Monitoring Notifications

This chapter describes the Cisco ASR 901 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 that are not listed.

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.

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.

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 procedure, go to:
  - http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a008021de3e.shtml
- 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.

Interface Notifications

Table 5-1 lists notifications generated by the Cisco ASR 901 routers for link-related (interface) events.

Table 5-1 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 ip interface brief** to determine the cause of the interface down.
linkUp	Indicates that the link is up. The value of if-OperStatus indicates the link's new state. Value is up (1).	The port manager reactivated a port in the linkdown state during a switchover.	No action is required.

Cisco MPLS Notifications

Table 5-2 lists MPLS-VPN notifications that can occur when an environmental threshold is exceeded.

Table 5-2 Cisco MPLS-VPN Notifications

Event	Description	Probable Cause	Recommended Action
mplsNumVrfRouteMidThreshExceeded	Indicates that the warning threshold is exceeded. Indicates that a threshold violation is occurred.	The system limit of four Route 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 route processors (RPs) are too large to fit in the DF table for one VPN. Try to configure the groups among existing RPs in the hardware, or configure the RP in another VPN.
mplsNumVrfRouteMaxThreshExceeded	Indicates that the maximum route limit is reached.	A route creation is unsuccessful since the maximum route limit is 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. Use the **maximum routes** command in VRF configuration mode to determine the maximum threshold value.

Service Notifications

Table 5-3 lists MPLS-Service notifications generated by the router to indicate conditions for services.

Table 5-3 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 a VRF interface transitioned 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 up state.	A VRF was removed from an interface or a VRF of an interface transitioned to the down state.	Check the operational 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 a 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 a 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.

Routing Protocol Notifications

Table 5-4 lists BGP4-MIB notifications that are Border Gateway Protocol (BGP) state changes generated by the Cisco ASR 901 router to indicate error conditions for routing protocols and services.

Table 5-4 Routing Protocol (BGP) Notifications

Event	Description	Probable Cause	Recommended Action
bgpEstablished	The BGP Finite State Machine (FSM) enters the ESTABLISHED state. It becomes active on the router.	BGP changed status.	No action is required.
bgpBackward-Transition	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.	BGP changed status.	This threshold value is configured using the CLI command **neighbor** *nbr_addr max_prefixes* [threshold] [warning-only].

Table 5-5 lists OSPF-MIB notifications that are Open Shortest Path First (OSPF) state changes generated by the Cisco ASR 901 router to indicate error conditions for routing protocols and services.

Table 5-5 Routing Protocol (OSPF) Notifications

Event	Description	Probable Cause	Recommended Action
ospfIfState-Change	This Notification signifies that there has been a change in the state of a non-virtual OSPF interface.	OSPF changed status.	No action is required.

Table 5-5 Routing Protocol (OSPF) Notifications

Event	Description	Probable Cause	Recommended Action
ospfTxRetransmit	Signifies than an OSPF packet has been retransmitted on a non-virtual interface. All packets that may be retransmitted are associated with an LSDB entry. LS type, LS ID, and Router ID are used to identify the LSDB entry.	OSPF changed status.	No action is required.
ospfIfAuthFailure	Signifies that a packet has been received on a non-virtual interface from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type.	Occurs when there is OSFP authentication key or authentication type conflicts.	Check for the OSFP authentication key and authentication type. There could be a mis-match between the two devices.

RTT Monitor Notifications

Table 5-6 lists CISCO-RTTMON-MIB notifications that can occur during round-trip time (RTT) monitoring.

Table 5-6 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.

Table 5-6 RTT Monitor Notifications

Event	Description	Probable Cause	Recommended Action
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 if 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 required.

Environmental Notifications

Table 5-7 lists CISCO-ENVMON-MIB notifications generated for events that might indicate the failure of the Cisco ASR 901 router or conditions that might affect the router functionality.

Table 5-7 Environmental Notifications

Event	Description	Probable Cause	Recommended Action
ciscoEnvMon-ShutdownNotification	A ciscoEnvMonShutdownNotification is sent if the environmental monitor detects a testpoint reaching a critical state and is about to initiate a reload. 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.	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 two minutes). 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.	No action is required.
ciscoEnvMon-FanStatus-ChangeNotif	A ciscoEnvMonFanStatusChangeNotif is sent if there is change in the state of a device being monitored by ciscoEnvMonFanState.	One of the fans in the fan array (where extant) fails or the fan status is changed.	Use the **show environment** command, to check for fan status.
ciscoEnvMon-SuppStatus-ChangeNotif	A ciscoEnvMonSupplyStatChangeNotif is sent if there is change in the state of a device being monitored by ciscoEnvMonSupplyState.	Power Supply status is changed.	Use the **show environment** command, to check for power supply status.

CPU Usage Notifications

Table 5-8 lists the CISCO-PROCESS -MIB notifications generated when the threshold for system-wide CPU utilization rises or falls.

Table 5-8 CISCO-PROCESS-MIB Notifications

Event	Description	Probable Cause	Recommended Action
cpmCPURisingThreshold	Indicates the rising threshold for system-wide CPU utilization.	When the system-wide CPU utilization crosses the rising threshold, a notification (SNMP or system log) is generated. A second rising threshold notification is sent only if a falling threshold notification corresponding to the first rising threshold notification is sent.	No action is required
cpmCPUFallingThreshold	Indicates the falling threshold for system-wide CPU utilization.	When the system-wide CPU utilization drops below the falling threshold, a SNMP or system log is generated. The falling threshold notification is generated only if a rising threshold notification was sent previously.	

REP Notifications

Table 5-9 lists the CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB notifications generated for an REP event.

Table 5-9 CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB Notifications

Event	Description	Probable Cause	Recommended Action
crepLinkStatus	Indicates an REP event.	When a REP interface enters or exits the REP link operational status.	No action is required
crepPreemptionStatus	Indicates an REP event.	Indicates the preemptive status triggered on the REP primary edge.	
crepPortRoleChange	Indicates an REP event.	When the role of a port changes from open to alternate.	

BFD Notifications

Table 5-10 lists the CISCO-IETF-BFD-MIB notifications generated for a BFD event.

Table 5-10 CISCO-IETF-BFD-MIB Notifications

Event	Description	Probable Cause	Recommended Action
ciscoBfdSessUp	Indicates a BFD event.	This notification is generated when the BFD session state changes to UP.	No action is required
ciscoBfdSessDown	Indicates a BFD event.	This notification is generated when the BFD session state changes to DOWN.	

Ethernet OAM Notifications

Table 5-11 lists the CISCO-DOT3-OAM-MIB notifications generated for an Ethernet OAM event.

Table 5-11 CISCO-DOT3-OAM-MIB Notifications

Event	Description	Probable Cause	Recommended Action
cdot3OamThresholdEvent	Indicates an Ethernet OAM event.	This notification is sent when a local or remote threshold crossing event is detected.	No action is required
cdot3OamNonThresholdEvent	Indicates an Ethernet OAM event.	This notification is generated when a local or remote non-threshold crossing event is detected.	

Ethernet CFM Notifications

Table 5-12 lists the IEEE8021-CFM-MIB notifications generated for an Ethernet CFM event.

Table 5-12 IEEE8021-CFM-MIB Notifications

Event	Description	Probable Cause	Recommended Action
dot1agCfmFaultAlarm	Indicates an Ethernet CFM event.	A MEP has a persistent defect condition. A notification (fault alarm) is sent to the management entity with the OID of the MEP that has detected the fault.	Check CFM session is up, ping and trace to remote MEP and each MIP.

Storm Control Notifications

Table 5-13 lists the CISCO-PORT-STORM-CONTROL-MIB notifications generated for a Storm Control event.

Table 5-13 CISCO-PORT-STORM-CONTROL-MIB Notifications

Event	Description	Probable Cause	Recommended Action
cpscEventRev1	Indicates a Storm Control event.	This notification is sent when a storm event occurs on an interface with respect to a particular traffic type.	Use the CLI command, **show storm-control [interface] [{broadcast | history | multicast | unicast}]** to verify the Storm Control entries.

Synchronous Ethernet (SyncE) Notifications

Table 5-14 lists the CISCO-NETSYNC-MIB notifications generated for a SyncE event.

Table 5-14 CISCO-NETSYNC-MIB Notifications

Event	Description	Probable Cause	Recommended Action
ciscoNetsyncSelectedT0Clock	T0 clock selection notification.	This notification is generated when one of the following conditions is met: • - A new clock source is selected by the T0 clock selection. • The clock quality of a T0 selected clock source is changed. • The configured priority of a T0 selected clock source is changed.	No action is required
ciscoNetsyncSelectedT4Clock	T4 clock selection notification.	This notification is generated when one of the following conditions is met: • A new clock source is selected by the T4 clock selection. • The clock quality of a T4 selected clock source is changed. • The configured priority of a T4 selected clock source is changed.	No action is required.

Table 5-14 CISCO-NETSYNC-MIB Notifications

Event	Description	Probable Cause	Recommended Action
ciscoNetsyncInputSignalFailureStatus	Input clock source signal failure notification.	This notification is generated when a signal failure event is reported on an input clock source. A signal failure event could be due to interface shutdown.	Make sure no signal failure on the link.
ciscoNetsyncInputAlarmStatus	Input clock source alarm notification.	This notification is generated when an alarm event is reported on an input clock source.	Make sure no alarms. Alarms might be caused due to several reasons such as misconfiguration of master and slave network options, LOS, LOF, or OOR.