



## CHAPTER 4

# Monitoring Notifications

---

This chapter describes the Cisco 7600 Series Router notifications supported by the MIB enhancements feature introduced in Cisco IOS Release 12.3(21)BC. SNMP uses notifications to report events on a managed device. The notifications are traps or informs for different events. The router also supports other notifications not listed.

This chapter contains the following sections:

- [SNMP Notification Overview, page 4-2](#)
- [Enabling Notifications, page 4-2](#)
- [Cisco SNMP Notifications, page 4-3](#)
  - [Functional Notifications, page 4-3](#)
  - [Cisco Router Line Card Notifications, page 4-5](#)
  - [Flash Card Notifications, page 4-7](#)
  - [Link Notifications, page 4-8](#)
  - [Packet Forwarding Engine Notifications, page 4-9](#)
  - [Configuration Notifications, page 4-10](#)
  - [MPLS Service Notifications, page 4-11](#)
  - [Interface Trap Descriptions, page 4-11](#)
  - [Routing Service Notifications, page 4-15](#)
  - [SONET Notifications, page 4-16](#)
  - [Chassis Notifications, page 4-17](#)
  - [RTT Monitor Notifications, page 4-18](#)
  - [Environmental Notifications, page 4-19](#)
  - [Redundancy Framework Notifications, page 4-20](#)
  - [Cable MIB Notifications, page 4-21](#)

# SNMP Notification Overview

An SNMP agent can notify the manager when important system events occur, such as the following:

- An interface or card starts or stops running
- Temperature thresholds are crossed
- Authentication failures occur

When an agent detects an alarm condition, the agent:

- Logs information about the time, type, and severity of the condition
- Generates a notification message, which it then sends to a designated IP host

SNMP notifications are sent as either:

- Traps—Unreliable messages, which do not require receipt acknowledgement from the SNMP manager.
- Informs—Reliable messages, which are stored in memory until the SNMP manager issues a response. Informs use more system resources than traps.

To use SNMP notifications on your system, you must specify trap recipients. These recipients indicate where Network Registrar notifications are directed. Traps are enabled depending on the command `snmp-server enable traps`.

Many commands use the word traps in the command syntax. Unless there is an option in the command to select either traps or informs, the keyword **traps** refers to either traps, informs, or both. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs. The types of traps can be specified in both commands.



## Note

Most notification types are disabled by default. However, some notification types cannot be controlled with the `snmp` command. For example, some notification types are always enabled and other types are enabled by a different command. The linkUpDown notifications are controlled by the `snmp trap link-status` command. If you enter this command with no notification-type keywords, the default is to enable all notification types controlled by this command.

Specify the trap types if you don't want all traps to be sent. Then use multiple `snmp-server enable traps` commands, one for each of the trap types that you used in the `snmp host` command. The Event Table must have an entry that specifies the action that is to be performed.

For detailed information about notifications and a list of notification types, refer the following Cisco documents at:

- *The Traps Sent with SNMP-Server Enabled Traps Configured* guide at: [http://www.cisco.com/en/US/tech/tk648/tk362/technologies\\_tech\\_note09186a008021de3e.shtml](http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a008021de3e.shtml)
- “Configuring SNMP Support” section in *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* guide at: [http://www.cisco.com/en/US/docs/ios/12\\_2/configfun/configuration/guide/fcf014.html](http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html)

## Enabling Notifications

You can enable MIB notifications using either of the following procedures:

Using the command-line interface (CLI)—Specify the recipient of the trap message and specify the types of traps sent. For detailed procedures, go to the following URLs:

- *The Traps Sent with SNMP-Server Enabled Traps Configured* guide at:  
[http://www.cisco.com/en/US/tech/tk648/tk362/technologies\\_tech\\_note09186a008021de3e.shtml](http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a008021de3e.shtml)
- *Cisco IOS Software Releases 11.3, SNMP Inform Requests* guide at:  
[http://www.cisco.com/en/US/docs/ios/11\\_3/feature/guide/snmpinfrm.html](http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/snmpinfrm.html)
- Performing an SNMP SET operation with the **setany** command—To enable or disable MIB notifications, perform an SNMP SET operation on a specific object.
  - To enable the notifications set the object to true(1).
  - To disable the notifications, set the object to false(2).

For detailed procedures, go to:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/snmp.html>



**Note**

If you issue the `snmp-server enable traps` command without a notification-type argument, the router generates traps for all types of events, which might not be desirable. Some MIBs require the user to set additional objects to enable some notifications.

## Cisco SNMP Notifications

This section contains tables that describe a MIB event, why the event occurred, and a recommendation as to how to handle the event. Each table lists the following information:

- Text string—The event display
- Brief description—What the event indicates
- Probable cause—What might have caused the notification
- Recommended action—Recommendation as to what should be done when the particular notification occurs



**Note**

In the following tables, where “*no action required.*” appears in the Recommended Action column, there might be instances where an application, such as trouble ticketing, occurs.

## Functional Notifications

Table 4-1 lists notifications generated for events that might indicate the failure of the Cisco CMTS uBR router or conditions that might affect the router functionality.

Table 4-1 Environmental and Functional Notifications

Event	Description	Probable Cause	Recommended Action
<b>cefcModuleStatusChange</b>	Indicates that the status of a module has changed. A management application can use this trap to update the status of a module it manages.	Module has unknown state	Enter the show module command to view error message details. For Syslog messages associated with this event, consult Messages and Recovery Procedures.
		A line card is provisioned for a slot but it is not present in the slot.	Insert a configured line card in the specific slot.
		Module is operational	No action is required.
<b>cefcPowerStatusChange</b>	Indicates that the power status of a field replaceable unit has changed.	Module has failed due to some condition	Enter the show module command to view error message details. For Syslog messages associated with this event, consult Messages and Recovery Procedures.
		FRU is powered off because of an unknown problem.	Enter the show power command to check the actual power usage. For Syslog messages associated with this event, consult Messages and Recovery Procedures
		FRU is powered on	No action is required.
<b>cefcFRUInserted</b>	Indicates that a FRU was inserted. The trap indicates the entPhysicalIndex of the slot that the line card was inserted in.	FRU is administratively off	No action is required.
		FRU is powered off because available system power is insufficient	Enter the show power command to check the actual power usage.
		A new field replaceable unit like a line card, SIP and SPA modules, fan, port, power supply, or redundant power supply was added.	No action is required; but you can enable this trap through the CLI or by setting cefcMIBEnableStatusNotification to true(1).
<b>cefcFRURemoved</b>	Indicates that a FRU was removed and indicates the entPhysicalIndex of the slot from which the line card was removed.	A field replaceable unit like line cards, SIP and SPA modules, fan, ports, power supply, or redundant power supply was removed.	Replace the field replaceable unit.
<b>chassisAlarmOn</b>	Indicates that a FRU status has changed.	The chassis temperature is too high, a minor or major alarm has been detected.	Inspect the indicated component closely to determine why it is operating out of the normal operating temperature range and whether it will eventually exceed the allowed operating temperature range.
		A redundant power supply has been powered off.	Replace the field replaceable unit.

**Table 4-1** Environmental and Functional Notifications (continued)

Event	Description	Probable Cause	Recommended Action
	Router's cooling fan could be close to failure.	One or more fans in the system fan tray have failed. Although this is a minor alarm, system components could overheat and be shut down.	Replace the fan as soon as possible or the system might shut itself down or fail to operate properly.
<b>chassisAlarmOff</b>	Indicates that a FRU status has changed.	A redundant power supply has been powered on.	No action required.
RAM to CPU Usage	<b>TBD</b>		

## Cisco Router Line Card Notifications

These notifications indicate the failure of a line card or error conditions on the card that might affect the functionality of all interfaces and connected customers.

[Table 4-2](#) lists ENTITY-MIB notifications generated by Cisco CMTS uBR router cards and SPAs.

**Table 4-2** Line Card Notifications

Event	Description	Probable Cause	Recommended Action
<b>entConfigChange</b>	An entry for the line card or a shared port adapter is removed from the entPhysicalTable (which causes the value of entLastchangeTime to change).	A line card was removed.	Replace the field replaceable unit.
<b>cefcModuleOperStatus</b>	Indicates that the line card operational state changed. A management application uses this trap to update the status of a module that it is managing.	A line card is provisioned for a slot but it is not present in the slot.	Add a module.
<b>entSensorThresholdNotification</b>	Indicates that the sensor value crossed the threshold. This notification reports the most recent measurement seen by the sensor and this notification indicates the value of the threshold.	The sensor value in a module crossed the threshold listed in entSensorThresholdTable. This notification is generated once each time the sensor value crosses the threshold.	Remove the configuration that bypasses the module shutdown due to sensor thresholds being exceeded. Shut down the module after removing the configuration. It exceeded major sensor thresholds.

Table 4-2 Line Card Notifications (continued)

Event	Description	Probable Cause	Recommended Action
		The local CPU was unable to access the temperature sensor on the module. The module will attempt to recover by resetting itself.	Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.
<b>ceAlarmAsserted</b>	The agent generates this trap when a physical entity asserts an alarm, such as the power entry module 0 failure.	You manually shut down the line card, then you get the line card error or the alarm <i>Card Stopped Responding OIR</i> occurs.	Check the entPhysicalDescr type and take the corresponding action; because there are many types of asserted alarms.
<b>ceAlarmCleared</b>	The agent generates this trap when a physical entity clears a previously asserted alarm or when the core or inlet temperature crosses a threshold, such as inlet critical temperature limit.	The agent generates this trap when: <ul style="list-style-type: none"> <li>a physical entity clears a previously asserted alarm</li> <li>a line card is installed in a slot and the alarm <i>Active Card Removed OIR</i> is cleared.</li> </ul>	

## Notes:

- \* Sensor entities are the physical entities whose entity class must be defined to type entity sensor(8) in the entPhysicalTable.
- \* Notifications happen only if the particular entity has an entry in entity table.
- \* If ceAlarmNotifiesEnable is set to 0, it disables ceAlarmAsserted and ceAlarmCleared notifications. Similarly, when ceAlarmSyslogEnable is set to 0, it disables syslog messages corresponding to alarms.
- \* If ceAlarmHistTableSize is set to 0, it prevents any history from being retained in the ceAlarmHistTable. In addition whenever the ceAlarmHistTableSize is reset (either increased or decreased) the existing log is deleted.
- \* When a new alarm condition is detected, the carrier alarm LEDs in the individual line cards are currently set by the line card software. The IOS alarm subsystem does not control the LEDs.

RAM to CPU Usage

**TBD**

## Flash Card Notifications

Table 4-3 lists CISCO-FLASH-MIB notifications generated by Cisco CMTS uBR router flash cards. These notifications indicate the failure of a flash card or error conditions on the card that might affect the functionality of all interfaces and connected custom

**Table 4-3** Flash Card Notifications

Event	Description	Probable Cause	Recommended Action
<b>ciscoFlashDeviceChangeTrap</b>	Indicates a removable flash device was inserted into the router.	Status change occurred when a removable flash card is inserted in the router.	To determine which flash card was inserted, use the <code>ciscoFlashDeviceIndex</code> to check the <code>ciscoFlashDeviceTable</code> .
<b>entConfigChange</b>	<p>This is generated every time a conceptual row is created, modified, or deleted in any of the following tables:</p> <ul style="list-style-type: none"> <li>• <code>entPhysicalTable</code></li> <li>• <code>entLogicalTable</code></li> <li>• <code>entLPMappingTable</code></li> <li>• <code>entAliasMappingTable</code></li> <li>• <code>entPhysicalContainsTable</code></li> </ul> <p>That means a new device (flash or any card) is added or removed from the router.</p> <p>And the <code>entLastChangeTime</code> is the <code>sysUpTime</code> at the time a flash card is added or deleted.</p>	Status change occurred when a flash card was added or removed.	To determine which flash card was removed from the router, use the <code>ciscoFlashDeviceIndex</code> to check the <code>ciscoFlashDeviceTable</code> .
<b>ciscoFlashCopyCompletionTrap</b> <b>ciscoFlashPartitioningCompletionTrap</b> <b>ciscoFlashMiscOpCompletionTrap</b>	Indicates that a flash operation has occurred.	<p>Sent when the following flash operations occur:</p> <ul style="list-style-type: none"> <li>• copy operation finishes</li> <li>• partitioning operation finishes</li> <li>• miscellaneous flash card operation finishes</li> </ul>	Enable this trap through the CLI or setting the corresponding flash object to <code>true(1)</code> .

## Link Notifications

Table 4-4 lists notifications generated by the router for link-related (interface) events.

**Table 4-4** *Interface Notifications*

Event	Description	Probable Cause	Recommended Action
<b>linkDown</b>	<ul style="list-style-type: none"> <li>Indicates that a link is about to enter the Down state, which means it can not transmit or receive traffic. The ifOperStatus object shows the link's current state. Value is down(2).</li> <li>Indicates that the wideband downstream ports on the SPA are in a down state.</li> </ul>	An internal software error might have occurred.	<p>To see if link traps are enabled or disabled on an interface, check ifLinkUpDownTrapEnable (IF-MIB) for the interface. To enable link traps, set ifLinkUpDownTrapEnable to enabled(1).</p> <p>Enable the IETF (RFC 2233) format of link traps by issuing the CLI command <b>snmp-server trap link ietf</b>.</p>
<b>linkUp</b>	<ul style="list-style-type: none"> <li>Indicates that a link is about to enter the Up state and the ifOperStatus object shows the link's current status.</li> <li>Indicates that the wideband downstream ports on the SPA are in a up state.</li> </ul>	The port manager reactivated a port in the link-down state during a switchover.	<p>To see if link traps are enabled or disabled on an interface, check ifLinkUpDownTrapEnable (IF-MIB) for the interface. To enable link traps, set ifLinkUpDownTrapEnable to enabled(1).</p> <p>Enable the IETF (RFC 2233) format of link traps by issuing the CLI command <b>snmp-server trap link ietf</b>.</p>

## Packet Forwarding Engine Notifications

Table 4-5 lists notifications generated by the router for Packet Forwarding Engine (PFE) events on the Cisco uBR10012 router. The Cisco uBR10012, the PFE is the parallel express forwarding network processor (PXF), which is part of the performance routing engine (PRE).

**Table 4-5** Packet Forwarding Engine Notifications

Event	Description	Probable Cause	Recommended Action
<b>cePfeHistThldEvent</b> Objects: <ul style="list-style-type: none"> <li>cePfeHistEntPhysIndex,</li> <li>cePfeHistType,</li> <li>cePfeHistThld,</li> <li>cePfeHistValue</li> </ul>	Indicates that the configured threshold is crossed. The threshold value and the type are found from the cePfeHistType and cePfeHistThld. And the event type can be any of the enumerations of the HistEventType.	A threshold event has occurred and the cePfeHistNotifiesEnable is set to notify(3) or logAndNotify(4).	After generation this notification, another notification is not sent out until the sample value falls below the threshold value.
<b>HistEventType</b> <ul style="list-style-type: none"> <li>thldUtilizationEvent</li> <li>thldEfficiencyEvent</li> <li>thld1MinUtilizationEvent</li> <li>thld1MinEfficiencyEvent</li> </ul>	Generated if the cePfePerfCurrentUtilization, at the time of sampling, becomes greater than or equal to the cePfePerfThldUtilization  Generated if the cePfePerfCurrentEfficiency, at the time of sampling, becomes less than or equal to the cePfePerfThldEfficiency.  Generated if the cePfePerfCurrent1MinUtilization, at the time of sampling, becomes greater than or equal to the cePfePerfThld1MinUtilization.  Generated if the cePfePerfCurrent1MinEfficiency, at the time of sampling, becomes less than or equal to the cePfePerfThld1MinEfficiency.		

**Table 4-5** Packet Forwarding Engine Notifications (continued)

Event	Description	Probable Cause	Recommended Action
<ul style="list-style-type: none"> <li>thld5MinUtilizationEvent</li> <li>thld5MinEfficiencyEvent</li> </ul>	<p>Generated if the cePfePerfCurrent5MinUtilization, at the time of sampling, becomes greater than or equal to the cePfePerfThld5MinUtilization.</p> <p>Generated if the cePfePerfCurrent5MinEfficiency, at the time of sampling, becomes less than or equal to the cePfePerfThld5MinEfficiency.</p>		
<b>cePfeHistRestartEvent</b>	Indicates a PFE restart occurred.	The PFE processor restarted	Enable this trap using the CLI <b>snmp-server</b> command or by setting cePfeHistNotifiesEnable to notify(3) or logAndNotify(4)

## Configuration Notifications

Table 4-6 lists notifications generated by the CMTS router for events related to system configuration.

**Table 4-6** CMTS Configuration Notifications

Event	Description	Probable Cause	Recommended Action
<b>ccCopyCompletion</b> <ul style="list-style-type: none"> <li>ccCopyServerAddress</li> <li>ccCopyFileName</li> <li>ccCopyState</li> <li>ccCopyTimeStarted</li> <li>ccCopyTimeCompleted</li> <li>ccCopyFailCause</li> </ul>	A ccCopyCompletion trap is sent when a config-copy request is completed. The ccCopyFailCause is not instantiated, and hence not included in a trap, when the ccCopyState is successful.	Sent when the CMTS router finishes copying a configuration file to or from another location.	Enable this trap by setting ccCopyNotificationOnCompletion to true(1).
<b>ciscoConfigManEvent</b>	The current configuration changed.	Sent when the running configuration changes.	No action required.

## MPLS Service Notifications

Table 4-7 lists service notifications generated by the CMTS router to indicate conditions for services.

Table 4-7 *MPLS-Service Notifications*

Event	Description	Probable Cause	Recommended Action
<b>mplsTunnelUp</b>	Indicates that a mplsTunnelOperStatus object for a configured tunnel is about to transition from the Down state to any state except NotPresent.	A configured tunnel transitioned from the Down state to any state except NotPresent. May be caused by an administrative or operational status check of the tunnel.	No action is required. Enable this trap through the CLI or by setting mplsTunnelTrapEnable to true(1)>
<b>mplsTunnelDown</b>	Indicates that the mplsTunnelOperStatus object for a configured MPLS traffic engineering tunnel is about to transition to the up(1) or the down(2) respectively.	A configured tunnel is transitioning to the down state. May be caused by an administrative or operational status check of the tunnel.	
<b>mplsTunnelRerouted</b>	Indicates that the signalling path for an MPLS traffic engineering tunnel changed.	A tunnel was rerouted or reoptimized.	If you use the actual path, then write the new path to mplsTunnelRerouted after the notification is issued.

## Interface Trap Descriptions

### To be provided

Admin Status of Interface Up/Down

Admin Status of Subinterface Up/Down

**Table 4-8** *Interface and Subinterface Traps*

Event	Trap and Trap Objects	Notes
Admin Status of Interface Up/Down	-MIB	
	•	
	-MIB	
	•	
	-MIB	
	•	
Admin Status of Subinterface Up/Down	-MIB	
	•	
	-MIB	
	•	

## Routing Protocol Notifications

Table 4-9 lists notifications generated by the Cisco CMTS uBR router to indicate error conditions for routing protocols.

**Table 4-9** Routing Protocol Notifications

Event	Description	Probable Cause	Recommended Action
<b>bgpEstablished</b>	The BGP FSM enters the ESTABLISHED state. It becomes active on the router.	The BGP routing protocol changed status.	No action is required.
<b>bgpBackwardTransition</b>	Indicates that the BGP protocol transitions from a higher-level state to a lower-level state. The prefix count for an address family on a BGP session exceeded the configured threshold value.	The BGP routing protocol changed status.	This threshold value is configured using the CLI command, <b>neighbor &lt;nbr_addr&gt; &lt;max_prefixes&gt; [threshold] [warning-only]</b>
<b>oamLoopbackPingCompletionTrap</b>	Indicates a loopback test.	Sent when an OAM loopback test completes.	Enable this trap through the CLI or by setting <b>oamLoopbackPingTrapOnCompletion</b> to true(1).
<b>cPppoeSystemSessionThresholdTrap</b>	Indicates that the PPPoE system session exceeded a threshold.	Sent when the number of active PPPoE sessions exceeds the value of <b>cPppoeSystemThresholdSessions</b> .	Enable this trap through the CLI.
<b>cPppoeVcSessionThresholdTrap</b>	Indicates that the PPPoE VC session exceeded a threshold.	Sent when the number of active PPPoE sessions on the VC exceeds the value of <b>cPppoeVcThresholdSessions</b> .	Enable this trap through the CLI.

## Interface Trap Descriptions

### To be provided

Admin Status of Interface Up/Down

Admin Status of Subinterface Up/Down

**Table 4-10** *Interface and Subinterface Traps*

Event	Trap and Trap Objects	Notes
Admin Status of Interface Up/Down	-MIB	
	•	
	-MIB	
	•	
	-MIB	
	•	
Admin Status of Subinterface Up/Down	-MIB	
	•	
	-MIB	
	•	

## Routing Service Notifications

Table 4-11 lists notifications generated by the Cisco CMTS uBR router to indicate error conditions for routing services.

**Table 4-11** Routing Protocol Notifications

Event	Description	Probable Cause	Recommended Action
<b>casServerStateChange</b>	<p>The casState object changes status.</p> <p>The object casState does not necessarily indicate the current state of the server. This is because casState is always up(1) unless an AAA request fails. In that case, casState is set to dead(2) and then reset to up(1) to allow the router to send requests to the server after a failure.</p> <p>The number of minutes casState remains dead(2) is specified by the radius-server deadtime minutes command. For example, if server deadtime is 5 minutes and an AAA request fails, a trap is generated with casState set to dead(2). Five minutes later, another trap is generated with casState set to up(1) even though the server may still be down.</p>	<p>Sent when the casState object changes state. The value of casState indicates if the router should send requests to the authentication, authorization, and accounting (AAA) server:</p> <ul style="list-style-type: none"> <li>• up(1)—Send requests to the server.</li> <li>• dead(2)—Do not send requests to the server. Send requests to the next available server instead.</li> </ul>	<p>Enable this trap by setting casServerStateChangeEnable to true(1).</p>
<b>ciscoSsgRadiusClientReboot</b>	<p>Sent when the Service Selection Gateway (SSG) detects that a RADIUS client has rebooted. (SSG uses RADIUS servers to authenticate subscribers.)</p>	<p>A RADIUS client has rebooted.</p>	<p>Enable this trap by setting ssgCfgRadiusClientRebootNotification to true(1).</p>

## SONET Notifications

Table 4-12 lists alarm notifications generated by the router for SONET events.

**Table 4-12** SONET Notifications

Event	Description	Probable Cause	Recommended Action
<b>ceAssertAlarm</b> <b>ceClearAlarm</b>	<p>These notifications indicate error conditions on a SONET circuit and the status of SONET layers.</p> <p>Note that not all SONET and Packet over SONET (POS) line cards generate all of the traps.</p>	Sent when one of the following alarm status has changed. See footnote below.	Check out the AlarmType and ceAlarmHistSeverity values.
<p>Paths, for example a Path Alarm Indication Signal</p> <p>Line, for example a Line Remove Failure Indication</p> <p>Section, for example a Section Loss of Frame Failure</p> <p>Clock problems, for example a Far End Clock Out of Range</p> <p>Signal, for example a Out of Frame Failure</p> <p>Near End/Far End, for example a Far End Alarm Indication Signal</p> <p>Thresholds, for example a Threshold Cross Alarm-B1</p>			

## Chassis Notifications

Table 4-13 lists CISCO-STACK-MIB notifications generated by the router to indicate that a chassis module has become active or stopped responding. These notifications are supported by the Cisco CMTS router.

**Table 4-13** Chassis Notifications

Event	Description	Probable Cause	Recommended Action
<b>moduleDown</b>	The status of a module changes from the OK state to another state.	The agent entity has detected that the moduleStatus object in this MIB has transitioned out of the ok (2) state for one of its modules. The generation of this trap can be controlled by the sysEnableModuleTraps object in this MIB.	Replace module.
<b>moduleUp</b>	The status of a module changes to the OK state.	The agent entity has detected that the moduleStatus object in this MIB has transitioned to the ok (2) state for one of its modules. The generation of this trap can be controlled by the sysEnableModuleTraps object in this MIB.	No action required.

## RTT Monitor Notifications

Table 4-14 lists CISCO-RTTMON-MIB notifications that can occur during round-trip time (RTT) monitoring.

**Table 4-14** RTT Monitor Notifications

Event	Description	Probable Cause	Recommended Action
<b>rttMonConnectionChangeNotification</b>	Sent when the value of <code>rttMonCtrlOperConnectionLostOccurred</code> changes.	Occurs when the connection to a target has either failed to be established or was lost and then re-established. Note that this is a connection to a target not to a hop in the path to the target.	Check for the connectivity to the target. There could be link problems to the target through different hops.
<b>rttMonTimeoutNotification</b>	A timeout occurred or was cleared during an RTT probe.	An RTT probe occurred and the system sends the notice when the value of <code>rttMonCtrlOperTimeoutOccurred</code> changes.	Check for the end-to-end connectivity if <code>rttMonCtrlOperTimeoutOccurred</code> if the notification returns true.  No action is required if <code>rttMonCtrlOperTimeoutOccurred</code> is false.
<b>rttMonThresholdNotification</b>	Threshold violation occurred during an RTT probe.	Indicates that the previous violation has subsided for a subsequent RTT operation, which results in <code>rttMonCtrlOperOverThresholdOccurred</code> changing value.	Check for the end-to-end connectivity if <code>rttMonCtrlOperOverThresholdOccurred</code> in the notification is true otherwise no action required.

## Environmental Notifications

Table 4-15 lists CISCO-ENVMON-MIB notifications generated for events that might indicate the failure of the Cisco CMTS uBR router or conditions that might affect the router's functionality.

**Table 4-15** Environmental Notifications

Event	Description	Probable Cause	Recommended Action
<b>ciscoEnvMonShutdownNotification</b>	<p>A ciscoEnvMonShutdown Notification is sent if the environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown.</p> <p>This notification contains no objects so that it may be encoded and sent in the shortest amount of time possible. Management applications should not rely on receiving such a notification as it may not be sent before the shutdown completes.</p>	<p>A test point nears a critical state and the router is about to shut down (for example, if auto-shutdown is enabled and the chassis core or inlet temperature reaches critical state and remains there for more than 2 minutes).</p> <p>The system has a configuration to shut down a module if its operating temperature exceeds a temperature threshold. This configuration has been bypassed, and a module will still operate in an over-temperature condition. Operating at an over-temperature condition can damage the hardware.</p>	<p>Do not override the system critical alarms like facility-alarm-intake-temperature.</p> <p>Enable this trap through the following CLI command <b>snmp-server-enable traps envmon shutdown</b> or by setting the ciscoEnvMonEnableShutdownNotification to true(1).</p>
<b>ciscoEnvMonFanNotification</b>	<p>Fan status. A ciscoEnvMonFanNotification is sent if the system detects a fan failure or an empty tray.</p>	<p>One or more fans in the system fan tray have failed, or the fan tray is missing. Although this is a minor alarm, system components could overheat and be shut down.</p>	<p>Replace the system fan tray.</p> <p>Enable this trap using the CLI <i>snmp-server-enable traps envmon fan</i> command or by setting ciscoEnvMonEnableFanNotification to true (1).</p>
<b>ciscoEnvMonRedundantSupplyNotification</b>	<p>Power supply status. Sent if the redundant power supply (if available) fails.</p>	<p>An environmental condition, an over-temperature condition, or inconsistent voltage to the module occurred. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification.</p>	<p>Ensure that the system power supplies are optimally redundant.</p> <p>Use power supplies with identical output ratings or reduce system power consumption.</p> <p>Enable this trap using the CLI <b>snmp-server enable traps envmon supply</b> command or by setting ciscoEnvMonEnableRedundantSupplyNotification to true (1).</p>

Table 4-15 Environmental Notifications (continued)

Event	Description	Probable Cause	Recommended Action
<code>ciscoEnvMonTempStatusChangeNotif</code>	<p>Temperature status. The core or inlet temperature is outside its normal range, when <code>ciscoEnvMonState</code> is at the Warning or Critical state.</p> <p>Since such a Notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the <code>ciscoEnvMonShutdownNotification</code>.</p>	<p>During previous reloads, this module experienced a timeout while accessing the temperature sensor. All further access to the temperature sensor will be disabled. This condition indicates a possible problem with the temperature sensor.</p>	<p>Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.</p> <p>Enable this trap using the CLI <code>snmp-server enable traps envmon temperature</code> command or by setting <code>ciscoEnvMonEnableTemperatureNotification</code> to true (1).</p>

\* The `cefcFRUPowerAdminStatus` is on(1) when a redundant power supply is disabled. When there is a redundant power supply, the `cefcFRUPowerAdminStatus` is always on(1) for both power supplies, regardless if the redundant power supply is disabled.

## Redundancy Framework Notifications

Table 4-16 lists CISCO-RF-MIB notifications that can occur in a redundant system. There are two types of notifications:

- Switch of Activity (SWACT)—Either a forced or automatic switch of active status from the active unit to the standby unit. The former standby unit is now referred to as the active unit.
- Progression—The process of making redundancy state of the standby unit equivalent to that of the active unit. This includes transitioning the RF state machine through several states which drives the RF clients on the active unit to synchronize any relevant data with their peer on the standby unit.

**Table 4-16 Redundancy Framework Notifications**

Event	Description	Probable Cause	Recommended Action
<b>ciscoRFSwactNotif</b>	Indicates that the RF state changed.  A switch of activity notification is sent by the newly active redundant unit.	A switch of activity occurs. If a SWACT event is indistinguishable from a reset event, then a network management station should use this notification to differentiate the activity.	If the switchover occurred due to active unit failed indicated by <code>cRFStatusLastSwactReasonCode</code> , see if there is any hardware failures, otherwise no action is required.
<b>ciscoRFProgressionNotif</b>	Indicates that the RF state changed.	The active redundant unit RF state changed or the RF state of the peer unit changed.	To avoid an increase of notifications for all state transitions, send notifications for transitions to the following RF states: <ul style="list-style-type: none"> <li>standbyCold(5)</li> <li>standbyHot(9)</li> <li>active(14)</li> <li>activeExtraload(15)</li> </ul>

## Cable MIB Notifications

Table 4-17 lists the notifications that occur in the following supported MIBs:

- DOCS-CABLE-DEVICE-TRAP-MIB
- CISCO-DOCS-REMOTE-QUERY-MIB
- CISCO-CABLE-METERING-MIB
- CISCO-DOCS-EXT-MIB

**Table 4-17 CABLE MIB Notifications**

MIB and Event	Description	Probable Cause	Recommended Action
<b>DOCS-CABLE-DEVICE-TRAP-MIB</b>			
<ul style="list-style-type: none"> <li>• docsDevCmtsInitRegReqFailTrap</li> </ul>	Indicates that a registration request failed. The failure was detected on the CMTS side.	A registration request failed during the CM initialization process.	Correct the registration request failure.
<ul style="list-style-type: none"> <li>• docsDevCmtsInitRegRspFailTrap</li> </ul>	Indicates a registration response failed. The failure was detected on the CMTS side.	A registration response failed during the CM initialization process.	Correct the registration response failures.
<ul style="list-style-type: none"> <li>• docsDevCmtsInitRegAckFailTrap</li> </ul>	Indicates a registration acknowledgement failed. The failure was detected on the CMTS side.	A registration acknowledgement failed during the CM initialization process.	Correct the registration acknowledgement failures.

Table 4-17 CABLE MIB Notifications (continued)

MIB and Event	Description	Probable Cause	Recommended Action
• docsDevCmtsDynServReqFailTrap	Indicates a dynamic service request failed. The failure was detected on the CMTS side.	A dynamic service request failed during the dynamic services process.	Correct the dynamic service request failures.
• docsDevCmtsDynServRspFailTrap	Indicates a dynamic service response failed. The failure was detected on the CMTS side.	A dynamic service response failed during the dynamic services process.	Correct the dynamic service response failures.
• docsDevCmtsDynServAckFailTrap	Indicates a dynamic service acknowledgement failed. The failure was detected on the CMTS side.	A dynamic service acknowledgement failed during the dynamic services process.	Correct the dynamic service acknowledgement failures.
• docsDevCmtsBpiInitTrap	Indicates a BPI initialization attempt failed. The failure was detected on the CMTS side.	A BPI initialization attempt failed during the CM registration process.	Correct the BPI initialization attempt failures.
• docsDevCmtsBPKMTrap	Indicates a BPKM operation failed. The failure was detected on the CMTS side.	A BPKM operation failed.	Correct the BPKM operation failures.
• docsDevCmtsDynamicSATrapTrap	Indicates a dynamic security association operation failed. The failure was detected on the CMTS side.	A dynamic security association operation failed.	Correct the dynamic security association operation failures.
• docsDevCmtsDCCReqFailTrap	A dynamic channel change request failed. The failure was detected on the CMTS side.	A dynamic channel change request failed during the dynamic channel change process	Correct the dynamic channel change request failures.
• docsDevCmtsDCCRspFailTrap	Indicates a dynamic channel change response failed. The failure was detected on the CMTS side.	A dynamic channel change response failed during the dynamic channel change process.	Correct the dynamic channel change response failures.
• docsDevCmtsDCCAckFailTrap	A dynamic channel change acknowledgement failed. The failure was detected on the CMTS side.	A dynamic channel change acknowledgement failed during the dynamic channel change process.	Correct the dynamic channel change acknowledgement failures.

**Table 4-17 CABLE MIB Notifications (continued)**

MIB and Event	Description	Probable Cause	Recommended Action
1 The following traps can be enabled using the CLI <code>snmp-server enable trap docsis-cmts</code> command.			
bpi—Enable BPI init fail trap bpkm—Enable BPKM fail trap dccack—Enable dynamic channel change acknowledgement fail trap dccreq—Enable dynamic channel change request fail trap dccrsp—Enable dynamic channel change response fail trap dsack—Enable dynamic service acknowledgement fail trap dsreq—Enable dynamic service request fail trap dsrsp—Enable dynamic service response fail trap dynsa—Enable Dynamic SA fail trap regack—Enable registration acknowledgement fail trap regreq—Enable registration request fail trap regrsp—Enable registration response fail trap			
2 The following traps can be enabled by setting the bit value in docsDevCmtsTrapControl:			
cmtsInitRegReqFailTrap( 0) cmtsInitRegRspFailTrap( 1) cmtsInitRegAckFailTrap( 2) cmtsDynServReqFailTrap( 3) cmtsDynServRspFailTrap( 4) cmtsDynServAckFailTrap( 5) cmtsBpiInitTrap( 6) cmtsBPKMTrap( 7) cmtsDynamicSATrap( 8) cmtsDCCReqFailTrap( 9) cmtsDCCRspFailTrap( 10) cmtsDCCAckFailTrap( 11)			
<b>DOCS-REMOTE-QUERY-MIB</b>			
<ul style="list-style-type: none"> <li>• cdrqCmtsCmRQDoneNotification</li> <li>• cdrqCmtsCmPollerStartTime</li> <li>• cdrqCmtsCmPollerStopTime</li> </ul>	Indicates the CMTS CM poller finished polling for the current cycle.  Indicates the time when the polling cycle started.  Indicates the time when the polling cycle finished.	CMTS CM poller started polling.  CMTS CM poller finished polling.	No action required  No action required
<b>CISCO-CABLE-METERING-MIB</b>			
<b>ccmtrCollectionNotification</b>	Indicates if the metering record file was created successfully or not and if streaming the file to the collection server was successful or not.	The receipt of this notification is an indication to the collection server that the file can be accessed through ftp or any file transfer protocol in the case of local storage.	Enable this trap by setting <code>ccmtrMeteringNotifEnable</code> to true(1)

Table 4-17 CABLE MIB Notifications (continued)

MIB and Event	Description	Probable Cause	Recommended Action
<ul style="list-style-type: none"> <li>• ccmtrCollectionStatus,</li> <li>• ccmtrCollectionDestination,</li> <li>• ccmtrCollectionTimestamp</li> </ul>	<p>Indicates the success or failure of the export.</p> <p>Indicates the destination of the export in both the success and failure scenarios.</p> <p>Indicates the timestamp of the export in both the success and failure scenarios.</p>		
<b>cdxCmtsCmDMICLockNotification</b>	Indicates a failure relating to DMIC.	Sent whenever a modem is locked because it failed the Dynamic Message Integrity Check (DMIC).	
<b>ccsSpecMgmtNotification</b>	Describes a change in status for cable hopping, modulation profile, or channel width.	Cable upstream runtime frequency (hopping), profile, or channel width status changed. See footnote below.	Use the cable upstream threshold command to change these values The CNR threshold for the secondary modulation profile defaults to 15 dB. The correctable FEC error threshold defaults to 1 percent of total packets received, and the invalid FEC error threshold defaults to 1 percent of total packets received.

1. In the case of frequency hopping, ccsUpSpecMgmtHopCondition would indicate whether SNR or modemOffline that caused the hopping.

2. Frequency hopping is based on the carrier-to-noise ratio (CNR) and the correctable FEC error and uncorrectable FEC error values. A channel will frequency hop if the CNR falls below the configurable threshold AND either the correctable or uncorrectable FEC error values exceed the configurable threshold values.

3. Channel width may be too small.