Monitoring Notifications

This chapter describes the Cisco RF Gateway-10 Router notifications supported by the MIB enhancements feature introduced in Cisco IOS Release 12.2(21)BC. SNMP uses notifications to report events on a managed device. The notifications are traps or informs for different events. The RFGW-10 also supports other notifications not listed.

This chapter contains the following sections:

- SNMP Notification Overview, page 4-1
- Enabling Notifications, page 4-2
- Cisco SNMP Notifications, page 4-2
  - Functional Notifications, page 4-3
  - Cisco RFGW-10 Line Card Notifications, page 4-4
  - Link Notifications, page 4-5
  - Configuration Notifications, page 4-6

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, see:

- The Traps Sent with SNMP-Server Enabled Traps Configured
- Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2

Enabling Notifications

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

Command line interface (CLI)—Specify the recipient of the trap message and specify the types of traps sent. This command also specifies which types of informs are enabled.

- For detailed procedures, go to:
  - http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a008021de3e.shtml
- Performing an SNMP SET operation using the **setany** command— To enable or disable MIB notifications, perform an SNMP **SET** operation on the a specific object.
  - To enable the notifications set the object to true(1)
  - To disable the notifications, set the object to false(2)

Note If you issue the snmp-server enable traps command without a notification-type argument, the RFGW-10 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* is documented, there might be instances where an application, such as trouble ticketing occurs. For detailed information, go to the following URL: http://www.cisco.com/en/US/products/sw/netmgtsw/ps996/tsd_products_support_series_home.html

Functional Notifications

Table 4-1 lists notifications generated for events that might indicate the failure of the Cisco RF Gateway-10 router or conditions that might affect the RFGW-10 functionality.

Table 4-1 Environmental and Functional Notifications

Event	Description	Probable Cause	Recommended Action
cefcModuleStatusChange	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.
		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.
cefcPowerStatusChange	Indicates that the power status of a field replaceable unit has changed.	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.
		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.

Table 4-1 Environmental and Functional Notifications (continued)

Event	Description	Probable Cause	Recommended Action
cefcFRUInserted	Indicates that a FRU was inserted. The trap indicates the entPhysicalIndex of the slot that the line card was inserted in.	A new field replaceable unit such as 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).
cefcFRURemoved	Indicates that a FRU was removed and indicates the entPhysicalIndex of the slot from which the line card was removed.	A field replaceable unit such as line cards, SIP and SPA modules, fan, ports, power supply, or redundant power supply was removed.	Replace the field replaceable unit.

Cisco RFGW-10 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 RF Gateway-10 router cards and SPAs.

Table 4-2 Line Card Notifications

Event	Description	Probable Cause	Recommended Action
entConfigChange	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.
ceAlarmAsserted	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 *Card Stopped Responding OIR* occurs.	Check the entPhysicalDescr type and take the corresponding action. Since, there are many types of asserted alarms.

Table 4-2 Line Card Notifications (continued)

Event	Description	Probable Cause	Recommended Action
ceAlarmCleared	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: • a physical entity clears a previously asserted alarm • a line card is installed in a slot and the alarm *Active Card Removed OIR* is cleared.	

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 or IOS-XE alarm subsystem does not control the LEDs.

Link Notifications

Table 4-3 lists notifications generated by the RFGW-10 for link-related (interface) events.

Table 4-3 Interface Notifications

Event	Description	Probable Cause	Recommended Action
linkDown	• 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). • Indicates that the wideband downstream ports on the SPA are in a down state.	An internal software error might have occurred.	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). Enable the IETF (RFC 2233) format of link traps by issuing the CLI command **snmp-server trap link ietf**.
linkUp	• Indicates that a link is about to enter the Up state and the ifOperStatus object shows the link's current status. • Indicates that the wideband downstream ports on the SPA are in a up state.	The port manager reactivated a port in the link-down state during a switchover.	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). Enable the IETF (RFC 2233) format of link traps by issuing the CLI command **snmp-server trap link ietf**.

Configuration Notifications

Table 4-4 lists notifications generated by the RFGW-10 for events related to system configuration.

Table 4-4 RFGW-10 Configuration Notifications

Event	Description	Probable Cause	Recommended Action
ccCopyCompletion • ccCopyServerAddress • ccCopyFileName • ccCopyState • ccCopyTimeStarted • ccCopyTimeCompleted • ccCopyFailCause	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 RFGW-10 finishes copying a configuration file to or from another location.	Enable this trap by setting ccCopyNotificationOnCompletion to true(1).
ciscoConfigManEvent	The current configuration changed.	Sent when the running configuration changes.	No action required.