Monitoring Notifications

This chapter describes the Cisco ASR 903 Series Aggregation Services Routers notifications supported by the MIB enhancements feature. 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 4-1
- Enabling Notifications, page 4-2
- Cisco SNMP Notifications, page 4-2

SNMP Notification Overview

An SNMP agent can notify the SNMP 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 one of the following:

- 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 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 key 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 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 command.

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 the command.

Specify the trap types if you do not 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.

For detailed information about notifications and a list of notification types, go to the following URLs:

* http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/snmpinfm.html
* http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/snmpprox.html
* http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/xdsl.html
* http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a008021de3e.shtml
* 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 and the types of informs that are enabled. For detailed procedures, go to:
    – http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a008021de3e.shtml
    – http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/snmpinfm.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)

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:

* Events—The 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." appears in the Rcommended Action column, there might be instances where an application, such as trouble ticketing occurs. Environmental or Functional Notifications

Table 4-1 lists notifications generated for events that might indicate the failure of the Cisco ASR 903 Series Router or conditions that might affect router functionality.

Table 4-1   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 due to some condition.	Enter the **show platform** 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 (FRU) has changed.	The 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.
cefcFRUInserted	Indicates that a FRU was inserted.	A new FRU, such as Cisco ASR 903 Series Router Switch Processor 1 (RSP 1), interface module, fan, transceiver, power supply, or redundant power supply was added.	No action is required.
cefcFRURemoved	Indicates that a FRU was removed.	A FRU, such as RSP1, interface module, fan, transceiver, power supply, or redundant power supply was removed.	Replace the FRU.

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

Event	Description	Probable Cause	Recommended Action
dsx1LineStatusChange	The dsx1LineStatus is a bit-map that contains loopback state and failure state information.	When a failure is detected, the corresponding dsx1LineStatus bit should change to reflect the failure. For example, when a Receiving LOS failure is detected, the corresponding bit (bit 64) should be set to indicate the failure and as a result, the dsx1LineStatus should change.	When the dsx1LineStatus reports a failure, the recommended action is correction of the conditions causing the error.
cdcVFileCollectionError	Indicates that data collection operations for a cdcVFileEntry has encountered an error.		
cdcFileXferComplete	A file transfer to the destination specified by the cdcVFileMgmtLastXferURL variable, has completed with the status specified by the cdcVFileMgmtLastXferStatus variable.	File transfer complete.	No action is required.

Table 4-2 lists ENTITY-MIB notifications generated by Cisco ASR 903 Series Router RSP cards.

Table 4-2   RSP Card Notifications

Event	Description	Probable Cause	Recommended Action
entConfigChange	An entry for the transceiver module is removed from the entPhysicalTable (which causes the value of entLastchangeTime to change).	A transceiver module was removed.	Replace the FRU.
entSensorThresholdNotification	Indicates that the sensor value crossed the threshold. This variable reports the most recent measurement seen by the sensor and the threshold value.	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. **Note** The command that shuts down the module in the event of a major sensor alarm has been overridden, so the specified module will not be shut down. The command used to override the shutdown is **no environment-monitor shutdown**.
		The local CPU on the RSP 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.
ceAlarmAsserted	The agent generates this trap when a physical entity asserts an alarm.	You manually shut down the IM, then you get the IM error.	Check the entPhysicalDescr type and take the corresponding action; there are many types of asserted alarms.

Table 4-2   RSP Card Notifications (continued)

Event	Description	Probable Cause	Recommended Action
ceAlarmCleared	The agent generates this trap when a physical entity clears a previously asserted alarm.	The agent generates this trap when a physical entity clears a previously asserted alarm.	No action is required.

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 the 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..

Flash Device Notifications

Table 4-3 lists CISCO-FLASH-MIB notifications generated by Cisco ASR 903 Series Router flash devices. These notifications indicate the failure of a flash device or error conditions on the device.

Table 4-3   Flash Device Notifications

Event	Description	Probable Cause	Recommended Action
ciscoFlashDeviceChangeTrap	Indicates a removable flash device was inserted into the router.	Status change occurred.	To determine which flash device was inserted, check the ciscoFlashDeviceTable.
	Indicates removable flash device was removed from the router.	Status change occurred.	To determine which flash device was removed, check the ciscoFlashDeviceTable.

Interface 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
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. Value is down(2).	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 no longer down. The value of ifOperStatus indicates the link's new state. Value is up(1).	The port manager reactivated a port in the down state during a switchover.	No action is required.

Cisco MPLS Notifications

Table 4-5 lists MPLS-VPN notifications that can occur when an environmental threshold is exceeded.

Table 4-5   MPLS-VPN Notifications

Event	Description	Probable Cause	Recommended Action
mplsNumVrfRouteMidThreshExceeded	Indicates that the warning threshold is exceeded. Indicates that a threshold violation occurred.	The system limit of four Route Switch Processors per VPN has been exceeded. The number of routes created has crossed the warning threshold. This warning is sent only at the time the warning threshold is exceeded.	The configured RSPs are too large to fit in the DF table for one VPN. Try to configure the groups among existing RSPs in the hardware, or configure the RSP in another VPN.

Table 4-5   MPLS-VPN Notifications (continued)

Event	Description	Probable Cause	Recommended Action
mplsNumVrfRouteMaxThreshExceeded	Indicates that the maximum route limit was reached.	A route creation was unsuccessful because the maximum route limit was reached. Another notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again.	Set the threshold value. The maximum-threshold value is determined by the **maximum routes** command in VRF configuration mode.
mplsLdpFailedInitSessionThreshold Exceeded	Indicates that a local LSR and an adjacent LDP peer attempt to set up an LDP session between them, but fail to do so after a specified number of attempts.	Eight failed attempts occurred to establish an LDP session between a local LSR and an LDP peer due to some type of incompatibility between the devices. Cisco routers support the same features across multiple platforms. Therefore, the most likely incompatibility to occur between Cisco LSRs is a mismatch of their respective ATM VPI/VCI label ranges.	If you specify a range of valid labels for an LSR that does not overlap the range of its adjacent LDP peer, the routers will try eight times to create an LDP session between themselves before the mplsLdpFailedInitSessionThresholdExceeded notification is generated and sent to the NMS as an informational message. Operationally, the LSRs with label ranges that do not overlap continue their attempts to create an LDP session between themselves after the eight retry threshold is exceeded. In such cases, the LDP threshold exceeded notification alerts the network administrator to the existence of a condition in the network that may warrant attention.

Service Notifications

Table 4-6 lists MPLS-Service notifications generated by the router to indicate conditions for services.

Table 4-6   MPLS Service Notifications

Event	Description	Probable Cause	Recommended Action
mplsVrfIfUp	Indicates that a VPN routing or forwarding instance (VRF) was assigned to an interface that is operational or for the transition of a VRF interface to the operationally up state.	A VPN routing or forwarding instance (VRF) was assigned to an interface that is operational or a VRF interface transitions to the up state.	No action is required.
mplsVrfIfDown,	Indicates that a VRF was removed from an interface or a VRF interface transitioned to the operationally down state.	A VRF was removed from an interface or a VRF of an interface transitioned to the down state.	Check the operation state of the interface Or the state of the connected interface on the adjacent router Or add the removed VRF.
mplsLdpSessionUp	Indicates that the MPLS LDP session is in the up state.	Trap generated when an LDP entity (a local LSR) establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).	No action is required.
mplsLdpSessionDown	Indicates that the MPLS LDP session is in the down state.	Trap generated when an LDP session between a local LSR and its adjacent LDP peer is terminated.	Check if the LDP session exists between the local LSR and adjacent LDP peer.
mplsLdpPVLMismatch	Indicates that a local LSR establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path vector limits.	An LDP session has two adjacent peer LSRs with dissimilar path vector limits. The value of the path vector limit can range from 0 through 255; a value of "0" indicates that loop detection is off; any value other than zero up to 255 indicates that loop detection is on.	Configure all LDP-enabled routers in the network with the same path vector limit. Accordingly, the mplsLdpPathVectorLimitMismatch object exists in the MPLS-LDP-MIB to provide a warning message to the NMS when two routers engaged in LDP operations have a dissimilar path vector limit.
mplsTunnelUp	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.

Table 4-6   MPLS Service Notifications (continued)

Event	Description	Probable Cause	Recommended Action
mplsTunnelDown	Indicates that the mplsTunnelOperStatus object for a configured MPLS traffic engineering tunnel is about to transition to the up(1) or the down(2) state respectively.	A configured tunnel is transitioning to the down state. May be caused by an administrative or operational status check of the tunnel.	
mplsTunnelRerouted	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.

Routing Protocol Notifications

Table 4-7 lists BGP4-MIB notifications that are Border Gateway Protocol (BGP) state changes generated by the Cisco ASR 903 Series Router to indicate error conditions for routing protocols and services.

Table 4-7   Routing Protocol Notifications

Event	Description	Probable Cause	Recommended Action
bgpEstablished	The BGP FSM enters the Established state. It becomes active on the router.	BGP changed status.	No action is required.
bgpBackwardTransition	Indicates that BGP 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.	BGP changed status.	This threshold value is configured using the CLI command **neighbor** *nbr_addr max_prefixes* [threshold] [warning-only].

RTT Monitor Notifications

Table 4-8 lists CISCO-RTTMON-MIB notifications that can occur during round-trip time (RTT) monitoring.

Table 4-8   RTT Monitor Notifications

Event	Description	Probable Cause	Recommended Action
rttMonConnectionChangeNotification	Sent when the value of rttMonCtrlOperConnectionLostOccurred changes.	Occurs when the connection to a target has either failed to be established or was lost and then re-established.	Check for the connectivity to the target. There could be link problems to the target through different hops.
rttMonTimeoutNotification	A timeout occurred or was cleared.	An RTT probe occurred and the system sends the notice when the value of rttMonCtrlOperTimeoutOccurred changes.	Check for the end-to-end connectivity if rttMonCtrlOperTimeoutOccurred in the notification returns true. No action is required if rttMonCtrlOperTimeoutOccurred is false.
rttMonThresholdNotification	Threshold violation occurred.	An RTT probe occurred or a previous violation has subsided in a subsequent RTT operation.	Check for the end-to-end connectivity if rttMonCtrlOperOverThresholdOccurred in the notification is true; otherwise, no action is required.

Redundancy Framework Notifications

Table 4-9 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 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 RF clients on the active unit to synchronize any relevant data with their peer on the standby unit.

Table 4-9   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, then 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)

CPU Usage Notifications

The Cisco ASR 903 Series Router does not support CPU Usage Notifications. To generate notification for the cpu threshold, you can use RMON-MIB alarm and event in conjunction with CISCO-PROCESS-MIB object which represents the CPU.