



## CHAPTER 3

# Monitoring Hardware Using Alarms

---

Once hardware is installed and operational, use alarms to monitor hardware status on a daily basis.

This chapter includes the following sections:

- [Router Design and Monitoring Hardware, page 3-1](#)
- [Approaches for Monitoring Hardware Alarms, page 3-1](#)
- [For More Information, page 3-3](#)

## Router Design and Monitoring Hardware

The Cisco ASR 1000 Series Aggregation Services Routers are designed to send alarm notifications when problems are detected. Network administrators do not need to use **show** commands to poll devices on a routine basis and can monitor the network remotely. However, network administrators can perform onsite monitoring if they so choose.

## Approaches for Monitoring Hardware Alarms

The following sections discuss ways in which you can monitor hardware using alarms:

- [Onsite Network Administrator Responds to Audible or Visual Alarms, page 3-1](#)
- [Network Administrator Checks Console or Syslog for Alarm Messages, page 3-2](#)
- [Network Management System Alerts Network Administrator When an Alarm Is Reported Through SNMP, page 3-3](#)

## Onsite Network Administrator Responds to Audible or Visual Alarms

An external element can be connected to a power supply using the DB-25 alarm connector on the power supply. The external element is a DC lightbulb for a visual alarm and a bell for an audible alarm.

If an alarm illuminates the CRIT, MIN, or MAJ LED on the Cisco ASR 1000 Series Route Processor (RP) faceplate, and a visual or audible alarm is wired, the alarm also activates an alarm relay in the power supply DB-25 connector (on the Cisco ASR 1006 Router and Cisco ASR 1004 Router). The bell rings or the lightbulb flashes.

## Clearing Audible and Visual Alarms

To clear an audible alarm, do *one* of the following:

- Press the Audible Cut Off button on the RP faceplate.
- Enter the **clear facility-alarm** command.

To clear a visual alarm, you must resolve the alarm condition. The **clear facility-alarm** command does not clear an alarm LED on the RP faceplate or turn off the DC lightbulb. For example, if a critical alarm LED is illuminated because an active SPA was removed without a graceful deactivation of the SPA, the only way to resolve that alarm is to replace the SPA.

## Network Administrator Checks Console or Syslog for Alarm Messages

The network administrator can monitor alarm messages by reviewing alarm messages sent to the system console or to a syslog. This section discusses the following topics:

- [Enabling the logging alarm Command, page 3-2](#)
- [Examples of Alarm Messages, page 3-2](#)
- [Reviewing and Analyzing Alarm Messages, page 3-3](#)

### Enabling the logging alarm Command

The **logging alarm** command must be enabled for the system to send alarm messages to a logging device, such as the console or a syslog. This command is not enabled by default.

You can specify the severity level of alarm to log. All alarms at and above the specified threshold generate alarm messages. For example, the following command sends only critical alarm messages to logging devices:

```
Router(config)# logging alarm critical
```

If alarm severity is not specified, alarm messages for all severity levels are sent to logging devices.

### Examples of Alarm Messages

The following alarm messages are examples of alarm messages that are sent to the console when a SPA is removed without first doing a graceful deactivation of the SPA. The alarm is cleared when the SPA is re-inserted.

#### SPA REMOVED

```
*Aug 22 13:27:33.774: %ASR1000_OIR-6-REMSPA: SPA removed from subslot 1/1, interfaces disabled
```

```
*Aug 22 13:27:33.775: %SPA_OIR-6-OFFLINECARD: SPA (SPA-4XT-SERIAL) offline in subslot 1/1
```

#### SPA RE-INSERTED

```
*Aug 22 13:32:29.447: %ASR1000_OIR-6-INSSPA: SPA inserted in subslot 1/1
```

```
*Aug 22 13:32:34.916: %SPA_OIR-6-ONLINECARD: SPA (SPA-4XT-SERIAL) online in subslot 1/1
```

```
*Aug 22 13:32:35.523: %LINK-3-UPDOWN: SIP1/1: Interface EOBC1/1, changed state to up
```

## Reviewing and Analyzing Alarm Messages

To facilitate the review of alarm messages, you can write scripts to analyze alarm messages sent to the console or syslog. Scripts can provide reports on events such as alarms, security alerts, and interface status.

Syslog messages can also be accessed through Simple Network Management Protocol (SNMP) using the history table defined in the CISCO-SYSLOG-MIB.

## Network Management System Alerts Network Administrator When an Alarm Is Reported Through SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network. Of all the approaches to monitor alarms, SNMP is the best approach for enterprise and service provider customers that have many routers to monitor.

SNMP provides notification of faults, alarms, and conditions that might affect services. SNMP allows a network administrator to access router information through a network management system (NMS) instead of by polling devices, reviewing logs, or reviewing log reports.

To use SNMP to get alarm notification, you must use the following MIBs:

- ENTITY-MIB, RFC 4133 (required for the CISCO-ENTITY-ALARM-MIB and CISCO-ENTITY-SENSOR-MIB to work)
- CISCO-ENTITY-ALARM-MIB
- CISCO-ENTITY-SENSOR-MIB (for SPA and transceiver environmental alarm information, which is not provided through the CISCO-ENTITY-ALARM-MIB)

## For More Information

For more information about the topics discussed in this chapter, see the following documents:

Topic	Document
Command descriptions	<a href="#">Cisco IOS Master Command List, All Releases</a> <a href="#">Command Lookup Tool</a> (Requires Cisco.com user ID and password)
Configuring MIB support	<a href="#">Cisco ASR 1000 Series Aggregation Services Routers MIB Specifications Guide</a>
Configuring SNMP	“SNMP Support” chapter in the <a href="#">Cisco IOS XE Network Management Configuration Guide, Release 2</a>
Graceful Deactivation of a SIP or SPA: Online insertion and removal (OIR)	“Installing and Removing a SIP” chapter in the <a href="#">Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide</a>

Topic	Document
MIBs supported on the Cisco ASR 1000 Series Aggregation Services Routers	<a href="#">Cisco ASR 1000 Series Aggregation Services Routers MIB Specifications Guide</a>
Power supplies and the DB-25 alarm connector	“Cisco ASR 1000 Series Routers Components” chapter in the <a href="#">Cisco ASR 1000 Series Aggregations Services Routers Hardware Installation and Initial Configuration Guide</a>