APPENDIX A

Alarm Message Reference

Revised: December 16, 2009, OL-14480-06

This section provides reference information about alarm messages displayed in the Cisco Media Gateway Controller (MGC) Node Manager (MNM) event browser. Specifically

- For the Cisco PGW 2200 Softswitch and the Cisco Billing and Measurements Server (BAMS), this section provides
  - References from which you can navigate to the relevant document to find the message you are interested in (see the "Cisco PGW 2200 Softswitch Host Alarm Messages" section on page A-2 and the "Cisco BAMS Alarm Messages" section on page A-3). A short description of each document is included.
  - Instructions for looking up the desired message in the referenced document (see the "Looking Up Cisco PGW 2200 Softswitch and Cisco BAMS Alarm Messages" section on page A-2).
  - A list and short description of application-related alarm messages (see the "Cisco PGW 2200 Softswitch Host and Cisco BAMS Resource Alarms" section on page A-4).
- For the Cisco ITP-L and Cisco LAN Switches, this section lists messages and provides short descriptions (see the "Cisco ITP-L Alarm Messages" section on page A-5).

Note Cisco IP Transfer Point LinkExtender (ITP-L) is the new name for Cisco Signaling Link Terminal (SLT). Over time, ITP-L will replace SLT in publications and the product.

Overview of Cisco MNM Alarm Management

Cisco MNM converts traps received from managed devices to alarms which are displayed in the Event Browser. For the Cisco ITP-L and the Cisco LAN switches, each trap has a corresponding Cisco MNM alarm. For example, the linkDown trap from the Cisco ITP-L corresponds to the "Link down" event description in the Cisco MNM Event Browser. For the Cisco BAMS and the Cisco PGW 2200 Softswitch, the trap serves as an envelope that can carry any one of numerous alarm messages.

Note Cisco MNM does not handle every possible trap that can be generated from each of the network elements, only those traps that are used for management of the devices as they are deployed to support the Cisco PGW 2200 Softswitch node configuration.

In addition to device-specific traps, Cisco MNM generates internal alarms. Appendix C, "Troubleshooting Cisco MNM" provides an explanation of these internal messages.

Looking Up Cisco PGW 2200 Softswitch and Cisco BAMS Alarm Messages

Use this procedure to look up information for a specific alarm message.

Step 1 In the Event Browser, check the Object Name to determine the network object that generated the event, and note the event description.

Step 2 In this document, go to the section that applies to that object.

Step 3 Click the name of the document or section (displayed in blue to indicate a link) that contains the information you want. The linked document opens.

Step 4 Press **Ctrl-F** for your browser's Find dialog box.

Step 5 In the dialog box, enter some of the initial text of the event description, and click **OK**.

Note If your search text is not found, it means that the Event Browser description does not match exactly the generated message. You can search on a different part of the description string, or scroll through the document to find the message.

Cisco PGW 2200 Softswitch Host Alarm Messages

Cisco MNM handles the traps in Table A-1 from the Cisco PGW 2200 Softswitch hosts. Each trap is used as an envelope for alarms of the corresponding type.

Table A-1 Cisco PGW 2200 Softswitch Host Traps

Trap	MIB
qualityOfService	CISCO-TRANSPATH-MIB
processingError	CISCO-TRANSPATH-MIB
equipmentError	CISCO-TRANSPATH-MIB
environmentError	CISCO-TRANSPATH-MIB
commAlarm	CISCO-TRANSPATH-MIB

For system messages information, see the *Cisco Media Gateway Controller Software Release 9 Messages Reference* at

http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/9/system/message/errmsg.html

The alarm documentation includes the following information for each event:

- Alarm category—Alarm or event message, corresponding to the event description in the Cisco MNM Event Browser.

- Description—Brief description of the alarm or event.
- Severity level—The severity of the alarm or event.
- Event reporting—Whether the event is reported to the management interface and can be obtained through the use of SNMP. (The Event Browser lists only those events that are reported.)
- Alarm/event cause—The condition causing the alarm or event.
- SNMP trap type—Which SNMP trap type pertains to the event, displayed with a numeric code for the trap type:
  - 0 = Do not send an SNMP trap
  - 1 = Communication alarm
  - 2 = Quality of service alarm
  - 3 = Processing error alarm
  - 4 = Equipment error alarm
  - 5 = Environment error alarm
- Suggested Action—Recommendations for resolving the problem.

Cisco BAMS Alarm Messages

All Cisco BAMS alarms are carried on a single trap, the AlarmTrap, as shown in Table A-2.

Table A-2 BAMS Traps

Trap	MIB
nusageAlarmTrap	ACECOMM-NUSAGE-MIB

The Cisco BAMS captures alarms and minor, major, or critical events and forwards them to network management systems such as Cisco MNM. The severity level for message forwarding defaults to minor and above but can be changed by the BAMS system administrator.

The *Cisco Billing and Measurements Server User's Guide* at http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/bams/3.30/guide/330_ug.html includes an appendix (Appendix A. Troubleshooting) that provides a discussion of these messages and their use in troubleshooting. Messages are related to the tasks the BAMS performs, and the appendix also includes an explanation of the BAMS tasks. The message documentation is organized by task.

Information for each system message is supplied in the following categories:

- Message ID—A six-character label that uniquely identifies each message. The first three characters are the application task ID, which identifies the application task that generated the message. (For example, MGR denotes the Manager task and MSC denotes the Mass Storage Control task.) The second three characters are the message number; for example, 013 or 122.
- Text—The verbal part of the message that appears in the system log file, which generally corresponds to the event description in the Cisco MNM Event Browser.
- Arguments—Variable parts of the message, enclosed in angle brackets.
- Description—An explanation of the event that generated the message.

Action—What you should do as a result of the event described in the message. In some cases; for example, informational messages, no action might be required. Actions for error messages (manual, warning, minor, major, and critical) might include steps that should be followed so that you can identify and correct problems. Error actions might also describe how the BAMS responds to the specified error condition.

Note The BAMS File Rename Failure alarm (POL115) must be manually cleared not only in Cisco MNM but also on the BAMS before new alarms of that type can be generated.

Cisco HSI Server Alarm Messages

The Cisco HSI server generates autonomous messages, or events, to notify you of problems or atypical network conditions. Depending on the severity level, events are considered alarms or informational events. HSI adjunct captures minor, major, and critical events and forwards them to the Cisco MNM.

The *Cisco H.323 Signaling Interface User Guide* at http://www.cisco.com/en/US/docs/voice_ip_comm/pgw/hsi/4.3/guide/43ug.html provides details on these messages and their use in troubleshooting. The following information is provided for each alarm message:

- Description
- Severity level and trap type
- Cause
- Troubleshooting procedure

Cisco PGW 2200 Softswitch Host and Cisco BAMS Resource Alarms

Cisco MNM traps application-related events that occur on the Cisco PGW 2200 Softswitch host or the Cisco BAMS (see Table A-3).

Note You can also monitor the performance of the following Cisco PGW 2200 Softswitch host and Cisco BAMS system components: fixed disk storage used, processor load, RAM, and virtual memory used. See the "Performance Data Collected for System Components" section on page B-11.

Table A-3 Resource Alarms

Alarm	MIB	Explanation
critAppDown	CRITAPP-MIB	A critical application is down.
critAppUp	CRITAPP-MIB	The critical application is up after being down. This clears the above alarm.
siFsAboveWarningThreshold	SIFSMONITOR-MIB	A monitored file system usage percentage is above the warning threshold.

Table A-3 Resource Alarms (continued)

Alarm	MIB	Explanation
siFsBelowWarningThreshold	SIFSMONITOR-MIB	The monitored file system usage is below the warning threshold. This clears the above alarm.
siFsAboveCriticalThreshold	SIFSMONITOR-MIB	A monitored file system usage percentage is above the critical threshold.
siFsBelowCriticalThreshold	SIFSMONITOR-MIB	The monitored file system usage is below the critical threshold. This clears the above alarm.

Cisco ITP-L Alarm Messages

Table A-4 Cisco ITP-L Alarms

Alarm	MIB	Explanation
coldStart	SNMPv2-MIB	The device was started from a power-off state. **Note** Clear this event manually.
warmStart	SNMPv2-MIB	The device was restarted from an on state. **Note** Clear this event manually.
linkUp	IF-MIB	An interface is up after being down.
linkDown	IF-MIB	An interface is down. This is cleared by one or more linkUp traps for the same interface.
authenthicationFailure	SNMPv2-MIB	The device received an SNMP message that was improperly authenticated.
syslogAlarm	CISCO-SYSLOG-MIB	—
configChange	CISCO-CONFIG-MAN-MIB-VISMI	There has been a configuration change (informational).

Cisco LAN Switch Alarm Messages

Catalyst 5500 and 6509 Alarms

Table A-5 Catalyst 5500 Alarms

Alarm	MIB	Explanation
coldStart	SNMPv2-MIB	The device was started from a power-off state. **Note** Clear this event manually.
warmStart	SNMPv2-MIB	The device was restarted from an on state. **Note** Clear this event manually.

Table A-5 Catalyst 5500 Alarms (continued)

Alarm	MIB	Explanation
linkUp	IF-MIB	An interface is up after being down.
linkDown	IF-MIB	An interface is down. This is cleared by one or more Link Up traps for the same interface.
authenticationFailure	SNMPv2-MIB	The device received an SNMP message that was improperly authenticated.
configChange	CISCO-CONFIG-MAN-MIB-VISMI	There has been a configuration change (informational).
switchModuleUp	CISCO-STACK-MIB	A module is up after being down.
switchModuleDown	CISCO-STACK-MIB	A module is down.

Catalyst 2900XL Alarms

Table A-6 Catalyst 2900XL Alarms

Alarm	MIB	Explanation
coldStart	SNMPv2-MIB	The device was started from a power-off state. **Note** Clear this event manually.
warmStart	SNMPv2-MIB	The device was restarted from an on state. **Note** Clear this event manually.
linkUp	IF-MIB	An interface is up after being down.
linkDown	IF-MIB	An interface is down. This is cleared by one or more Link Up traps for the same interface.
authenthicationFailure	SNMPv2-MIB	The device received an SNMP message that was improperly authenticated.
syslogAlarm	CISCO-SYSLOG-MIB	—
configChange	CISCO-STACK-MIB	There has been a configuration change (informational).

Cisco PGW 2200 Softswitch Alarm Messages

The Cisco PGW 2200 Softswitch generates messages, or events, to notify you of problems or atypical network conditions. Depending on the severity level, events are considered alarms or informational events. Events with a severity level of critical, major, or minor are classified as alarms, and then reported to the built-in alarm relay unit (ARU). The alarms can be retrieved through MML and a Simple Network Management Protocol (SNMP) manager.

Alarms and informational events follow the Telcordia Transaction Language 1 (TL1) message format.

Alarms produce different system responses from that the informational events produce. An alarm is reported when an alarm state changes (assuming the alarm does not have a nonreported severity). It is a significant violation of existing management systems to report consecutive state changes, active or clear, for a particular alarm on a single entity.

An informational event is reported without a state change being required. It is a warning that an abnormal condition has occurred that does not require corrective action by the management center. An invalid protocol call state transition is an example of an informational event. The event needs to be reported, and if it is transient, there is no corrective action that can be initiated by the management center to fix the problem.

An informational event is reported once, upon occurrence, through the MML and SNMP interfaces. The MML interface must be in the RTRV-ALMS::CONT mode for the event to be displayed; it is not displayed in subsequent RTRV-ALMS requests.

Table A-7 defines the Cisco PGW 2200 Softswitch message components that are displayed by means of the RTRV-ALMS::CONT command in its state of listening for alarm events.

Table A-7 Cisco PGW 2200 Softswitch Message Components

Component	Description
systemid	The name of your device and its identifier.
YYYY-MM-DD	Year, month, and day of alarm or event.
hh-mm-ss-ms	Hour, minute, second, and millisecond of alarm or event, displayed in system time.
timezone	Time zone for which the system time is configured.
severity	Two-character indicator with the following descriptions: • *C—Critical alarm. Reported to the built-in ARU. • **—Major alarm. Reported to the built-in ARU. • *^—Minor alarm. Reported to the built-in ARU. • A^—Informational event. Research if you receive the same event frequently, because it may be an indicator of a more significant problem. • —(empty spaces in two leftmost columns.) Alarm or event has been cleared. “STATE=CLEARED” is displayed. The informational events and cleared alarms or events are not reported to the built-in ARU. They can be obtained from your SNMP manager or by issuing the RTRV-ALMS::CONT MML command.
comp	MML name of the component that is generating the alarm/event. See the *Cisco Media Gateway Controller Software Release 9 Provisioning Guide* for more information about components.
almCat	Alarm category (or event category). A text string that indicates whether the message is an alarm or an informational event and lists the MML alarm or event message. **Note** Despite its name, Alarm Category field is used for both alarms and information events.
params	Supplemental parameters used to further clarify the alarm or event.
comment	Supplemental comment used to indicate cause or appropriate action. See the *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide* for more information on clearing alarms.