



Cisco HSI Alarms and Troubleshooting

Introduction

This chapter contains information about Cisco H.323 Signaling Interface (HSI) alarms, troubleshooting procedures for these alarms, and information about detailed logging. This chapter contains the following sections:

- [Alarms Overview, page 6-1](#)
- [Troubleshooting, page 6-6](#)
- [Detailed Logging, page 6-16](#)

Alarms Overview

An alarm can be in one of the following states:

- Raised, when a persistent fault occurs in the system
- Cleared, when the fault is fixed

Debounce

The alarms have a timeout (debounce) period. The debounce period is the delay time that occurs before an alarm condition is accepted. Use the `ALARMDEBOUNCETIME` parameter to set the debounce period (see [Chapter 5, “Provisioning the Cisco HSI”](#)). The default debounce period is 0.

Severity Levels

The Cisco HSI 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. [Table 6-1](#) lists the severity levels and the required responses.

Table 6-1 Alarm Severity Levels

Severity Level	Description
Critical	A serious problem exists in the network. Clear critical alarms immediately. A critical alarm should force an automatic restart of the application.
Major	A disruption of service has occurred. Clear this alarm immediately.
Minor	No disruption of service has occurred, but clear this alarm as soon as possible.
Informational	A warning that an abnormal condition that does not require corrective action has occurred (for example, an invalid protocol call state transition). An informational event is reported but is transient. No corrective action is required by the management center to fix the problem.

Alarms

Events with a severity level of critical, major, or minor are classified as alarms and can be retrieved through the Man-Machine Language (MML) interface and a Simple Network Management Protocol (SNMP) manager.

An alarm must be reported when an alarm state changes (assuming the alarm does not have a nonreported severity).

Informational Events

Informational events do not require state changes. An informational event is a warning that an abnormal condition that does not require corrective action has occurred. An invalid protocol call state transition is an example of an informational event. The informational event needs to be reported, but it is transient. No corrective action is required 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-alm:cont` mode for the event to be displayed. The event is not displayed in subsequent `rtrv-alm` requests.

SNMP Trap Types

Alarms have SNMP trap types associated with them. Table 6-2 identifies the trap types.

Table 6-2 SNMP Trap types

Trap Type	Description
0	No error
1	Communication alarm
2	Quality of service
3	Processing error
4	Equipment error
5	Environment error

Retrieving Alarm Messages

Alarms can be displayed in noncontinuous mode or in continuous mode.

Noncontinuous Mode

To display all current alarms, use the **rtrv-alm**s MML command.

Figure 6-1 shows an example of an alarm message displayed with the **rtrv-alm**s MML command (noncontinuous mode). For more information about the **rtrv-alm**s MML command, see Appendix A, “MML Commands.”

Figure 6-1 Sample Alarm Message

Node ID	Alarm Category	Severity Level	Displayed only if state=cleared
"H323-GW1:ALM=	\"VSC FAILURE\"	,SEV=MJ	STATE=CLEARED

The example in Figure 6-1 shows a Cisco Public Switched Telephone Network (PSTN) Gateway (PGW 2200) communication failure on the Cisco HSI with the ID H323-GW1 and indicates that the message is an alarm with a *major* severity level.

Continuous Mode

To display the names of active alarms and new alarm events, use the **rtrv-alm**s:cont MML command.

Table 6-3 defines the message components that are displayed when the **rtrv-alm**s:cont MML command is used. The following is sample output from this command. For more information about the **rtrv-alm**s:cont MML command, see Appendix A, “MML Commands.”

```

GW Signaling Gateway      2000-12-05 14:19:22
M   RTRV
"H323-GW1: 2000-11-27 11:25:12.259, ** ALM=\"VSC FAILURE\",SEV=MJ"
"H323-GW1: 2000-11-27 11:25:13.259, ALM=\"VSC FAILURE\",SEV=MJ"STATE=CLEARED
"H323-GW1: 2000-11-27 11:25:13.260, ** ALM=\"CONFIGURATION FAILURE\",SEV=MJ"
"H323-GW1: 2000-11-27 11:25:14.011, A^ ALM=\"ENDPOINT CHANNEL INTERFACE FAILURE\",SEV=IF"
"H323-GW1: 2000-11-27 11:25:14.012, A^ ALM=\"ENDPOINT CHANNEL INTERFACE FAILURE\",SEV=IF"

/* Listening for alarm events... (Ctrl-C to stop) */

"H323-GW1: 2000-11-27 11:25:13.259, ** ALM=\"VSC FAILURE\",SEV=MJ"

/* Ctrl-C pressed */

```

Table 6-3 Continuous Mode Messages

Element	Description
systemId	The name of your device and its identifier.
YYYY-MM-DD	The year, month, and day that the alarm or information event occurred.
hh-mm-ss-ms	The hour, minute, second, and millisecond that the alarm or information event occurred.
severity	<p>The severity level of the alarm or information event. Severity is represented by a two-character indicator with the following meanings:</p> <ul style="list-style-type: none"> • *C—Critical alarm. Critical alarms indicate that a serious problem exists in the network. Critical alarms cause a restart or reboot of the Cisco HSI. Clear critical alarms immediately. • **—Major alarm. Major alarms indicate that a problem that disrupts service exists. Clear major alarms immediately. Major alarms differ from critical alarms in that they do not initiate automatic recovery processes. • *^—Minor alarm. Minor alarms indicate a problem that does not disrupt service. Minor alarms should be noted and cleared as soon as possible. • A^—Informational event. Informational events indicate atypical network conditions, such as timer expirations, values that have exceeded preset thresholds, or unexpected responses from end points to signaling messages sent by the Cisco HSI. • — (Empty spaces in two leftmost columns). The alarm or event has been cleared. “STATE=CLEARED” is displayed.
almCat	<p>Alarm category. A text string that indicates whether the message is an alarm or an informational event and the MML alarm or event message. See Table 6-4 for a list of alarm categories.</p> <p>Note Despite its name, the alarm category field is used for both alarms and informational events.</p>
Acknowledgement	Determines whether the alarm has been acknowledged.

Acknowledging and Clearing Alarms

To acknowledge that an alarm is recognized but not cleared, use the **ack-alm** MML command. See [Appendix A, “MML Commands,”](#) for more information.

To clear an alarm, use the **clr-alm** MML command. See [Appendix A, “MML Commands,”](#) for more information.

Alarms List

Table 6-4 lists the alarms and information events. Troubleshooting information for each of the alarms and information events can be found in the “Troubleshooting” section on page 6-6.

Table 6-4 Alarms and Informational Events

Alarm Events and Reference	Severity Level
H323_STACK_FAILURE , page 6-6	Critical
CONFIGURATION_FAILURE , page 6-6	Major
EISUP_PATH_FAILURE , page 6-7	Major
GATEKEEPER_INTERFACE_FAILURE , page 6-8	—
GENERAL_PROCESS_FAILURE , page 6-8	Major
IP_LINK_FAILURE , page 6-8	Major
LOW_DISK_SPACE , page 6-9	Major
OVERLOAD_LEVEL3 , page 6-9	Major
VSC_FAILURE , page 6-10	Major
OVERLOAD_LEVEL2 , page 6-11	Minor
CONFIG_CHANGE , page 6-11	Information
ENDPOINT_CALL_CONTROL_INTERFACE_FAILURE , page 6-12	Information
ENDPOINT_CHANNEL_INTERFACE_FAILURE , page 6-12	Information
GAPPED_CALL_NORMAL , page 6-13	Information
GAPPED_CALL_PRIORITY , page 6-13	Information
OVERLOAD_LEVEL1 , page 6-14	Information
PROVISIONING_INACTIVITY_TIMEOUT , page 6-14	Information
PROVISIONING_SESSION_TIMEOUT , page 6-15	Information
STOP_CALL_PROCESSING , page 6-15	Information

Troubleshooting

This section provides troubleshooting procedures for the alarms listed in [Table 6-4](#).

H323_STACK_FAILURE

Description

Irrecoverable failure in the RADVision stack. This alarm is reported to the management interface and can be obtained with SNMP.

Severity Level and Trap Type

The severity level is critical. The trap type is 4.

Cause

The H.323 RADVision stack has failed to correctly initialize on an application startup. An automatic application restart is initiated, and the application reverts to the base configuration data.

Troubleshooting

To clear the H.323 stack failure alarm, complete the following steps:

-
- Step 1 Allow the application to restart and revert back to the base configuration data that is known to be reliable.
 - Step 2 Review the H323_SYS parameters in a provisioning session, ensuring that the values are correct and within the memory limits of the machine.
 - Step 3 Use the **prov-cpy** MML command to recommit the new H323_SYS parameters.
 - Step 4 Use the **restart-softw** MML command to initiate a software restart.
 - Step 5 Use the **rtrv-alm**s MML command to check the alarm list to see if the H.323 stack correctly initializes.
-

CONFIGURATION_FAILURE

Description

The configuration has failed. This alarm is reported to the management interface and can be obtained with SNMP.

Severity Level and Trap Type

The severity level is major. The trap type is 4.

Cause

A major error has occurred in the configuration of the software packages. This is a potentially nonrecoverable situation that requires an application restart.

Troubleshooting

To clear the CONFIGURATION_FAILURE alarm, complete the following steps:

-
- Step 1** Use the **restart-softw:init** command to restart the application and revert to the base configuration.
 - Step 2** Review the modified parameters and ensure that the values are correct.
 - Step 3** Use the **prov-cpy** MML command to recommit the new parameters.
 - Step 4** Use the **restart-softw** MML command to initiate a software restart.
 - Step 5** Use the **rtrv-alm**s MML command to check the alarm list to see if the problem has been resolved.
-

EISUP_PATH_FAILURE

Description

A failure of the RUDP layer has occurred. This alarm is reported to the management interface and can be obtained with SNMP.

Severity Level and Trap Type

The severity level is major. The trap type is 4.

Cause

Both IP links A and B to a single Cisco PGW 2200 have gone down.

Troubleshooting

To clear the EISUP_Path_Failure alarm, complete the following steps:

-
- Step 1** Use the **rtrv-dest** command to assess which Cisco PGW 2200 (standby or active) has been lost.
 - Step 2** Check the network connections, cables, and routers.
 - Step 3** Use the **clr-alm**s MML command to attempt to clear the alarm.
-

GATEKEEPER_INTERFACE_FAILURE

This alarm has not been implemented.

GENERAL_PROCESS_FAILURE

Description

A general process failure has occurred. This alarm is reported to the management interface and can be obtained with SNMP.

Severity Level and Trap Type

The severity level is major. The trap type is 4.

Cause

The Cisco HSI (GWmain program) quit unexpectedly (that is, there were no requests to stop or restart the application). The process manager (PMmain) raises the GENERAL_PROCESS_FAILURE alarm so that a trap is sent to the Rambler.

The process manager clears the GENERAL_PROCESS_FAILURE alarm when it restarts the Cisco HSI (GWmain).

Troubleshooting

To trace the problem, look at either the core file or the log files.

IP_LINK_FAILURE

Description

A failure of the IP link has occurred. This alarm is reported to the management interface and can be obtained with SNMP.

Severity Level and Trap Type

The severity level is major. The trap type is 4.

Cause

One of the two links to a single Cisco PGW 2200 has failed.

Troubleshooting

To clear the IP link failure alarm, complete the following steps:

-
- | | |
|---------------|--|
| Step 1 | Use the rtrv-dest command to assess which PGW 2200 (standby or active) has been lost. |
| Step 2 | Check the network connections, cables, and routers. |
| Step 3 | Use the clr-alm MML command to attempt to clear the alarm. |
-

LOW_DISK_SPACE

Description

The disk space is low. This alarm is reported to the management interface and can be obtained with SNMP. The alarm automatically clears when the disk usage decreases below the alarm limit.

Severity Level and Trap Type

The severity level is major. The trap type is 4.

Cause

The percentage of disk usage is greater than the alarm limit.

Troubleshooting

To obtain more disk space, remove old versions of installed software that are no longer required, or archive log files from the *\$GWHOME/var/log* directory, for example.

OVERLOAD_LEVEL3

Description

An overload level 3 condition exists. This alarm is reported to the management interface and can be obtained with SNMP. This alarm automatically clears when the CPU occupancy or the number of active calls drops below the lower limits set in the overload configuration for level 3.

Severity Level and Trap Type

The severity level is major. The trap type is 4.

Cause

The OVERLOAD_LEVEL3 alarm is triggered when the CPU occupancy or the number of active calls rises above the upper limits set in the overload configuration for level 3. Gapping is then initiated.

Troubleshooting

To clear the OVERLOAD_LEVEL3 alarm, complete the following steps:

-
- Step 1 Wait for the number of calls to drop.
 - Step 2 If CPU occupancy remains high, request assistance from the system administrator.
-

VSC_FAILURE

Description

This alarm is derived by the Cisco HSI application from RUDP/SM events. This alarm is reported to the management interface and can be obtained with SNMP.

Severity Level and Trap Type

The severity level is major. The trap type is 5.

Cause

Links to both (active and standby) Cisco PGW 2200s have gone down.

Troubleshooting

To clear the VSC_FAILURE alarm, complete the following steps:

-
- Step 1 Use the **rtrv-dest** command to confirm that links to the Cisco PGW 2200s have gone down.
 - Step 2 Check the network connections, cables, and routers.
 - Step 3 Refer to the *Cisco Media Gateway Controller Software Release 9 Operations, Maintenance, and Troubleshooting Guide* for detailed information about this alarm.
 - Step 4 Use the **clr-alm** command to attempt to clear the alarm.
-

OVERLOAD_LEVEL2

Description

An overload level 2 condition exists. This alarm is reported to the management interface and can be obtained with SNMP. This alarm automatically clears when the CPU occupancy or the number of active calls drops below the lower limits set in the overload configuration for level 2.

Severity Level and Trap Type

The severity level is minor. The trap type is 4.

Cause

The OVERLOAD_LEVEL2 alarm is triggered when the CPU occupancy or the number of active calls rises above the upper limits set in the overload configuration for level 2. Gapping is then initiated.

Troubleshooting

To clear the OVERLOAD_LEVEL2 alarm, complete the following steps:

-
- | | |
|---------------|--|
| Step 1 | Wait for the number of calls to drop. |
| Step 2 | If CPU occupancy remains high, request assistance from the system administrator. |
-

CONFIG_CHANGE

Description

The running configuration has been modified.

Severity Level and Trap Type

The severity level is information. The trap type is 0.

Cause

A new configuration has been activated within a provisioning session.

Troubleshooting

This is an informational event.

ENDPOINT_CALL_CONTROL_INTERFACE_FAILURE

Description

An individual call failure has occurred. This informational event is reported to the management interface and can be obtained with SNMP.

Severity Level and Trap Type

The severity level is information. The trap type is 3.

Cause

The RADVision stack reports this alarm.

Troubleshooting

This is an informational event.

ENDPOINT_CHANNEL_INTERFACE_FAILURE

Description

An individual call failure has occurred. This informational event is reported to the management interface and can be obtained with SNMP.

Severity Level and Trap Type

The severity level is information. The trap type is 3.

Cause

The RADVision stack reports this alarm.

Troubleshooting

This is an informational event.

GAPPED_CALL_NORMAL

Description

A normal call has been rejected due to call gapping. This informational event is reported to the management interface and can be obtained with SNMP.

Severity Level and Trap Type

The severity level is information. The trap type is 2.

Cause

The GAPPED_CALL_NORMAL alarm is triggered when gapping levels cause a normal call to be rejected.

Troubleshooting

To clear the GAPPED_CALL_NORMAL informational event, complete the following steps:

-
- Step 1 Use the **rtrv-gapping** MML command to retrieve gapping information.
 - Step 2 If the MML-specific gap levels are active, use the **set-gapping** MML command to modify them.
 - Step 3 If the overload-specific gap levels are active, either modify the provisioned overload gapping percent levels or reduce the cause of the overload (see [OVERLOAD_LEVEL1](#), page 6-14, [OVERLOAD_LEVEL2](#), page 6-11, and [OVERLOAD_LEVEL3](#), page 6-9).
-

GAPPED_CALL_PRIORITY

Description

A priority or emergency call has been rejected due to call gapping. This informational event is reported to the management interface and can be obtained with SNMP.

Severity Level and Trap Type

The severity level is information. The trap type is 2.

Cause

The GAPPED_CALL_NORMAL alarm is triggered when gapping levels cause a priority or emergency call to be rejected.

Troubleshooting

To clear the GAPPED_CALL_PRIORITY informational event, complete the following steps:

-
- Step 1 Change the MML gapping levels to less than 100 percent and change the call type to normal.
 - Step 2 Change the provisioned overload call filter type to normal.
-

OVERLOAD_LEVEL1

Description

An overload level 1 condition exists. This informational event is reported to the management interface and can be obtained with SNMP.

Severity Level and Trap Type

The severity level is information. The trap type is 4.

Cause

The OVERLOAD_LEVEL1 alarm is triggered when the CPU occupancy or the number of active calls rises above the upper limits set in the overload configuration for level 1. Gapping is then initiated.

Troubleshooting

To clear the OVERLOAD_LEVEL1 informational event, complete the following steps:

-
- Step 1 Wait for the number of calls to drop.
 - Step 2 If CPU occupancy remains high, request assistance from the system administrator.
-

PROVISIONING_INACTIVITY_TIMEOUT

Description

A provisioning session has been inactive for 20 minutes. The text of the output is:

```
"H323-GW1:2001-01-30 11:12:57.421,A^ ALM="\PROVISIONING INACTIVITY TIMEOUT\","SEV=IF"
```

Severity Level and Trap Type

The severity level is information. The trap type is 3.

Cause

The provisioning session has been inactive for 20 minutes. The provisioning session will be closed if there is no activity within the next 5 minutes.

Troubleshooting

Ensure that activity in the provisioning session occurs at least every 20 minutes.

PROVISIONING_SESSION_TIMEOUT

Description

The current session has been terminated. The text of the output is:

```
"H323-GW1:2001-01-30 11:17:57.422,A^ ALM=\"PROVISIONING SESSION  
TIMEOUT\" ,SEV=IF"
```

Severity Level and Trap Type

The severity level is information. The trap type is 3.

Cause

The provisioning session has been inactive for longer than the time allowed.

Troubleshooting

Ensure that activity within the provisioning session occurs at least every 20 minutes.

STOP_CALL_PROCESSING

Description

A stop call processing request has been entered through the MML.

Severity Level and Trap Type

The severity level is information. The trap type is 4.

Cause

A user has entered the **stp-callproc** command through the MML.

Troubleshooting

This is an informational event.

Detailed Logging

Logging occurs on 16 different levels for each package, and the logging mask (which is a 16-bit number from 0x0000 to 0xFFFF) allows each specific log level to be turned on and off. The most-significant-bit positions correspond to higher (that is, more processor intensive) levels of debugging.

We recommend that you set the logging level of all packages to 0x0000 in a live network. For debugging a single call in an off-line network, the recommended level of debug is:

- Set Eisup, CallControl, and H323 package log levels to 0xFFFF.
- Set all other package log levels to 0x0000.
- Turn radlog on by entering the MML command **radlog::start**.

Once the test call has been made, remember to set all the logging levels back to 0x0000 and to turn radlog off by entering the MML command **radlog::stop**.