Monitoring Notifications

This chapter describes the Cisco ASR 9000 Series routernotifications supported by the MIB enhancements feature introduced in Cisco IOS XR Software Release 3.7. SNMP (Simple Network Management Protocol) uses notifications to report events on a managed device. The notifications are traps for different events. The router also supports other notifications not listed.

This chapter contains the following sections:

SNMP Notification Overview

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

- 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 one of the following:

- Traps—Unreliable messages, which do not require receipt acknowledgement from the SNMP manager.

To use SNMP notifications on your system, you must specify their recipients. These recipients indicate where Network Registrar notifications are directed. By default, all notifications are enabled, but no recipients are defined. Until you define the recipients, no notifications are sent.

Many commands use the **traps** keyword in the command syntax.

Note   Most notification types are disabled by default. However, some notification types cannot be controlled with the **snmp** command. For example, some notification types can be enabled by **snmp** or CLI (command–line interface) and other types are enabled by a combination of CLI and **snmp**. The linkUpDown notifications are controlled by the **snmp trap link-status** and **snmp-server trap link ietf** commands.

Specify the trap types to avoid having all traps sent, then use multiple **snmp-server traps** commands, one for each of the trap types used in the **snmp host** command.

Enabling Notifications

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

- CLI—Specify the recipient of the trap message and specify the types of traps sent. The enabling command also specifies which types of traps are enabled. For detailed procedures, go to the following URL:

  http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/vfw/command/reference/vfr37snp.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 the following URL:
  http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/system_management/command/reference/yr37snmp.html

Note   If you issue the **snmp-server 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:

- Event—Event display

- 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 is required"* is documented, there might be instances where an application, such as trouble ticketing, occurs. For detailed information, go to:

http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/system_management/command/reference/yr37snmp.html

Environmental or Functional Notifications

Table 6-1 lists notifications generated for events that might indicate the failure of the Cisco Carrier Routing System or conditions that might affect router functionality.

Table 6-1 *Environmental or Functional Notifications*

Event	Description	Probable Cause	Recommended Action
cefcModuleStatusChange	Indicates that the status of a module has changed.	Module has unknown state.	Enter the **show platform** command to view error message details. For syslog messages associated with this event, consult Messages and Recovery Procedures.
		Module is operational.	No action is required.
		Module has failed because of 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 FRU has changed.	FRU is powered off because of unknown problem.	Enter the **show environment** 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 as the available system power is insufficient.	Enter the **show environment** command to check the actual power usage.
cefcFRUInserted	Indicates that a FRU was inserted.	A new field-replaceable unit such as a fan, transceiver, power supply, or redundant power supply was added.	No action is required.

Table 6-1   Environmental or Functional Notifications (continued)

Event	Description	Probable Cause	Recommended Action
cefcFRURemoved	Indicates that a FRU was removed.	A field-replaceable unit such as a fan, transceiver, power supply, or redundant power supply was removed.	Replace the field-replaceable unit.
cPimNbrLoss	Indicates the loss of an adjacency with a neighbor.	The neighbor timer expires, and the router has no other neighbors on the same interface with a lower IP address than itself.	Use the CLI command **show tech-support multicast address-family** {**ipv4**	**ipv6**} **vrf** *vrf-name* to gather information for the affected VRF when the traps are received.

Flash Card Notifications

Table 6-2 lists CISCO-FLASH-MIB notifications generated by Cisco Carrier Routing System 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.

Table 6-2   Flash Card Notifications

Event	Description	Probable Cause	Recommended Action
ciscoFlashDeviceInsertedNotif	Indicates a removable flash device was inserted into the router.	A removable flash device was inserted into the router.	Check for the flash card that was inserted from ciscoFlashDeviceTable. This information is also provided in the notification itself.
ciscoFlashDeviceRemovedNotif	Indicates a removable flash card was removed from the router.	A removable flash device was removed from the router.	Check the ciscoFlashDeviceTable to identify the removed flash card. This information is also provided in the notification itself.

Interface Notifications

Table 6-3 lists notifications generated by the router for link-related (interface) events.

Table 6-3   Interface Notifications

Event	Description	Probable Cause	Recommended Action
linkDown	Indicates that a link is about to enter the down state, which means it cannot transmit or receive traffic. The ifOperStatus object shows the previous state of the link. Value is down(2).	An internal software error might have occurred.	Use the CLI command, **show interface MgmtEth 0/2/CPU0/0**, to determine the cause of the interface down.
linkUp	Indicates that the link is up. The value of ifOperStatus indicates the new link state. Value is up(1).	The port manager reactivated a port in the linkdown state during a switchover.	No action is required.

Routing Protocol Notifications

Table 6-4 lists BGP4-MIB notifications that are Border Gateway Protocol (BGP) state changes generated by the Cisco Carrier Routing System to indicate error conditions for routing protocols and services.

Table 6-4   Routing Protocol Notifications

Event	Description	Probable Cause	Recommended Action
bgpEstablished	The BGP FSM[1] enters the ESTABLISHED state. It becomes active on the router.	The BGP routing protocol changed status.	No action is required.
bgpBackwardTransition	Indicates BGP protocol transition 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 **neighbor nbr_addr max_prefixes** [*threshold*] [*warning-only*]

1. FSM = finite state machine

Redundancy Framework Notifications

Table 6-5 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—Process of making the 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 clients on the active unit to synchronize any relevant data with their peer on the standby unit.

Table 6-5   *Redundancy Framework Notifications*

Event	Description	Probable Cause	Recommended Action
ciscoRFSwactNotif	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, a network management station should use this notification to differentiate the activity.	If the switchover occurred because the active unit failed (indicated by cRFStatusLastSwactReasonCode), see if there are any hardware failures; otherwise, no action is required.
ciscoRFProgressionNotif	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: • standbyCold(5) • standbyHot(9) • active(14) • activeExtraload(15)