynamic Reconfiguration” section on page 3-66.

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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

**Calls Fail at the Cisco PGW 2200 Softswitch**

If calls appear to be failing at the Cisco PGW 2200 Softswitch, and the calls are not appearing on the associated media gateway, perform the following steps:

**Step 1**
If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**
Debug the interface on the media gateway associated with the Cisco PGW 2200 Softswitch. If your system is configured for signaling, the interface is Q.931. If your system is configured for call control, the interface is MGCP. See 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 3. Otherwise, resolve the problems with the interface as described in the documentation for the associated media gateway.
Resolving Bearer Channel Connection Problems

Step 3 Verify that the signaling channels are in-service, as described in the “Verifying the Status of all Signaling Services” section on page 3-9.

If any of the signaling channels are out-of-service, attempt to bring them into service using the appropriate procedures. Otherwise, proceed to Step 4.

Step 4 Run a call trace as described in the “Performing a Call Trace” section on page 8-151.

Step 5 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

3.1 KHz (ISDN Category 3) Calls are Failing

If 3.1 KHz calls (also known as ISDN category 3 calls) are failing, perform the following steps:

Note The following procedure is valid only if your Cisco PGW 2200 Softswitch is using the BTNUP protocol.

Step 1 If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 If your system is configured for the BTNUP protocol, proceed to Step 3. Otherwise, proceed to Step 7.

Step 3 Verify the setting for the defaultBC property on the trunk group associated with the failed calls by entering the following MML command at the active Cisco PGW 2200 Softswitch:

```
prov-rtrv:trnkgrpprop:name="trnkgrpname"
```

Where `trnkgrpname` is the MML name of the trunk group associated with the failed calls.

The system returns a response listing the values of all of the properties for the specified trunk group. The defaultBC property should be set to 3_1_KHZ to ensure proper processing of 3.1 KHz calls. If the defaultBC property is set to 3_1_KHZ, proceed to Step 7. Otherwise, proceed to Step 4.

Note Setting the defaultBC property changes the identifying information for incoming 3.1 KHz (ISDN category 3) calls to match the settings for speech (ISDN category 2) calls. This change allows these calls to be processed by far-end switches that ordinarily reject 3.1 KHz calls.

Step 4 Start a provisioning session as described in the “Starting a Provisioning Session” section on page 3-64.

Step 5 Modify the appropriate signaling service settings using the following command:

```
prov-ed:trnkgrpprop:name="trnkgrpname",defaultBC="3_1_KHZ"
```

Where `trnkgrpname` is the MML name for the affected trunk group.

Step 6 Save and activate your new configuration as described in the “Saving and Activating your Provisioning Changes” section on page 3-65.

If your system now completes 3.1 KHz calls, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Calls are Misrouting

If your calls are misrouting, you may have a problem with your dial plan or routing data. To identify the source of the problem and resolve it, perform the following steps:

Step 1 If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Perform a diagnostic trace of your dial plan and routing data using the translation verification viewer, as described in the “Using the Translation Verification Viewer” section on page 3-134.

If the diagnostic trace does not reveal any configuration errors in your dial plan or routing data, proceed to Step 8. Otherwise, proceed to Step 3 to correct the configuration errors.

Step 3 Correct your dial plan and/or routing data as indicated in the output of the translation verification viewer and proceed to Step 7.

Note The MML commands to be used to correct the data differ based on the elements of the configuration to be changed. For more information on the appropriate MML commands for changing the configuration of individual dial plan and routing data elements, see the Cisco PGW 2200 Softswitch Release 9.8 Dial Plan Guide.

If the call that is misrouting is an MGCP dial call, the value for the MGCPDIALPKG result type could be incorrect. To correct the value of the MGCPDIALPKG result type, proceed to Step 4.

Step 4 Verify the current setting of the MGCPDIALPKG result type using the following MML command:

```
numan-rtrv:resulttable:custgrpid="group_number",name="result_name",resulttype="MGCPDIALPKG",SETNAME="set_name"
```

Where:
- `group_number`—Customer group identification number associated with the affected dial plan.
- `result_name`—Result name associated with the affected dial plan.
- `set_name`—Name of the set associated with the affected MGCP dial plan.

If the setting is not correct, proceed to Step 5. Otherwise, proceed to Step 8.

Step 5 Change the MGCPDIALPKG settings using the following MML command:

```
numan-ed:resulttable:custgrpid="group_number",name="result_name",resulttype="MGCPDIALPKG",SETNAME="set_name" DW1="call_type" DW2="x"
```

Where:
- `group_number`—Customer group identification number associated with the affected dial plan.
- `result_name`—Result name associated with the affected dial plan.
- `set_name`—Name of the set associated with the affected MGCP dial plan.
- `call_type`—Call type for the MGCP calls. Valid values are digital, analog, and dynamic.
Resolving SIP Communication Problems

The Cisco PGW 2200 Softswitch software can be used for SIP communications. The procedures dealing with resolving problems on signaling channels and bearer channels cover most of the steps you would need to take to resolve a SIP communication problem. The section below is a SIP-specific procedure.

Stopping SIP-to-SIP Calls

Cisco PGW 2200 Softswitch software can control SIP-to-SIP calls. To stop a particular SIP-to-SIP call, log in to the active Cisco PGW 2200 Softswitch, start an MML session, and enter the following command:

```
kill-call:sip_sig_srv:cid="name",confirm
```

Where:
- `sip_sig_srv`—The MML name for the SIP signaling service associated with the SIP-to-SIP call.
- `name`—The SIP call identification name. This can be obtained using the `rtrv-sip` MML command, as described in the “Retrieving SIP Call Information” section on page 3-61.

For example, the following MML command stops a SIP-to-SIP call on a SIP signaling service called `sip_svc1`:

```
kill-call:sip_svc1:cid="ccdd33ee-423fde3d-55438954-10172.22.119.215",confirm
```

Tracing

Tracing on the Cisco PGW 2200 Softswitch is described in the following sections:
- Performing a Call Trace, page 8-151
- Alternatives to Call Tracing, page 8-160
Performing a Call Trace

After checking all physical connections, signal links, bearer channels, and destinations, the person who is troubleshooting the Cisco PGW 2200 Softswitch 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 8-151
- Starting A Call Trace (on Release 9.7(3) Patch 8), page 8-153
- Stopping A Call Trace, page 8-156
- Retrieving Names of Open Call Trace Files, page 8-156
- Viewing the Call Trace, page 8-157
- Deleting Call Trace Files, page 8-158
- Understanding the Call Trace, page 8-158

Starting A Call Trace

To start the call trace, perform the following steps:

1. **Step 1** Log in to the active Cisco PGW 2200 Softswitch, 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_yyyymmdhhmmss.btr`
   - For `sta-sc-trc:trkgrp:confirm` the filename is:
Tracing

The filename (yyyyymmddhhmmss.btr) 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.
- span—The span ID, an integer value denoting the traffic channel for the sig_path (NFAS only).
- rng—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.
- tc—The traffic channel of interest in integer form.
- trk—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.

   \texttt{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.

   \texttt{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.

   \texttt{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.

   \texttt{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.

\[ \text{sta-sc-trc}: \text{trkgrp}::\text{trk}=w \]

**Note** See the *Cisco PGW 2200 Softswitch Release 9 MML Command Reference* for detailed information on using the `sta-sc-trc` command.

---

**Starting A Call Trace (on Release 9.7(3) Patch 8)**

You can perform advanced call traces starting from Cisco PGW 2200 Softswitch Release 9.7(3) Patch 8. The advanced call trace is based on the existing call trace function and adds the calling party number, the called party number, the MCL (Machine Congestion Level) setting, the cause value, and the call duration as call trace criteria. This enhancement makes the call trace more accurate and reduces system performance impacts on the Cisco PGW 2200 Softswitch when the Cisco PGW 2200 Softswitch is performing call traces.

To start the call trace, perform the following steps:

---

**Step 1**

Log in to the active Cisco PGW 2200 Softswitch, start an MML session, and enter the command.

This command can be entered in either of the following two formats:

\[ \text{sta-sc-trc:<sig_path>:[span=x,[rng=y]][,tc=z[,rng=w]][,anubmer=\text{"calling party number"}][,bnumber=\text{"called party number"}][,causevalue=c][,incompleteoverlapnumber][,\text{duration=d}][,mcl=m][,autostop][,prd=n][,log=\text{"log"}],confirm} \]

\[ \text{sta-sc-trc:<trunkgroup>:}[\text{trk=x,[rng=y]}][,anubmer=\text{"calling party number"}][,bnumber=\text{"called party number"}][,causevalue=c][,incompleteoverlapnumber][,\text{duration=d}][,mcl=m][,autostop][,prd=n][,log=\text{"log"}],confirm} \]

**Table 8-3** provides a parameter list for this `sta-sc-trc` MML command.
### Table 8-3 Parameter List of the MML Command sta-sc-trc

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
<th>Parameter Category</th>
<th>Parameter Combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>sig_path</td>
<td>See the section, “Starting A Call Trace, page 8-151”.</td>
<td>Trace location</td>
<td>Possible combinations:</td>
</tr>
<tr>
<td>span</td>
<td>See the section, “Starting A Call Trace, page 8-151”. This parameter is used with the parameter “rng” and “sig_path”.</td>
<td></td>
<td>• sig_path:[span=x[,rng=y][,tc=w[,rng=z]]]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• trunkgroup:[trk=x[,rng=y]]</td>
</tr>
<tr>
<td>rng</td>
<td>See the section, “Starting A Call Trace, page 8-151”.</td>
<td></td>
<td>Note If “sig_path” is present, all span/CICs at this sigpath will be traced. If “sig_path” and “span” are present, all CICs at this sig_path/span will be traced. If “trunkgroup” is present, all trunks in this trunk group will be traced.</td>
</tr>
<tr>
<td>tc</td>
<td>See the section, “Starting A Call Trace, page 8-151”. This parameter is used with the parameter “rng”, “span”, and “sig_path”.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>trunkgroup</td>
<td>See the section, “Starting A Call Trace, page 8-151”.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>trk</td>
<td>See the section, “Starting A Call Trace, page 8-151”. This parameter is used with the parameter trunkgroup and rng.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rng</td>
<td>See the above “rng”.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>anumber</td>
<td>The original calling party number up to 32 digits. Allowed digits are 0123456789abcdefABCDEF*. The wildcard &quot;]*&quot; at the end is supported.</td>
<td>Call trace trigger</td>
<td>Optional parameters. If more than one call trace trigger parameters are present, the system collects the call trace when all these conditions are met.</td>
</tr>
<tr>
<td>bnumber</td>
<td>The original calling party number up to 32 digits. Allowed digits are 0123456789abcdefABCDEF*. The wildcard &quot;]*&quot; at the end is supported.</td>
<td></td>
<td>Note If none of these trigger parameter is present, this command is used in the legacy way which is described in Starting A Call Trace, page 8-151”.</td>
</tr>
<tr>
<td>causevalue</td>
<td>The internal cause value for the release message. Valid values are from 1 to 300.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>incompleteoverlapnumber</td>
<td>The indicator to collect incomplete-number overlap call traces. These calls are failed calls with incomplete numbers.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>duration</td>
<td>The call duration. It is measured in seconds. Valid values are from 3600 to 2147483. This parameter value must be set less than “prd” in the presence of the parameter “prd”. If the call duration of the call is greater than “prd”, the trace criterion is met and the system stops the call trace. At the same time, the system adds one new parameter CallNumberToWriteIntoTracefile in the file XECfgParm.dat to limit the number of calls (default: 200) that are included in the trace file.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 8-3 Parameter List of the MML Command sta-sc-trc

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
<th>Parameter Category</th>
<th>Parameter Combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>mcl</td>
<td>The machine congestion level. Valid values are integer from 0 to 3. Default value is 1. Where 0: Do not stop the call trace when MCL occurs. 1: Stop the call trace when the MCL reaches MCL1. 2: Stop the call trace when the MCL reaches MCL2. 3: Stop the call trace when the MCL reaches MCL3.</td>
<td>Stop condition</td>
<td>Optional parameters. If more than one stop condition parameters are present, the system stops the call trace when any one of these stop conditions is met.</td>
</tr>
<tr>
<td>autocall</td>
<td>The indicator to stop the call trace when one trace (for example, all input trace criteria are matched) is collected. This parameter is unavailable in the presence of the parameter &quot;duration&quot; or in the absence of all the other parameters.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>prd</td>
<td>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 the trace is stopped automatically.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>log</td>
<td>See the section, “Starting A Call Trace, page 8-151”.</td>
<td>Other parameters</td>
<td></td>
</tr>
<tr>
<td>confirm</td>
<td>See the section, “Starting A Call Trace, page 8-151”.</td>
<td>Mandatory</td>
<td></td>
</tr>
</tbody>
</table>

The following paragraphs present examples of possible command variations:

1. Use the following command to trace the call with the calling number 7300 and the called number 7000 at the sigpath ss7svc6:
   
   `sta-sc-trc:ss7svc6,anumber="7300",bnumber="7000",confirm`

2. Use the following command to trace the call with the calling number 7300 at the sigpath ss7svc6. Stop the call trace when the required call trace is collected:
   
   `sta-sc-trc:ss7svc6,anumber="7300",autostop,confirm`

3. Use the following command to trace the call at the sigpath ss7svc6 with CIC range from 22 to 30. Stop the call trace when the MCL reaches MCL2:
   
   `sta-sc-trc:ss7svc6,span=65535,tc=22,rng=8,mcl=2,confirm`

4. Use the following command to trace the call with the internal cause value 44 at the sigpath ss7svc6:
   
   `sta-sc-trc:ss7svc6,causevalue=44,confirm`

5. Use the following command to trace the failed call whose overlap flag is set and the called number is incomplete at the sigpath ss7svc6:
   
   `sta-sc-trc:ss7svc6,bnumber="7000",incompleteoverlapnumber,confirm`
6. Use the following command to start a twelve-hour call trace of the call with duration longer than three hours in the trunk group tg-6006:

```
stp-sc-trc:tg-6006,duration=10800,prd=43200,confirm
```

**Note** On a standby Cisco PGW 2200 Softswitch, you can use the following two commands to perform call traces.

```
stp-sc-trc:<sig_path>:<span=x[,rng=y][,tc=z[,rng=w]]][,mcl=m][,prd=n][,log="log"],confirm
```

```
stp-sc-trc:<trunkgroup>:<trk=x[,rng=y]][,mcl=m][,prd=n][,log="log"],confirm
```

**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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch, 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"
```
Starting from Cisco PGW 2200 Softswitch Release 9.7(3) Patch 8, you can use the following command to retrieve the stop reason of the last trace file.

```
rtrv-sc-trc::stopreason
```

The call trace stops for one of the following four reasons.

- **The call trace is stopped because the MCL is reached.**
  ```
  MG0C-02 - Media Gateway Controller 2008-04-28 10:25:36.782 EDT
  M RTRV
  "../var/trace/eisup-0428_eisup-pgw2_20080427223536.btr: MCL reached.
  "
  ;
  ```

- **The call trace is automatically stopped and the desired call trace is collected.**
  ```
  MG0C-02 - Media Gateway Controller 2008-04-30 14:39:19.042 CST
  M RTRV
  "../var/trace/_ss7svc1_20080430143908.btr: automatically stopped.
  "
  ;
  ```

- **The call trace is stopped manually.**
  ```
  MG0C-02 - Media Gateway Controller 2008-04-30 14:39:59.849 CST
  M RTRV
  "../var/trace/_ss7svc1_20080430143951.btr: manually stopped.
  "
  ;
  ```

- **The call trace is stopped because the trace period is over.**
  ```
  MG0C-02 - Media Gateway Controller 2008-04-30 14:43:59.982 CST
  M RTRV
  "../var/trace/_ss7svc1_20080430144354.btr: trace period expired.
  "
  ;
  ```

### 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 8-151, and the Cisco PGW 2200 Softswitch 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, see the “Using the Trace Viewer” section on page 3-134.

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. For more information on the less utility, enter the UNIX command `man less` on your 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, see the “Understanding SimPrint” section on page 8-160.
- **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 information on .trc files, see the “Understanding Trace Files” section on page 8-159.
- **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, see the “Understanding the Conversion Analyzer” section on page 8-159.
- **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 8-165.

### Understanding the Call Trace

Call traces record information in a trace file that shows how the Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch to see where it fails.

The trace output is in binary format. It shows:

- The PDU that the Cisco PGW 2200 Softswitch receives
- How the Cisco PGW 2200 Softswitch decodes the PDU
- The PDU that the Cisco PGW 2200 Softswitch 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 cmdgCall” message for the next “end cmdgCall” 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 PGW 2200 Softswitch 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 PGW 2200 Softswitch 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 PGW 2200 Softswitch. This is why the conversion from a .btr file to a .trc file is usually done on the Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch 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 PGW 2200 Softswitch.
- **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 PGW 2200 Softswitch 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
If the hung call is a SIP-to-SIP call, proceed to Step 3. Otherwise, proceed to Step 2.

Step 2
Log in to the active Cisco PGW 2200 Softswitch and enter the following command:

```plaintext
prt-call: sig_path; cic=number [,log="xyz"]
```

or

```plaintext
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 the Cisco PGW 2200 Softswitch.
  - Signaling path of in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco PGW 2200 Softswitch.
  - Signaling path of in-band TDM signaling up to NAS and then converted to NI2 and sent to the Cisco PGW 2200 Softswitch over IP (that is, FE box<-sig/tdm->NAS<-NI2/IP->Cisco PGW 2200 Softswitch).
  - Signaling path or routeset associated with an 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`—An optional parameter that names the 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 service called dms100-pc using a CIC of 124:

```plaintext
prt-call: dms100-pc; cic=124
```

Proceed to Step 4.

Step 3
Log in to the active Cisco PGW 2200 Softswitch and enter the following command:

```plaintext
prt-call: sig_path; cid="name" [,log="xyz"]
```

Where:

- `sig_path`—The MML name for the signaling service associated with the SIP-to-SIP call.
- `name`—The SIP call identification name. This can be obtained using the `rtrv-sip` MML command, as described in the “Retrieving SIP Call Information” section on page 3-61.
Tracing

- **xyz**—An optional parameter that names the 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 particular call on a SIP signaling service called sip_svc1:

```
prt-call:sip_svc1:cid="ccdd33ee-423fdedd-55438954-10172.22.119.215"
```

**Step 4**
Change directories to access the log file by entering the following command:
```
cd /opt/CiscoMGC/var/trace
```

**Step 5**
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 PGW 2200 Softswitch, start an MML session, and enter the following command:

```
sta-abn-trc:sig_path|all[,log=xyz] [,prd=],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 PGW 2200 Softswitch.
  - Signaling path of in-band TDM signaling up to CU and then encapsulated and sent over IP to the Cisco PGW 2200 Softswitch.
  - Signaling path of in-band TDM signaling up to NAS and then converted to NI2 and sent to the Cisco PGW 2200 Softswitch over IP (that is, FE box<-sig/tdm->NAS<-NI2/IP->Cisco PGW 2200 Softswitch).
  - 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 PGW 2200 Softswitch, 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.
Tracing

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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch, 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 PGW 2200 Softswitch, starting an MML session, and entering the following command:

```
stc-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 8-83. 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 PGW 2200 Softswitch platform:

- Verifying Cisco PGW 2200 Softswitch Ethernet Operation, page 8-164
- Deleting Unnecessary Files to Increase Available Disk Space, page 8-165
- Recovering from a Switchover Failure, page 8-166
- Recovering from Cisco PGW 2200 Softswitch(es) Failure, page 8-167
- Restoring Stored Configuration Data, page 8-172
- Restoring a Backup File from a Device, page 8-174
- Configuration Export Failed Due to MMDB, page 8-175
- Measurements Are Not Being Generated, page 8-176
- Call Detail Records Are Not Being Generated, page 8-176
- Resolving a Failed Connection to a Peer, page 8-177
- Rebooting Software to Modify Configuration Parameters, page 8-178
- Diagnosing SNMP Failure, page 8-179
- Correcting the System Time, page 8-180
- Securing your Network, page 8-182
- TIBCO Interface Not Working, page 8-190
- Installing the License File, page 8-192
- Replacing a Failed Disk, page 8-192

---

**Verifying Cisco PGW 2200 Softswitch Ethernet Operation**

See the documentation provided by Sun Microsystems for more information on verifying the proper functioning of the Ethernet connections on your Cisco PGW 2200 Softswitch.
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 PGW 2200 Softswitch. The following procedure steps you through the process of deleting all three file types.

**Step 1**
Log in to the active Cisco PGW 2200 Softswitch 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, see 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 3-127. 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 3-127.
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 PGW 2200 Softswitch is unavailable to process calls and a critical alarm occurs on the active Cisco PGW 2200 Softswitch.

To recover from a switchover failure, complete the following steps:

Step 1  If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Log in to the active Cisco PGW 2200 Softswitch, start an MML session, and view the current alarms, as described in the “Retrieving All Active Alarms” section on page 8-3.

Step 3  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 4  See the “Alarm Troubleshooting Procedures” section on page 8-4 for descriptions of the steps necessary to resolve the critical alarm that caused the switchover attempt.

Step 5  Log in to the standby Cisco PGW 2200 Softswitch, start an MML session, and view the current alarms, as described in the “Retrieving All Active Alarms” section on page 8-3.

Step 6  Resolve the listed alarm(s). See the “Alarm Troubleshooting Procedures” section on page 8-4 for descriptions of the steps necessary to resolve the alarm(s).

If resolving the alarms does not stabilize the standby Cisco PGW 2200 Softswitch, proceed to Step 7.

Step 7  Generate a ping from the active Cisco PGW 2200 Softswitch to the standby Cisco PGW 2200 Softswitch by entering the following UNIX command at the active Cisco PGW 2200 Softswitch:

```
ping standby_addr
```

Where `standby_addr` is the IP address of the standby Cisco PGW 2200 Softswitch.

If the ping fails, proceed to Step 8. Otherwise, proceed to Step 9.

Step 8  Verify the Ethernet interfaces between the active Cisco PGW 2200 Softswitch and the standby Cisco PGW 2200 Softswitch. See the Sun Microsystems documentation that came with your system for more information.

If an element of the Ethernet interfaces between the active Cisco PGW 2200 Softswitch and the standby Cisco PGW 2200 Softswitch is found to be faulty, replace it. Otherwise, proceed to Step 9. See 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 9.

Step 9  Verify that the host name for each Cisco PGW 2200 Softswitch is unique. To do this, log on as root to each Cisco PGW 2200 Softswitch and view the contents of the host file in the /etc directory. If a Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch.
Step 10  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
- *.Virtual_IP_Addr

If the IP address settings are correct, proceed to Step 11. Otherwise, update the IP address parameters for each host, using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 11.

Step 11  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 = 1000

If the foverd settings are correct, proceed to Step 12. Otherwise, update the foverd settings in the XECfgParm.dat files using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 12.

Step 12  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

 Recovering from Cisco PGW 2200 Softswitch(es) 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 PGW 2200 Softswitch or failed Cisco PGW 2200 Softswitches. (for example, if the Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch. For more information on backing up your Cisco PGW 2200 Softswitch, see the “Backing Up System Software” section on page 3-28.
Successful recovery from a natural or man-made disaster depends upon your planning in advance for a possible disaster. See the “Creating a Disaster Recovery Plan” section on page 3-28 for more information.

The following sections contain the procedures that describe how to recover from Cisco PGW 2200 Softswitch failure:

- Recovering from a Cisco PGW 2200 Softswitch Failure in a Simplex System, page 8-168
- Recovering from a Single Cisco PGW 2200 Softswitch Failure in a Continuous Service System, page 8-170
- Recovering from a Dual Cisco PGW 2200 Softswitch Failure in a Continuous Service System, page 8-171

**Recovering from a Cisco PGW 2200 Softswitch Failure in a Simplex System**

To recover from a Cisco PGW 2200 Softswitch failure in a system equipped with only one Cisco PGW 2200 Softswitch, perform the following steps:

**Step 1** Reload the Solaris 10 operating system on the Cisco PGW 2200 Softswitch, as described in the *Installing the Sun Solaris 10 Operating System* chapter of the *Cisco PGW 2200 Softswitch Release 9 Software Installation and Configuration Guide*.

**Step 2** Reload the Cisco PGW 2200 Softswitch software on the Cisco PGW 2200 Softswitch, as described in the *Installing the Cisco PGW 2200 Softswitch Software* chapter of the *Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide*.

**Step 3** Restore the configuration of your Cisco PGW 2200 Softswitch from your latest backup file, as described in the “Restoring Stored Configuration Data” section on page 8-172.

**Note** If your backup files are stored on a remote server, have your network administrator re-establish the path between the Cisco PGW 2200 Softswitch and the server that stores your backups.

**Note** Any changes you made to the Cisco PGW 2200 Softswitch system subsequent to your last backup are lost.

**Step 4** Start the Cisco PGW 2200 Softswitch software, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

**Recovering from a DiskSuite Failure on the Opteron Platform**

To recover from a DiskSuite failure on the Opteron platform, perform the following steps:

**Step 1** Shut down the Cisco PGW 2200 Softswitch. See “Cisco PGW 2200 Softswitch Shutdown Procedure” section on page 2-4.

**Step 2** Remove the damaged disk, for example, Disk 1.

**Step 3** Boot up the system from Disk 2.

The system enters the maintenance mode automatically
Step 4 Enter the following command and press Enter to delete state database replicas of the damaged disk.

```
metadb -d c0t2d0s4
```

**Note** In the above command, the last parameter is the device ID of damaged disk. In this example, the device ID for that damaged disk is c0t2d0s4. You can use the command `metadb` to get the device ID of the damaged disk which is marked as unknown.

Step 5 Plug in a new disk to replace the damaged Disk 1 in the slot for Disk 1.

Step 6 Enter the following command and press Enter.

```
reboot -- -r
```

**Note** You need to change the boot sequence in the bios settings. Make sure the system boots up from Disk 2 rather than the newly inserted disk. The system enters the maintenance mode automatically.

Step 7 Enter the following command in the console and press Enter.

```
format
```

Step 8 Enter 1 to select Disk 2.

Step 9 Enter the following command in the console and press Enter to enter the partition menu.

```
partition
```

Step 10 Enter the following command to name the current partition table.

```
name
```

Step 11 Enter cisco for the current partition table name.

Step 12 Enter the following command and press Enter.

```
quit
```

Step 13 Enter the following command press Enter. This new disk/partition definitions are saved to the default file ./format.dat.

```
save
```

Step 14 Enter the following command and press Enter.

```
quit
```

Step 15 Enter the following command and press Enter.

```
format -x ./format.dat
```

Step 16 Enter 0 to select the newly inserted disk.

Step 17 Enter the following command and press Enter.

```
partition
```

Step 18 Enter the following command and press Enter.

```
select
```

Step 19 Enter 0 to specify the table number.
Step 20 Enter the following command and press Enter. A list of the current partition table is listed.

```
print
```

Step 21 Enter the following command and press Enter to label the disk.

```
label
```

Step 22 Enter y to confirm the labeling.

Step 23 Enter quit and press Enter to quit the partition operation.

Step 24 Enter quit and press Enter to quit the format operation.

Step 25 Enter the following command and press Enter.

```
metadb -a -c 3 c0t2d0s4
```

Note See Step 4 for the meaning of the last parameter.

---

Step 26 Enter the following command and press Enter to check which submirrors are failed.

```
metastat | grep metareplace
```

The list similar to the following is displayed.

```
Invoke: metareplace d12 c0t2d0s5 <new device>
Invoke: metareplace d9 c0t2d0s3 <new device>
Invoke: metareplace d6 c0t2d0s1 <new device>
Invoke: metareplace d3 c0t2d0s0 <new device>
Invoke: metareplace d15 c0t2d0s6 <new device>
```

Step 27 Enter the following commands to enable the failed submirrors according to the list generated in Step 26.

```
metareplace -e d12 c0t2d0s5
metareplace -e d9 c0t2d0s3
metareplace -e d6 c0t2d0s1
metareplace -e d3 c0t2d0s0
metareplace -e d15 c0t2d0s6
```

Step 28 Enter the following command to check data mirroring progress.

```
metastat | grep "Resync in progress"
```

Text similar to the following is displayed.

```
Resync in progress: 1% done
Resync in progress: 16% done
Resync in progress: 30% done
Resync in progress: 39% done
Resync in progress: 98% done
```

---

Recovering from a Single Cisco PGW 2200 Softswitch Failure in a Continuous Service System

To recover from a single Cisco PGW 2200 Softswitch failure in a system equipped with two Cisco PGW 2200 Softswitches, perform the following steps:
Step 1  Reload the Solaris 10 operating system on the affected Cisco PGW 2200 Softswitch, as described in the Installing the Sun Solaris 10 Operating System chapter of the Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide.

Step 2  Reload the Cisco PGW 2200 Softswitch software on the affected Cisco PGW 2200 Softswitch, as described in the Installing the Cisco PGW 2200 Softswitch Software chapter of the Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide.

Step 3  Restore the configuration of the affected Cisco PGW 2200 Softswitch from your latest backup file, as described in the “Restoring Stored Configuration Data” section on page 8-172.

Note  If your backup files are stored on a remote server, have your network administrator re-establish the path between the affected Cisco PGW 2200 Softswitch and the server that stores your backups.

Step 4  Open the XECfgParm.dat file on the affected Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch software, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

Step 8  Synchronize the databases of the active and standby Cisco PGW 2200 Softswitches, using the procedure described in the Synchronizing Databases section of the Configuring the Cisco PGW 2200 Softswitch Software Release 9.8 chapter of the Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide.

Recovering from a Dual Cisco PGW 2200 Softswitch Failure in a Continuous Service System

To recover from a dual Cisco PGW 2200 Softswitch failure in a system equipped with two Cisco PGW 2200 Softswitches, perform the following steps:

Step 1  Select one of the Cisco PGW 2200 Softswitches to be your active system, and the other to be your standby system.

Step 2  Reload the Solaris 10 operating system on the active Cisco PGW 2200 Softswitch, as described in the Installing the Sun Solaris 10 Operating System chapter of the Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide.

Step 3  Reload the Cisco PGW 2200 Softswitch software on the active Cisco PGW 2200 Softswitch, as described in the Installing the Cisco PGW 2200 Softswitch Software chapter of the Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide.

Step 4  Restore the configuration of the active Cisco PGW 2200 Softswitch from your latest backup file, as described in the “Restoring Stored Configuration Data” section on page 8-172.

Note  If your backup files are stored on a remote server, have your network administrator re-establish the path between the active Cisco PGW 2200 Softswitch and the server that stores your backups.

Step 5  Open the XECfgParm.dat file on the active Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch software on the active Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

Step 9  Reload the Solaris 10 operating system on the standby Cisco PGW 2200 Softswitch, as described in the Installing the Sun Solaris 10 Operating System chapter of the Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide.

Step 10  Reload the Cisco PGW 2200 Softswitch software on the standby Cisco PGW 2200 Softswitch, as described in the Installing the Cisco Cisco PGW 2200 Softswitch Software chapter of the Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide.

Step 11  Restore the configuration of the standby Cisco PGW 2200 Softswitch from your latest backup file, as described in the “Restoring Stored Configuration Data” section on page 8-172.

Note  If your backup files are stored on a remote server, have your network administrator re-establish the path between the standby Cisco PGW 2200 Softswitch and the server that stores your backups.

Step 12  Open the XECfgParm.dat file on the standby Cisco PGW 2200 Softswitch 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 PGW 2200 Softswitch software, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

Step 16  Synchronize the databases of the active and standby Cisco PGW 2200 Softswitches, using the procedure described in the Synchronizing Databases section of the Configuring the Cisco PGW 2200 Softswitch Software Release 9 chapter of the Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide.

Restoring Stored Configuration Data

Typically, restoration of stored configuration data is performed in severe troubleshooting situations where the Cisco PGW 2200 Softswitch is not functioning properly, due to hardware failure, natural disaster, or software corruption. The procedures in this section describe how to restore the Cisco PGW 2200 Softswitch configuration data stored either on a tape drive or on a remote network server.

There are two restoration methods available for the Cisco PGW 2200 Softswitch software, one for software releases up to 9.1(4), and another for software releases from 9.1(5) 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 PGW 2200 Softswitch Software, page 8-173
Restoring Procedures for Cisco PGW 2200 Softswitch Software

This restoration method uses a script to restore the configuration data for the Cisco PGW 2200 Softswitch software, select UNIX administrative files, and the Main Memory Database (MMDB).

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, see “Verifying the Patch Level of the Cisco PGW 2200 Softswitch” section on page 3-100.

The following sections provide the restoration procedures:

- Listing Backup Files, page 8-173
- Restoring a Backup File from a Directory, page 8-173
- Restoring a Backup File from a Device, page 8-174

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 PGW 2200 Softswitch Software” section on page 3-28.

Listing Backup Files

To list the backup files in a particular directory path, enter the following UNIX command on the Cisco PGW 2200 Softswitch:

`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
mgc_venus_20011011_153003_backup
mgc_venus_20011012_153003_backup
```

Restoring a Backup File from a Directory

To restore the configuration data stored in a particular backup file stored in a directory, enter the following UNIX command on the affected Cisco PGW 2200 Softswitch to run the restore script:

You can restore a backup file only when you are logged in to your system as `mgcusr`. You cannot restore a backup file while you are logged in as `root`.

```
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 stored in a directory path called /var/cisco, you would enter the following command:

```
mgcrestore -d /var/cisco -f mgc_venus_20011012_153003_backup
```

### Restoring a Backup File from a Device

To restore the configuration data stored in a particular backup file stored on a device, such as a tape drive, enter the following UNIX command on the affected Cisco PGW 2200 Softswitch to run the restore script:

```
mgcrestore -d
```

Where `device` is the device where your backup files are stored.

For example, to restore a backup file stored on a tape drive called /dev/rmt/0, you would enter the following command:

```
mgcrestore -d /dev/rmt/0
```

### Restoring a Backup File Using the Mgcrestore Script

You can also restore a configuration by running the mgcrestore script. To restore the configuration data stored in a particular backup file stored in a directory, perform the following steps:

**Note**  You can restore a backup file only when you are logged in to your system as `mgcusr`. You cannot restore a backup file while you are logged in as `root`.

**Step 1** Enter the following UNIX command on the Cisco PGW 2200 Softswitch:

```
mgcrestore
```

The system returns a response similar to the following:

```
Restore Main Menu
--------------------
Note: to exit the script at anytime use ctrl-c
1. Restore a backup
2. List Backup Files
3. Exit
Selection:
```

**Step 2** Enter 1 to restore a backup file.

The system returns a response similar to the following:

```
Restore a Backup
-----------------
NameRetriesTimeoutDayTimeDirectory
Back15 60 everyday12:00/var/cisco
```
Mybackup030weekdays04:00/var/cisco

Enter the name of the backup to be restored:

Step 3 Enter the name of the automatic backup operation you want to restore.

The system returns a response similar to the following:

Restore this backup (Y or N)?

Step 4 Enter Y if you want to continue with restoring a backup, or enter N if you do not want to restore a backup.

Note You can enter a Ctrl-C keyboard command at any time to halt the execution of the mgcrestore script.

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 *.desiredPlatformState parameter in the XECfgParm.dat file on each host is either master or slave, using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.

Configuration Export Failed Due to MMDB

If you attempt to export your configuration settings using the prov-exp:all MML command and the MMDB is not running, the system returns a failure message. The MMDB must be running for the prov-exp:all MML command to function. To resolve this problem, perform the following steps:

Step 1 If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Log in to the active Cisco PGW 2200 Softswitch and determine whether the MMDB is running by entering the following UNIX command:

```
ps -ef | grep timesten
```

If the system returns a list of running timesten processes such as those listed below, the MMDB is running:

```
root   234     1  0   Dec 21 ?        0:04 /opt/TimesTen32/32/bin/timestend
root   235   234  0   Dec 21 ?        0:03 /opt/TimesTen32/32/bin/timestensubd -id 0
root   236   234  0   Dec 21 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 1
root   237   234  0   Dec 21 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 2
root   238   234  0   Dec 21 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 3
root   239   234  0   Dec 21 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 4
root   240   234  0   Dec 21 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 5
root   241   234  0   Dec 21 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 6
root   242   234  0   Dec 21 ?        0:00 /opt/TimesTen32/32/bin/timestensubd -id 7
mgcusr 14246 14127  0 09:19:38 pts/1    0:00 grep timesten
root 24327   234  0   Dec 26 ?        9:44 /opt/TimesTen32/32/bin/timestenrepd -id 8
-datastore /opt/TimesTen32/datastore/
```

If the MMDB is running, proceed to Step 5. Otherwise, proceed to Step 3.

Step 3 Log in to the active Cisco PGW 2200 Softswitch as root and enter the following UNIX command:
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Platform Troubleshooting

/\etc/init.d/tt4.1_32bit start

If the system response indicates that the database has started, proceed to Step 4. Otherwise, proceed to Step 5.

Step 4  Re-attempt to export your system configuration using the following MML command:

prov-exp:all

If the export is successful, the procedure is complete. Otherwise, proceed to Step 5.

Step 5  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Measurements Are Not Being Generated

If your Cisco PGW 2200 Softswitch is not generating system measurements, perform the following procedure:

Step 1  If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Verify that the amdmpr process is running, as described in the “Verifying That Processes Are Running” section on page 3-4.

If the amdmpr process is not running, proceed to Step 3. Otherwise, proceed to Step 4.

Step 3  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 8-178.

Step 4  Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Call Detail Records Are Not Being Generated

If call detail records are not being generated on your Cisco PGW 2200 Softswitch, perform the following steps:

Step 1  If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2  Verify that the dmpr-01 process is running, as described in the “Verifying That Processes Are Running” section on page 3-4.

If the dmpr-01 process is not running, proceed to Step 3. Otherwise, proceed to Step 5.

Step 3  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 4.
Step 4 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 8-178.

```plaintext
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 5 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

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 If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 If your system is provisioned to control Voice over IP (VoIP) calls that do not originate or terminate on SS7 or PRI (such as SIP-to-SIP or SIP-to-EISUP/H.323 calls), you must synchronize the system state data before continuing. To do this, proceed to Step 3.

If your system is provisioned to control VoIP calls in which at least one call leg is SS7 or PRI, proceed to Step 4.

Step 3 To synchronize the system state data, you must restart the Cisco PGW 2200 Softswitch software on the standby Cisco PGW 2200 Softswitch. To restart the Cisco PGW 2200 Softswitch software, stop the software, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4 and then start the software, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

Step 4 Verify that the path to the affected peer is out-of-service, as described in the “Verifying the Status of all Signaling Services” section on page 9.

If the destination is in-service, or there is no destination associated with the peer, proceed to Step 5.

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 8-95.

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 8-146.

If that resolves the problem, this procedure is complete. Otherwise, proceed to Step 5.

Step 5 Trace the route to the peer by entering the following UNIX command on your active Cisco PGW 2200 Softswitch:

```
traceroute ip_addr
```
Where \( \text{ip\_addr} \) 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 7.

If the system response indicates that you were unable to reach the identified peer, proceed to Step 6.

**Step 6**

Log in to the peer identified in Step 4 and verify that the Ethernet interfaces for this peer are working correctly. See the documentation for the peer for more information.

If the Ethernet interfaces are working properly, proceed to Step 7.

If the Ethernet interfaces are not working properly, replace the element that is not working properly. See the documentation of the peer for more information. 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

---

### 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 PGW 2200 Softswitch software. Perform this step only while in contact with Cisco Technical Assistance Center (TAC) personnel. See the “Obtaining Documentation and Submitting a Service Request” section on page xx for information on contacting the Cisco TAC.

**Step 1**

If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

**Step 2**

Log in to the standby Cisco PGW 2200 Softswitch and change directories to the etc subdirectory by entering the following UNIX command:

```bash
cd /opt/CiscoMGC/etc
```

**Step 3**

Open the XECfgParm.dat using a text editor, such as vi.

**Step 4**

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 11. Otherwise, proceed to Step 5 to begin the process of correcting your configuration.

**Step 5**

Modify the incorrect parameters identified in Step 4 to match their correct values.

**Step 6**

Save your changes and close the text editor.

**Step 7**

Stop the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

**Step 8**

Restart the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.
Step 9 Perform a manual switchover from the active Cisco PGW 2200 Softswitch, as described in the “Performing a Manual Switchover” section on page 3-95.

Warning Switchover operations cause the loss of all SS7 messages transmitted to the Cisco PGW 2200 Softswitch for approximately three seconds. This affects unstable in-progress calls as well as new calls. Stable in-progress calls are not affected.

Step 10 Repeat steps 2 through 9 for the newly standby Cisco PGW 2200 Softswitch.

If that resolves the problem, the procedure is complete. Otherwise, proceed to Step 10.

Step 11 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Diagnosing SNMP Failure

Failure of the Cisco PGW 2200 Softswitch to respond to SNMP requests can be caused by a variety of problems. The Cisco PGW 2200 Softswitch uses Sun Microsystems’ Solaris 10 or Solaris 8 as its operating system. Solaris 8 or Solaris 10 is a 64-bit operating system, and some older hardware platforms cannot support it. SNMP failure can occur in your Cisco PGW 2200 Softswitch system if your system hardware does not meet the requirements of the Cisco PGW 2200 Softswitch software. Another possibility is that when the Solaris 8 or Solaris 10 operating system was installed on your system, the 32-bit kernel was selected instead of the 64-bit kernel. In such situations, the application that handles SNMP functions on the Cisco PGW 2200 Softswitch, CIAgent, may fail and be unable to restart.

To diagnose the source of the SNMP failure, perform the following procedure:

Step 1 If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.

Step 2 Determine whether the SNMP daemon (snmpdm) is running on your system by entering the following command:

```bash
ps -ef | grep snmp
```

The system should return a response similar to the following:

```
root 12061 1 0 Aug 27 ? 0:03 /opt/CiscoMGC/snmp/critagt -d
root 12072 12061 0 Aug 27 ? 0:00 /opt/CiscoMGC/snmp/brassagt -d
root 5233 5231 0 20:06:25 pts/2 0:00 grep snmp
root 12143 12061 0 Aug 27 ? 8:13 /opt/CiscoMGC/snmp/mib2agt -d
root 12144 12061 0 Aug 27 ? 5:54 /opt/CiscoMGC/snmp/hostagt -d
root 12145 12061 0 Aug 27 ? 0:00 /opt/CiscoMGC/snmp/fsagt -d
root 12068 12061 0 Aug 27 ? 13:38 /opt/CiscoMGC/snmp/snmpdm -tcplocal -d
```

If the response from your system does not include snmpdm, the SNMP daemon is not running.

If the SNMP daemon is not running, proceed to Step 3. Otherwise, proceed to Step 11.

Step 3 Verify that the host name and IP address information for your Cisco PGW 2200 Softswitch system configured on your SNMP server is correct.

If the host name and IP address information are incorrect, proceed to Step 4. Otherwise, proceed to Step 4.
Step 4 Modify the host name and IP address information for your Cisco PGW 2200 Softswitch system on your SNMP server.
If this resolves the problem, proceed to Step 10. Otherwise, proceed to Step 5.

Step 5 Verify that the 64-bit kernel instruction sets are installed in your system by entering the following UNIX command:
```
isalist
```
The system should return a response similar to the following:
```
sparcv9+vis sparcv9 sparcv8plus+vis sparcv8plus sparcv8 sparcv8-fsmuld sparcv7 sparc
```
If the response from your system does not include the sparcv9+vis and sparcv9 instruction sets, the 64-bit kernel is not installed on your system.
If the response indicates that the 64-bit kernel is installed in your system, proceed to Step 11. Otherwise, proceed to Step 6.

Step 6 Re-install the operating system as described in the *Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide*. Ensure that the 64-bit kernel is selected during installation.
If the operating system installs successfully, proceed to Step 7. Otherwise, proceed to Step 9.

Step 7 Repeat Step 5 to ensure that the 64-bit kernel has been installed.
If the 64-bit kernel is installed, proceed to Step 8. Otherwise, proceed to Step 9.

Step 8 Re-install the Cisco PGW 2200 Softswitch software as described in the *Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide*.
If the Cisco PGW 2200 Softswitch software installs successfully, proceed to Step 10. Otherwise, proceed to Step 11.

Step 9 Your system hardware is unable to support the 64-bit kernel. To operate the Cisco PGW 2200 Softswitch software, the 64-bit kernel must be installed. You must upgrade your hardware to enable your system to support the 64-bit operating system. Instructions for upgrading your hardware can be found in the Sun Microsystems documentation for the host platform.
Once the upgrade is complete, repeat this procedure starting from Step 6. If the hardware upgrade resolves the problem, proceed to Step 10. Otherwise, proceed to Step 11.

Step 10 Repeat the above steps on the other Cisco PGW 2200 Softswitch in your system.
If the problem is resolved after fixing both Cisco PGW 2200 Softswitches, 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, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.

Correcting the System Time

Note Cisco recommends that you configure your Cisco PGW 2200 Softswitches to use NTP to maintain system time as described in the *Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide*. 
In instances where the system time is incorrect, there are procedures you can use to correct the system time, which vary based on how system time is set on your system, and whether the Cisco PGW 2200 Softswitch is being used to record your call detail records (CDRs). These procedures are as follows:

- **NTP is Not Used and Cisco PGW 2200 Softswitch is Not the Source of the CDRs, page 8-181**
- **NTP is Not Used and Cisco PGW 2200 Softswitch is the Source of the CDRs, page 8-181**
- **NTP is Used and Cisco PGW 2200 Softswitch is the Source of the CDRs, page 8-182**

Caution
Cisco strongly recommends that the synchronization of the host system clock be done in a manner that does not adversely impact operating system or application processes. A rapid change of the system clock can have adverse effects on call processing, system logs, and CDRs.

Caution
Correcting the system time on your Cisco PGW 2200 Softswitches requires that the user be logged in as root. We recommend that you closely control the use of the super-user (root) password and privileges.

**NTP is Not Used and Cisco PGW 2200 Softswitch is Not the Source of the CDRs**

To correct the system time when NTP is not used to maintain system time and the Cisco PGW 2200 Softswitch is not the source of the CDRs, perform the procedure below. This procedure is not service impacting, if performed during a maintenance window.

1. **Step 1**
   - If the time on one Cisco PGW 2200 Softswitch is correct, proceed to Step 2. If the time is incorrect on both Cisco PGW 2200 Softswitches, proceed to Step 3.

2. **Step 2**
   - If the Cisco PGW 2200 Softswitch with the incorrect time is the active Cisco PGW 2200 Softswitch, perform a manual switchover, as described in the “Performing a Manual Switchover” section on page 3-95.
   - If the Cisco PGW 2200 Softswitch with the incorrect time is the standby Cisco PGW 2200 Softswitch, proceed to Step 3.

3. **Step 3**
   - Stop the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch (which has the incorrect time), as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

4. **Step 4**
   - Correct the time on the standby Cisco PGW 2200 Softswitch using the UNIX command `date`. For more information about the date command, see man page for `date`.

5. **Step 5**
   - Restart the Cisco PGW 2200 Softswitch software on your standby Cisco PGW 2200 Softswitch, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.
   - If the time was incorrect on only one of the Cisco PGW 2200 Softswitches, the procedure is complete. Otherwise, repeat steps 1 through 5 for the other Cisco PGW 2200 Softswitch with the incorrect time.

**NTP is Not Used and Cisco PGW 2200 Softswitch is the Source of the CDRs**

To correct the system time when NTP is not used to maintain system time and the Cisco PGW 2200 Softswitch is the source of the CDRs, perform the procedure below.
Platform Troubleshooting

Caution
This procedure is service impacting and should be performed during a maintenance window.

Step 1
Stop the Cisco PGW 2200 Softswitch software on both Cisco PGW 2200 Softswitches, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

Step 2
Correct the time on both Cisco PGW 2200 Softswitches using the UNIX command date. For more information about the date command, see man page for date.

Step 3
Restart the Cisco PGW 2200 Softswitch software on both Cisco PGW 2200 Softswitches, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

NTP is Used and Cisco PGW 2200 Softswitch is the Source of the CDRs

In this situation the system time can only get out of synchronization with the NTP server if a user with root access (which should be strictly controlled) modifies the time on an Cisco PGW 2200 Softswitch. The time on the NTP server cannot be modified. To correct the system time when an NTP server is used to maintain system time, and the Cisco PGW 2200 Softswitch is the source of your CDRs, perform the following steps:

Caution
This procedure is service impacting and should be performed during a maintenance window.

Step 1
Stop the Cisco PGW 2200 Softswitch software on both Cisco PGW 2200 Softswitches, as described in the “Shutting Down the Cisco PGW 2200 Softswitch Software Manually” section on page 2-4.

Step 2
Reboot your Cisco PGW 2200 Softswitches, as described in Sun Microsystems documentation that came with your system. Rebooting the Cisco PGW 2200 Softswitches restarts the Xntp demon, which synchronizes the system time with the time on the NTP server.

Step 3
Restart the Cisco PGW 2200 Softswitch software on both Cisco PGW 2200 Softswitches, as described in the “Starting the Cisco PGW 2200 Softswitch Software” section on page 2-2.

Securing your Network

Cisco PGW 2200 Softswitch introduces a security enhancement for your network. To enable this enhancement, you must have completed installing the CSCOh020 security package on your network (which can consist of Cisco PGW 2200 Softswitch, BAMS, and HSI). The procedure for installing this security package can be found in the Cisco PGW 2200 Softswitch Release 9.8 Software Installation and Configuration Guide.

The process of securing your network is defined in the following sections:

- Securing the Cisco PGW 2200 Softswitch, page 8-183
- Securing Cisco BAMS, page 8-184
Securing the Cisco PGW 2200 Softswitch

Perform the following steps to secure the Cisco PGW 2200 Softswitch:

**Step 1** Before you begin the securing process you must identify the last CDR that has been pulled into BAMS. Log in to the active Cisco PGW 2200 Softswitch as root and enter the following UNIX command to change directories:

```
# cd /opt/CiscoMGC/var/spool
```

**Step 2** Enter the following UNIX command to verify the CDR:

```
# ls -l cdr_yyyymmdd
```

Where `yyyymmdd` represents the current date, entered in the following format:

- **yyy**—year
- **mm**—month
- **dd**—day

A list of files is displayed when you enter this command.

**Step 3** Check the list of files that is displayed for the last finished filename preceded by a period (.) and write down the file name—you will need this information later.

**Step 4** Log in to the standby Cisco PGW 2200 Softswitch as root and enter the following command to change directory:

```
# cd /opt/sun_install
```

**Step 5** Enter the following command to toggle FTP off:

```
# toggle_ftp.sh disable filename
```

Where `filename` is a name that you selected.

The system returns a response similar to the following:

```
You are running as root - Good...
Operating System: SunOS 5.8
Disable ftp in inetd.conf file
```

**Step 6** Enter the following command to toggle Telnet off:

```
# toggle_telnet.sh disable filename
```

Where `filename` is a name that you selected.

The system returns a response similar to the following:

```
You are running as root - Good...
Operating System: SunOS 5.8
Disable ftp in inetd.conf file
```

**Step 7** Log in to the active Cisco PGW 2200 Softswitch as root and enter the following command to change directory:

```
# cd /opt/sun_install
```

**Step 8** Enter the following command to toggle FTP off:

```
# toggle_ftp.sh disable filename
```

Where `filename` is a name that you selected.
The system returns a response similar to the following:

You are running as root - Good...
Operating System: SunOS 5.8
Disable ftp in inetd.conf file

Step 9  Enter the following command to toggle Telnet off:

```
# toggle_telnet.sh disable filename
```

Where *filename* is a name that you selected.

The system returns a response similar to the following:

You are running as root - Good...
Operating System: SunOS 5.8
Disable ftp in inetd.conf file

Step 10 Verify that Telnet and FTP are off. Telnet or FTP to your active Cisco PGW 2200 Softswitch. If Telnet and FTP are turned off, you will get the following error message:

Connection refused.

This completes the procedures for securing your Cisco PGW 2200 Softswitch. If you have BAMS on your network, continue to the “Securing Cisco BAMS” section on page 8-184.

Securing Cisco BAMS

To secure Cisco BAMS on your network:

Step 1  Log in to the standby Cisco BAMS by enter the following command:

```
% bams
```

Step 2  The following steps require you to use MML commands. To use MML commands, enter the following command:

```
% mml
```

Step 3  Enter the node of the Cisco PGW 2200 Softswitch that is being changed. At the MML command line type the following and press *Enter*:

```
<bams hostname> set-mode:<x>:
```

Where *<x>* is a number between 1 through 8.

Note  In this example, the node number is 2.

Step 4  Check for alarms by entering the following command:

```
<bams hostname> rtrv-alms
```

The system returns a response similar to the following:

```
Billing and Measurements Server - BAMS-00 2003-02-12 15:12:05
B RTRV
02/12/03 14:58:14 *C POL402: Cannot connect to unit va-hoover
02/12/03 15:00:15 *C POL401: Max FTP failures for one file reached
02/12/03 15:00:25 *C POL402: Cannot connect to unit va-hoover_b
```
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Platform Troubleshooting

02/12/03 15:02:36 *C POL402: Cannot connect to unit va-fish
02/12/03 15:04:46 *C POL402: Cannot connect to unit va-fish_b
;
B COMPLD
;

Note Look for the line containing POL402. POL402 indicates the presence of an alarm. Proceed to

Step 5.

In this text display, “va-hoover” and “va-fish” are Cisco PGW 2200 Softswitch and Cisco BAMS
host name examples.

Step 5  Log in as root.

Step 6  Type the following command and press Enter to change directory:

# cd /opt/sun_install

Step 7  Type the following command to toggle FTP off:

# toggle_ftp.sh disable <filename>

Note <filename> is a name that you selected.

Text similar to the following is displayed:

You are running as root - Good...
Operating System: SunOS 5.8
Disable ftp in inetd.conf file

Done!

Step 8  Type the following command and press Enter to toggle Telnet off:

# toggle_telnet.sh disable <filename>

Note <filename> is a name that you selected.

Text similar to the following is displayed:

You are running as root - Good...
Operating System: SunOS 5.8
Disable ftp in inetd.conf file

Done!

Step 9  On the active host (BAMS 1), log in as bams.

Step 10 Repeat Step 2 through Step 8.

Step 11 On the standby Cisco BAMS, while logged in as root, type the following command and press Enter to
change the directory:

# cd /opt/sun_install

Step 12 As root, enter the following command to set up the SSH process:

# setupSSH.sh

Text similar to the following is displayed:
BAMS is installed, proceeding with SSH configuration
Warning:
Before running this script, SSH must be installed on all PGW and BAMS hosts

This script will disable the standard FTP client on BAMS and set up
SSH connections from BAMS to PGW and from BAMS to BAMS.

If you want to use the standard FTP client, it is still available
in the file /usr/bin/ftp.orig

Do you want to continue [y/n]:

**Step 13** Enter y (yes) to continue and press Enter.

Text similar to the following is displayed:
Sun Microsystems Inc. SunOS 5.6 Generic August 1997
Warning:
Before running this script, SSH must be installed on all PGW and BAMS hosts.

This script will reset the existing known hostkeys
and user keys for bams user for each host entered during this session.
You need to run this script every time the PGW or BAMS is re-installed.
You also need to run this script if SSH is re-installed on PGW or BAMS.

Do you want to continue [y/n]:

**Step 14** Enter y (yes) to continue and press Enter.

Text similar to the following is displayed:
Generating security keys, this will take a couple of minutes...
Generating public/private rsa key pair.
Your identification has been saved in /opt/CiscoBAMS/local/.ssh/id_rsa.
Your public key has been saved in /opt/CiscoBAMS/local/.ssh/id_rsa.pub.
The key fingerprint is:
Generating public/private dsa key pair.
Your identification has been saved in /opt/CiscoBAMS/local/.ssh/id_dsa.
Your public key has been saved in /opt/CiscoBAMS/local/.ssh/id_dsa.pub.
The key fingerprint is:

You will be prompted for the user name and password for each PGW
or BAMS host.
Please remember to enter both PGW host names for a failover pair.
You also need to enter the other BAMS host if this is a redundant setup.

Please enter a PGW or BAMS host name, or q to quit
Enter a host name now:

**Step 15** Enter host name PGW1 and press Enter.

Text similar to the following is displayed:
Please enter a PGW or BAMS host name, or q to quit
Enter a host name now:

**Step 16** Enter the host name mgcusr (the login name of PGW1) and press Enter.

Text similar to the following is displayed:
Are you sure you want to continue connecting (yes/no)? yes

**Step 17** Enter y (yes) and press Enter.
Text similar to the following is displayed:

```
mgcusr@<hostname>'s password:
```

**Step 18** Enter the password and press **Enter**.

Text similar to the following is displayed:

```
mgcusr@<BAMS 1>'s password:
```

**Step 19** Enter **y** (yes) again and press **Enter**.

Text similar to the following is displayed:

```
mgcusr on <BAMS> successfully configured
```

Do you want to configure second interface for <BAMS>? **n**

**Step 20** You can answer either **y** (yes) or **n** (no):

a. **Yes** (configuring a second interface) is **optional**. If you answer **y**, repeat Step 1 through Step 19.

b. If you answer **no**, proceed to Step 21.

**Step 21** Repeat Step 15 through Step 19 for additional Cisco PGW 2200 Softswitch nodes.

Text similar to the following is displayed:

```
mgcusr on <BAMS1> successfully configured
```

Do you want to configure second interface for <BAMS1>? **n**

**Step 22** Enter **n** (no) and press Enter.

Text similar to the following is displayed:

```
Please enter a PGW or BAMS host name, or q to quit
Enter a host name now:
```

**Step 23** While still on the standby Cisco BAMS, type the active Cisco BAMS unit information (Cisco BAMS name, Cisco BAMS login password).

**Step 24** When all the Cisco BAMS interfaces have been configured, type **q** to quit and press **Enter**.

Text similar to the following is displayed:

```
Done
```

---

**Note** Look out for the following error message. If some hosts were not configured, follow the recommendation in this message.

```
Failed to configure some hosts. Please check for SSH installation on these hosts and/or the user name and password for these hosts.
```

**Step 25** Log in to the active Cisco BAMS as **root**.

**Step 26** Change the directory. Type the following command and press **Enter**:

```
# cd /opt/install
```

**Step 27** Enter the following command and press **Enter**:

```
# setupSSH.sh
Text similar to the following is displayed:

BAMS is installed, proceeding with SSH configuration
Warning:
Before running this script, SSH must be installed on all PGW and BAMS hosts

This script will disable the standard FTP client on BAMS and set up
SSH connections from BAMS to PGW and from BAMS to BAMS.

If you want to use the standard FTP client, it is still available
in the file /usr/bin/ftp.orig

Do you want to continue [y/n]:

Step 28  Enter y to continue and press Enter.

Text similar to the following is displayed:

Sun Microsystems Inc.  SunOS 5.6       Generic August 1997
Warning:
Before running this script, SSH must be installed on all PGW and BAMS hosts.

This script will reset the existing known hostkeys
and user keys for bams user for each host entered during this session.
You need to run this script every time the PGW or BAMS is re-installed.
You also need to run this script if SSH is re-installed on PGW or BAMS.

Do you want to continue [y/n]:

Step 29  Enter y (yes) to continue and press Enter.

Text similar to the following is displayed:

Generating security keys, this will take a couple of minutes...
Generating public/private rsa key pair.
Your identification has been saved in /opt/CiscoBAMS/local/.ssh/id_rsa.
Your public key has been saved in /opt/CiscoBAMS/local/.ssh/id_rsa.pub.
The key fingerprint is:
Generating public/private dsa key pair.
Your identification has been saved in /opt/CiscoBAMS/local/.ssh/id_dsa.
Your public key has been saved in /opt/CiscoBAMS/local/.ssh/id_dsa.pub.
The key fingerprint is:

You will be prompted for the user name and password for each PGW
or BAMS host.
Please remember to enter both PGW host names for a failover pair.
You also need to enter the other BAMS host if this is a redundant setup.

Please enter a PGW or BAMS host name, or q to quit
Enter a host name now:

Step 30  Enter host name PGW1 and press Enter.

Text similar to the following is displayed:

Please enter a PGW or BAMS host name, or q to quit
Enter a host name now:

Step 31  Enter the host name mgcusr (the login name of PGW1) and press Enter.

Text similar to the following is displayed:

Are you sure you want to continue connecting (yes/no)? yes
Step 32  Enter y (yes) and press Enter.
Text similar to the following is displayed:
```
mgcusr@<hostname>'s password: 
id_dsa.pub           100% |*****************************|   602       00:00
```
Type the password and press Enter.
Text similar to the following is displayed:
```
mgcusr@<BAMS 1>'s password:
```
Step 33  Enter y (yes) again and press Enter.
Text similar to the following is displayed:
```
mgcusr on <BAMS> successfully configured
Do you want to configure second interface for <BAMS>? n
```
Step 34  You can answer either y (yes) or n (no):
  a. Yes (configuring a second interface) is optional. If you answer y, repeat Step 1 through Step 19.
  b. If you answer no, proceed to Step 21.
Step 35  Repeat Step 15 through Step 19 for additional Cisco PGW 2200 Softswitch nodes.
Text similar to the following is displayed:
```
mgcusr on <BAMS1> successfully configured
Do you want to configure second interface for <BAMS1>? n
```
Step 36  Enter n (no) and press Enter.
Text similar to the following is displayed:
```
Please enter a PGW or BAMS host name, or q to quit
Enter a host name now:
```
Step 37  While still on the active Cisco BAMS, enter the standby Cisco BAMS unit information (Cisco BAMS name, Cisco BAMS login password).
Step 38  When all the Cisco BAMS interfaces have been configured, type q to quit and press Enter.
Text similar to the following is displayed:
```
Done
```
Step 39  Go to the active Cisco PGW 2200 Softswitch (Host A) in the “Securing the Cisco PGW 2200 Softswitch” section on page 8-183 and repeat Step 1 and Step 2.
Text similar to the following is displayed:
```
-rw-rw-r--   1 mgcusr   mgcgrp       182 Feb 12 14:29 cdr_20030212142403_037281.finished
-rw-rw-r--   1 mgcusr   mgcgrp       182 Feb 12 14:34 cdr_20030212142903_037282.finished
-rw-rw-r--   1 mgcusr   mgcgrp       182 Feb 12 14:39 cdr_20030212143403_037283.finished
-rw-rw-r--   1 mgcusr   mgcgrp       182 Feb 12 14:44 cdr_20030212143903_037284.finished
-rw-rw-r--   1 mgcusr   mgcgrp       182 Feb 12 14:49 cdr_20030212144403_037285.finished
-rw-rw-r--   1 mgcusr   mgcgrp       182 Feb 12 14:54 cdr_20030212144903_037286.finished
-rw-rw-r--   1 mgcusr   mgcgrp       182 Feb 12 14:59 cdr_20030212150403_037287.finished
-rw-rw-r--   1 mgcusr   mgcgrp       182 Feb 12 15:09 cdr_20030212150903_037288.finished
-rw-rw-r--   1 mgcusr   mgcgrp       182 Feb 12 15:14 cdr_20030212151403_037289.finished
-rw-rw-r--   1 mgcusr   mgcgrp       182 Feb 12 15:19 cdr_20030212151904_037290.bin
-rw-rw-r--   1 mgcusr   mgcgrp       182 Feb 12 15:24 cdr_20030212151904_037291.bin
-rw-rw-r--   1 mgcusr   mgcgrp       182 Feb 12 15:30 cdr_20030212152434_037293.bin
```
Step 40  Make sure that the CDR file number you noted down in Step 3 has changed from .bin to .finished.

Step 41  Check for alarms on Cisco BAMS. Enter the following command and press Enter:

```
<bams hostname> rtrv-alms
```

Text similar to the following is displayed:

```
Billing and Measurements Server - BAMS-00 2003-02-12 16:02:08
B  RTRV
02/12/03 15:02:36 *C POL402: Cannot connect to unit <bams1 hostname>
02/12/03 15:04:46 *C POL402: Cannot connect to unit <bams2 hostname>
B  COMPLD
```

Note  The CDR file POL402 (which indicates the presence of an alarm, shown in Step 4) for the active Cisco PGW 2200 Softswitch and standby Cisco BAMS should be gone.

Step 42  Verify that both BAMS 1 and BAMS 2 are communicating with each other.

CDR file POL329 indicates that the active Cisco BAMS (BAMS 1) is sending information to the standby Cisco BAMS (BAMS 2).

Note  Since Cisco BAMS polls the Cisco PGW 2200 Softswitch at regular intervals, you may still see an alarm for a while. When you do, wait a few minutes and check the logs (see Step 43).

Step 43  To check the logs for alarms (the log name within this directory is syslog), change directory to the following:

```
# cd /opt/CiscoBAMS/files/s0x
```

Note  x in s0x is the node you are in.

The process for securing your network is now complete.

**TIBCO Interface Not Working**

The TIBCO interface enables you to use a TIBCO management system to add, modify, delete, and retrieve provisioning data from the Cisco PGW 2200 Softswitch. If you are experiencing difficulties with your TIBCO interface, perform the following steps:

Step 1  If you have not already gathered system data, collect it as described in the “Collecting System Data for Cisco TAC” section on page 8-87.
Step 2 Verify that the TIBCO adapter daemon is running by entering the following UNIX command on the active Cisco PGW 2200 Softswitch:

```
ps -ef
```

The system returns a response similar to the following:

```
UID   PID  PPID  C    STIME TTY      TIME CMD
root     0     0  0 10:28:20 ?        0:00 sched
root     1     0  0 10:28:20 ?        0:27 /etc/init -
mgcusr 14437 14427  0 13:57:19 ?        0:00 /opt/CiscoMGC/bin/perl
/opt/CiscoMGC/local/tibAdapter.pl
mgcusr 14427     1  0 13:57:18 ?        0:00 -csh -c /opt/CiscoMGC/local/tibAdapter.pl
```

If the daemon is running, proceed to Step 9. Otherwise, proceed to Step 3.

Note If your system is also equipped with an SNMP interface, a trap is generated when the Cisco PGW 2200 Softswitch software cannot start the TIBCO daemon.

Step 3 Log in to the standby Cisco PGW 2200 Softswitch as root and change directories to the etc subdirectory by entering the following UNIX command:

```
cd /opt/CiscoMGC/etc
```

Step 4 Open the XECfgParm.dat using a text editor, such as vi.

Step 5 Search for the *.tibcoSupport parameter and verify that it is set to enable. If it is set properly, exit the text editor and proceed to Step 9. Otherwise proceed to Step 6.

Step 6 Change the *.tibcoSupport parameter to enable using the procedure in the “Rebooting Software to Modify Configuration Parameters” section on page 8-178.

Step 7 Verify that the TIBCO adapter daemon is running by entering the following UNIX command on the active Cisco PGW 2200 Softswitch:

```
ps -ef
```

The system returns a response similar to the following:

```
UID   PID  PPID  C    STIME TTY      TIME CMD
root     0     0  0 10:28:20 ?        0:00 sched
root     1     0  0 10:28:20 ?        0:27 /etc/init -
mgcusr 14437 14427  0 13:57:19 ?        0:00 /opt/CiscoMGC/bin/perl
/opt/CiscoMGC/local/tibAdapter.pl
mgcusr 14427     1  0 13:57:18 ?        0:00 -csh -c /opt/CiscoMGC/local/tibAdapter.pl
```

If the daemon is running, proceed to Step 8. Otherwise, proceed to Step 9.

Step 8 Repeat steps 3 through 7 for the newly standby Cisco PGW 2200 Softswitch. If that resolves the problem, the procedure is finished. Otherwise, proceed to Step 9.

Step 9 Contact the Cisco TAC to further analyze the problem and determine a solution. For more information about contacting the Cisco TAC, see the “Obtaining Documentation and Submitting a Service Request” section on page xx.
Installing the License File


Replacing a Failed Disk

This section describes the process of replacing a defective Cisco PGW 2200 Softswitch disk. Each Cisco Cisco PGW 2200 Softswitch system element contains two hard disks (disk 0 and disk 1) that are mirrored using Sun Solaris Disk Suite. The disk mirroring application must be disabled between the two disks in order to replace the defective disk.

Before starting the disk replacement procedures, the following procedures must be completed:

- Identify the disk that needs to be replaced by viewing the /var/adm/messages
- Cisco recommends that the new disk part number must be the same as the defective disk and the size of the replacement disk must be equal to the good disk.

To replace a failed disk on Cisco PGW 2200 Softswitch, perform the following procedure:

**Step 1** Enter the following command and press Enter to check the status of DiskSuite objects.

```bash
# metastat -i
```

Text similar to the following is displayed:

```
d12: Mirror
   Submirror 0: d10
      State: Okay
   Submirror 1: d11
      State: Needs maintenance
      Pass: 1
      Read option: roundrobin (default)
      Write option: parallel (default)
      Size: 259963830 blocks (123 GB)

d10: Submirror of d12
   State: Okay
   Size: 259963830 blocks (123 GB)
   Stripe 0:
   Device     Start Block  Dbase        State Reloc Hot Spare
   c3t0d0s5          0     No            Okay   Yes


d11: Submirror of d12
   State: Needs maintenance
   Invoke: metareplace d12 c3t1d0s5 <new device>
   Size: 259963830 blocks (123 GB)
   Stripe 0:
   Device     Start Block  Dbase        State Reloc Hot Spare
   c3t1d0s5          0     No     Maintenance   Yes


d9: Mirror
   Submirror 0: d7
      State: Okay
   Submirror 1: d8
```
### State: Needs maintenance
- Pass: 1
- Read option: roundrobin (default)
- Write option: parallel (default)
- Size: 8193150 blocks (3.9 GB)

<table>
<thead>
<tr>
<th>d7: Submirror of d9</th>
<th>State: Okay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size: 8193150 blocks (3.9 GB)</td>
<td></td>
</tr>
<tr>
<td>Stripe 0:</td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>Start Block</td>
</tr>
<tr>
<td>c3t0d0s3</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>d8: Submirror of d9</th>
<th>State: Needs maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoke: metareplace d9 c3t1d0s3 &lt;new device&gt;</td>
<td></td>
</tr>
<tr>
<td>Size: 8193150 blocks (3.9 GB)</td>
<td></td>
</tr>
<tr>
<td>Stripe 0:</td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>Start Block</td>
</tr>
<tr>
<td>c3t1d0s3</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>d6: Mirror</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submirror 0: d4</td>
</tr>
<tr>
<td>State: Okay</td>
</tr>
<tr>
<td>Submirror 1: d5</td>
</tr>
<tr>
<td>State: Needs maintenance</td>
</tr>
<tr>
<td>Pass: 1</td>
</tr>
<tr>
<td>Read option: roundrobin (default)</td>
</tr>
<tr>
<td>Write option: parallel (default)</td>
</tr>
<tr>
<td>Size: 10249470 blocks (4.9 GB)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>d4: Submirror of d6</th>
<th>State: Okay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size: 10249470 blocks (4.9 GB)</td>
<td></td>
</tr>
<tr>
<td>Stripe 0:</td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>Start Block</td>
</tr>
<tr>
<td>c3t0d0s1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>d5: Submirror of d6</th>
<th>State: Needs maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoke: metareplace d6 c3t1d0s1 &lt;new device&gt;</td>
<td></td>
</tr>
<tr>
<td>Size: 10249470 blocks (4.9 GB)</td>
<td></td>
</tr>
<tr>
<td>Stripe 0:</td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>Start Block</td>
</tr>
<tr>
<td>c3t1d0s1</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>d3: Mirror</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submirror 0: d1</td>
</tr>
<tr>
<td>State: Okay</td>
</tr>
<tr>
<td>Submirror 1: d2</td>
</tr>
<tr>
<td>State: Needs maintenance</td>
</tr>
<tr>
<td>Pass: 1</td>
</tr>
<tr>
<td>Read option: roundrobin (default)</td>
</tr>
<tr>
<td>Write option: parallel (default)</td>
</tr>
<tr>
<td>Size: 4096575 blocks (2.0 GB)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>d1: Submirror of d3</th>
<th>State: Okay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size: 4096575 blocks (2.0 GB)</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Stripe 0:
Device     Start Block  Dbase        State Reloc Hot Spare
c3t0d0s0          0     No            Okay   Yes

d2: Submirror of d3
State: Needs maintenance
Invoke: metareplace d3 c3t1d0s0 <new device>
Size: 4096575 blocks (2.0 GB)

Stripe 0:
Device     Start Block  Dbase        State Reloc Hot Spare
c3t1d0s0          0     No     Maintenance   Yes

Device Relocation Information:
Device   Reloc  Device ID
c3t1d0   Yes    id1,sd8n5000c5000914e78b
c3t0d0   Yes    id1,sd8n5000c50008cc7c13

Step 2  Delete state database replicas (indicated with State: Needs maintenance) of the defective disk using the following command:
# metadb -d c3t1d0s4

Step 3  Reboot the Cisco PGW 2200 Softswitch.
# reboot -- -r

Step 4  Remove the defective disk from the Cisco PGW 2200 Softswitch.

Step 5  Insert the new disk into the Cisco PGW 2200 Softswitch.

Step 6  Detect the new disk using the following command:
# devfsadm

Step 7  Display the available disk information using the following command:
# format

Text similar to the following is displayed:
(Use ctrl-c to exit.)

Searching for disks...done

AVAILABLE DISK SELECTIONS:
  0. c3t0d0 <DEFAULT cyl 17845 alt 2 hd 255 sec 63>
    /pci079,0/pci1022,7458011/pci1000,306002/sd00,0
  1. c3t1d0 <DEFAULT cyl 17845 alt 2 hd 255 sec 63>
    /pci079,0/pci1022,7458011/pci1000,306002/sd01,0

Specify disk (enter its number):

Step 8 Use the following command to check the status of DiskSuite objects.

# metastat -i

Text similar to the following is displayed:

d12: Mirror
  Submirror 0: d10
    State: Okay
  Submirror 1: d11
    State: Needs maintenance
    Pass: 1
    Read option: roundrobin (default)
    Write option: parallel (default)
    Size: 259963830 blocks (123 GB)

d10: Submirror of d12
    State: Okay
    Size: 259963830 blocks (123 GB)
    Stripe 0:
      Device     Start Block  Dbase        State Reloc Hot Spare
      c3t0d0s5          0     No            Okay   Yes

d11: Submirror of d12
    State: Needs maintenance
    Invoke: metareplace d12 c3t1d0s5 <new device>
    Size: 259963830 blocks (123 GB)
    Stripe 0:
      Device     Start Block  Dbase        State Reloc Hot Spare
      c3t1d0s5          0     No     Maintenance   Yes

d9: Mirror
  Submirror 0: d7
    State: Okay
  Submirror 1: d8
    State: Needs maintenance
    Pass: 1
    Read option: roundrobin (default)
    Write option: parallel (default)
    Size: 8193150 blocks (3.9 GB)

d7: Submirror of d9
    State: Okay
    Size: 8193150 blocks (3.9 GB)
    Stripe 0:
      Device     Start Block  Dbase        State Reloc Hot Spare
c3t0d0s3 0 No Okay Yes

d8: Submirror of d9
State: Needs maintenance
Invoke: metareplace d9 c3t1d0s3 <new device>
Size: 8193150 blocks (3.9 GB)
Stripe 0:

<table>
<thead>
<tr>
<th>Device</th>
<th>Start Block</th>
<th>Dbase</th>
<th>State</th>
<th>Reloc</th>
<th>Hot Spare</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t1d0s3</td>
<td>0</td>
<td>No</td>
<td>Maintenance</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

d6: Mirror
Submirror 0: d4
State: Okay
Submirror 1: d5
State: Needs maintenance
Pass: 1
Read option: roundrobin (default)
Write option: parallel (default)
Size: 10249470 blocks (4.9 GB)

d4: Submirror of d6
State: Okay
Size: 10249470 blocks (4.9 GB)
Stripe 0:

<table>
<thead>
<tr>
<th>Device</th>
<th>Start Block</th>
<th>Dbase</th>
<th>State</th>
<th>Reloc</th>
<th>Hot Spare</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t0d0s1</td>
<td>0</td>
<td>No</td>
<td>Okay</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

d5: Submirror of d6
State: Needs maintenance
Invoke: metareplace d6 c3t1d0s1 <new device>
Size: 10249470 blocks (4.9 GB)
Stripe 0:

<table>
<thead>
<tr>
<th>Device</th>
<th>Start Block</th>
<th>Dbase</th>
<th>State</th>
<th>Reloc</th>
<th>Hot Spare</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t1d0s1</td>
<td>0</td>
<td>No</td>
<td>Maintenance</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

d3: Mirror
Submirror 0: d1
State: Okay
Submirror 1: d2
State: Needs maintenance
Pass: 1
Read option: roundrobin (default)
Write option: parallel (default)
Size: 4096575 blocks (2.0 GB)

d1: Submirror of d3
State: Okay
Size: 4096575 blocks (2.0 GB)
Stripe 0:

<table>
<thead>
<tr>
<th>Device</th>
<th>Start Block</th>
<th>Dbase</th>
<th>State</th>
<th>Reloc</th>
<th>Hot Spare</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t0d0s0</td>
<td>0</td>
<td>No</td>
<td>Okay</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

d2: Submirror of d3
State: Needs maintenance
Invoke: metareplace d3 c3t1d0s0 <new device>
Size: 4096575 blocks (2.0 GB)
Stripe 0:
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Device     Start Block  Dbase        State Reloc Hot Spare

<table>
<thead>
<tr>
<th>Device</th>
<th>Start Block</th>
<th>Dbase</th>
<th>State</th>
<th>Reloc</th>
<th>Hot Spare</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t1d0s0</td>
<td>0</td>
<td>No</td>
<td>Maintenance</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
| d15: Mirror
  Submirror 0: d13
    State: Okay
  Submirror 1: d14
    State: Needs maintenance
    Pass: 1
    Read option: roundrobin (default)
    Write option: parallel (default)
    Size: 4096575 blocks (2.0 GB)
| d13: Submirror of d15
  State: Okay
  Size: 4096575 blocks (2.0 GB)
  Stripe 0:
<table>
<thead>
<tr>
<th>Device</th>
<th>Start Block</th>
<th>Dbase</th>
<th>State Reloc Hot Spare</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t0d0s6</td>
<td>0</td>
<td>No</td>
<td>Okay</td>
</tr>
</tbody>
</table>
| d14: Submirror of d15
  State: Needs maintenance
  Invoke: metareplace d15 c3t1d0s6 <new device>
  Size: 4096575 blocks (2.0 GB)
  Stripe 0:
<table>
<thead>
<tr>
<th>Device</th>
<th>Start Block</th>
<th>Dbase</th>
<th>State Reloc Hot Spare</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t1d0s6</td>
<td>0</td>
<td>No</td>
<td>Maintenance</td>
</tr>
</tbody>
</table>

Device Relocation Information:
Device  Reloc  Device ID
<table>
<thead>
<tr>
<th>Device</th>
<th>Reloc</th>
<th>Device ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t0d0</td>
<td>Yes</td>
<td>id1,sd@n5000c50008cc7c13</td>
</tr>
</tbody>
</table>

Step 9  Import the volume table of contents from the existing disk to the new disk using the following command:

```
# prtvtoc /dev/rdsk/c3t0d0s2 | fmthard -s - /dev/rdsk/c3t1d0s2
```

Text similar to the following is displayed:

fmthard:  New volume table of contents now in place.

Step 10  Create the initial state database using the following commands:

```
# metadb -f -a /dev/dsk/c3t1d0s4
```

Step 11  Display the status of the disk state databases using the following command:

```
# metadb -i
```

Text similar to the following is displayed:

```
flags     first blk    block count
a  m  p  luo  16   8192   /dev/dsk/c3t0d0s4
a  u       16   8192   /dev/dsk/c3t1d0s4
```

r - replica does not have device relocation information
o - replica active prior to last mddb configuration change
u - replica is up to date
l - locator for this replica was read successfully
c - replica's location was in /etc/lvm/mddb.cf
p - replica's location was patched in kernel
m - replica is master, this is replica selected as input
W - replica has device write errors
a - replica is active, commits are occurring to this replica
M - replica had problem with master blocks
D - replica had problem with data blocks
F - replica had format problems
S - replica is too small to hold current database
R - replica had device read errors

Step 12 Use the following commands to enable the mirror/submirror components that need maintenance shown in Step 8.

```
# metareplace -e d15 c3t1d0s6
# metareplace -e d12 c3t1d0s5
# metareplace -e d9 c3t1d0s3
# metareplace -e d6 c3t1d0s1
# metareplace -e d3 c3t1d0s0
```

Step 13 Verify that the status of DiskSuite objects is okay using the following command:

```
# metastat -i
```

Text similar to the following is displayed:

```
d12: Mirror
   Submirror 0: d10
      State: Okay
   Submirror 1: d11
      State: Okay
      Pass: 1
      Read option: roundrobin (default)
      Write option: parallel (default)
      Size: 259963830 blocks (123 GB)

d10: Submirror of d12
      State: Okay
      Size: 259963830 blocks (123 GB)
      Stripe 0:
         Device     Start Block  Dbase        State Reloc Hot Spare
c3t0d0s5          0     No            Okay   Yes

d11: Submirror of d12
      State: Okay
      Size: 259963830 blocks (123 GB)
      Stripe 0:
         Device     Start Block  Dbase        State Reloc Hot Spare
c3t1d0s5          0     No            Okay   Yes

d9: Mirror
   Submirror 0: d7
      State: Okay
   Submirror 1: d8
      State: Okay
      Pass: 1
      Read option: roundrobin (default)
      Write option: parallel (default)
      Size: 8193150 blocks (3.9 GB)

d7: Submirror of d9
      State: Okay
      Size: 8193150 blocks (3.9 GB)
      Stripe 0:
         Device     Start Block  Dbase        State Reloc Hot Spare
c3t0d0s3          0     No            Okay   Yes
```
Chapter 8  Troubleshooting the Cisco PGW 2200 Softswitch Platform

Platform Troubleshooting

d8: Submirror of d9
State: Okay
Size: 8193150 blocks (3.9 GB)
Stripe 0:

<table>
<thead>
<tr>
<th>Device</th>
<th>Start Block</th>
<th>Dbase</th>
<th>State Reloc</th>
<th>Hot Spare</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t1d0s3</td>
<td>0</td>
<td>No</td>
<td>Okay</td>
<td>Yes</td>
</tr>
</tbody>
</table>

d6: Mirror
Submirror 0: d4
State: Okay
Submirror 1: d5
State: Okay
Pass: 1
Read option: roundrobin (default)
Write option: parallel (default)
Size: 10249470 blocks (4.9 GB)

d4: Submirror of d6
State: Okay
Size: 10249470 blocks (4.9 GB)
Stripe 0:

<table>
<thead>
<tr>
<th>Device</th>
<th>Start Block</th>
<th>Dbase</th>
<th>State Reloc</th>
<th>Hot Spare</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t0d0s1</td>
<td>0</td>
<td>No</td>
<td>Okay</td>
<td>Yes</td>
</tr>
</tbody>
</table>

d5: Submirror of d6
State: Okay
Size: 10249470 blocks (4.9 GB)
Stripe 0:

<table>
<thead>
<tr>
<th>Device</th>
<th>Start Block</th>
<th>Dbase</th>
<th>State Reloc</th>
<th>Hot Spare</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t1d0s1</td>
<td>0</td>
<td>No</td>
<td>Okay</td>
<td>Yes</td>
</tr>
</tbody>
</table>

d3: Mirror
Submirror 0: d1
State: Okay
Submirror 1: d2
State: Okay
Pass: 1
Read option: roundrobin (default)
Write option: parallel (default)
Size: 4096575 blocks (2.0 GB)

d1: Submirror of d3
State: Okay
Size: 4096575 blocks (2.0 GB)
Stripe 0:

<table>
<thead>
<tr>
<th>Device</th>
<th>Start Block</th>
<th>Dbase</th>
<th>State Reloc</th>
<th>Hot Spare</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t0d0s0</td>
<td>0</td>
<td>No</td>
<td>Okay</td>
<td>Yes</td>
</tr>
</tbody>
</table>

d2: Submirror of d3
State: Okay
Size: 4096575 blocks (2.0 GB)
Stripe 0:

<table>
<thead>
<tr>
<th>Device</th>
<th>Start Block</th>
<th>Dbase</th>
<th>State Reloc</th>
<th>Hot Spare</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t1d0s0</td>
<td>0</td>
<td>No</td>
<td>Okay</td>
<td>Yes</td>
</tr>
</tbody>
</table>

d15: Mirror
Submirror 0: d13
State: Okay
### Submirror 1: d14
- **State:** Okay
- **Pass:** 1
- **Read option:** roundrobin (default)
- **Write option:** parallel (default)
- **Size:** 4096575 blocks (2.0 GB)

### d13: Submirror of d15
- **State:** Okay
- **Size:** 4096575 blocks (2.0 GB)

<table>
<thead>
<tr>
<th>Stripe 0:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>c3t0d0s6</td>
</tr>
</tbody>
</table>

### d14: Submirror of d15
- **State:** Okay
- **Size:** 4096575 blocks (2.0 GB)

<table>
<thead>
<tr>
<th>Stripe 0:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>c3t1d0s6</td>
</tr>
</tbody>
</table>

### Device Relocation Information:

<table>
<thead>
<tr>
<th>Device</th>
<th>Reloc</th>
<th>Device ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>c3t1d0</td>
<td>Yes</td>
<td>id1, sd0n5000c5000914e78b</td>
</tr>
<tr>
<td>c3t0d0</td>
<td>Yes</td>
<td>id1, sd0n5000c50008cc7c13</td>
</tr>
</tbody>
</table>