CHAPTER 6

SNMP, RMON, and Alarm Configuration

This chapter contains information on the following system management topics:

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an application-layer protocol that allows an SNMP manager, such as a network management system (NMS), and an SNMP agent on the managed device to communicate. Remote Monitoring (RMON) allows you to see the activity on network nodes. By using RMON in conjunction with the SNMP agent on the Cisco 6400, you can monitor traffic through network devices, segment traffic that is not destined for the Cisco 6400, and create alarms and events for proactive traffic management.

For a complete description of SNMP, SNMP Management Information Bases (MIBs), and how to configure SNMP, see the "Configuring Simple Network Management Protocol (SNMP)" chapter of the "Cisco IOS System Management" part of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

Identifying and Downloading MIBs

To identify and download MIBs supported by the Cisco 6400, go to the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Using the NSP as the SNMPv3 Proxy Forwarder for the NRP-2

The SNMPv3 Proxy Forwarder feature enables all NSP and NRP-2 components of the Cisco 6400 system to be managed as one functional entity. With the Proxy Forwarder feature enabled, the NSP:

- Forwards all SNMPv3 formatted messages (such as manager requests to get or set data) destined for the NRP-2s
- Routes the SNMPv3 formatted traps from NRP-2s to the NSP combined network management Ethernet (NME) interface

Note The SNMPv3 Proxy Forwarder feature was introduced in Cisco IOS Releases 12.1(4)DB and 12.1(4)DC for the node route processor 2 (NRP-2). The feature is not supported in earlier releases or by the node route processor 1 (NRP-1).

To configure the Proxy Forwarder feature, complete the following tasks:

- Task 1: Configuring the NSP as the Proxy Forwarder
- Task 2: Configuring the NRP-2 to Use the NSP as the Proxy Forwarder

Task 1: Configuring the NSP as the Proxy Forwarder

To enable the NSP to act as the proxy forwarder for the NRP-2s in the Cisco 6400 chassis, enter the following NSP commands in global configuration mode:

	Command (Entered on the NSP)	Purpose
Step 1	`Switch(config)# snmp-server group` *groupname* `v3 noauth`	Configures a new SNMPv3 group.
Step 2	`Switch(config)# snmp-server user` *username groupname* `v3`	Configures a new user to an SNMPv3 group. Make sure that you use the same *groupname* in Steps 1 and 2.
Step 3	`Switch(config)# snmp-server forwarder`	Enables the NSP SNMPv3 proxy forwarder.
Step 4	`Switch(config)# snmp-server host` *host-address* `vrf 6400-private version 3 noauth` *username*	Specifies the recipient of NRP-2 SNMPv3 trap messages.

When you complete the previous steps, the NSP automatically generates **snmp-server user** and **snmp-server group** commands in the configuration.

Each time the NSP reloads or you insert an NRP-2 into the chassis, the NSP automatically generates **snmp-server engineID** commands in the configuration.

Note Do not modify or delete the automatically generated commands, because doing so may prevent SNMP from working properly.

Example

In the following example, the NSP is configured to act as the proxy forwarder:

```
snmp-server group usmgrp v3 noauth
snmp-server user usmusr usmgrp v3
snmp-server forwarder
snmp-server host 10.100.100.100 vrf 6400-private version 3 noauth trapusr
```

The previous commands cause the NSP to automatically generate the following commands:

```
snmp-server engineID remote 10.3.0.2 vrf 6400-private 800000090300000107BA9C7A0
snmp-server user trapusr trapusr v3
snmp-server user trapusr trapusr remote 10.3.0.2 vrf 6400-private v3
snmp-server user usmusr usmgrp remote 10.3.0.2 vrf 6400-private v3
snmp-server group trapusr v3 noauth notify *tv.FFFFFFFF.FFFFFFFF
```

Task 2: Configuring the NRP-2 to Use the NSP as the Proxy Forwarder

To configure the NRP-2 to communicate with the NSP as the proxy forwarder, complete the following steps in global configuration mode:

	Command (Entered on the NRP-2)	Purpose
Step 1	`Router(config)# snmp-server group` *groupname* `v3 noauth`	Configures a new SNMPv3 group. Make sure that the *groupname* argument entry matches that entered on the NSP in Task 1.
Step 2	`Router(config)# snmp-server user` *username groupname* `v3`	Configures a new user to an SNMPv3 group. Make sure that the *username* and *groupname* argument entries match those entered on the NSP in Task 1.
Step 3	`Router(config)# snmp-server enable traps [config | syslog | bgp | ipmulticast | rsvp | frame-relay | rtr | snmp authentication linkdown linkup coldstart]`	Enables the NRP-2 to send traps. Optionally, you can select from specific types of traps.
Step 4	`Router(config)# snmp-server host 10.`*nrp2-slot*`.0.1 vrf 6400-private version 3 noauth` *username*	Specifies the NSP as the recipient of SNMPv3 trap messages. The **10.***nrp2-slot***.0.1** IP address is the private address for the internal NSP interface to the NRP-2 PAM mailbox serial interface.

When you complete the previous steps, the NRP-2 automatically generates **snmp-server user** and **snmp-server group** commands in the configuration.

If you do not select any specific types of traps, the NRP-2 also automatically generates **snmp-server enable traps** commands to specify all available types of traps.

Note Do not modify or delete the automatically generated commands, because doing so may prevent SNMP from working properly.

Example

In the following example, the NRP-2 is configured to allow the NSP to act as the proxy forwarder:

```
snmp-server group usmgrp v3 noauth
snmp-server user usmusr usmgrp v3
snmp-server enable traps
snmp-server host 10.3.0.1 vrf 6400-private version 3 noauth trapusr
```

The previous commands cause the NRP-2 to automatically generate the following commands:

```
snmp-server user trapusr trapusr v3
snmp-server group trapusr v3 noauth notify *tv.FFFFFFFF.FFFFFFFF
snmp-server enable traps snmp authentication linkdown linkup coldstart
snmp-server enable traps config
snmp-server enable traps syslog
snmp-server enable traps bgp
snmp-server enable traps ipmulticast
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
```

Verifying the SNMPv3 Proxy Forwarder

To verify successful configuration of the SNMPv3 Proxy Forwarder feature, use the **more system:running-config** EXEC command. On both the NSP and NRP-2, check that you properly configured the commands described in the previous tasks.

Also check that the automatically generated commands correctly appear on both the NSP and NRP-2 running configurations. On the NSP, the three automatically generated commands that include an IP address are generated for every active NRP-2 in the chassis. The other automatically generated commands are created only once, regardless of the number of active NRP-2s installed in the chassis.

Remote Monitoring

The Remote Monitoring (RMON) option makes individual nodal activity visible and allows you to monitor all nodes and their interaction on a LAN segment. RMON, used in conjunction with the SNMP agent in the NSP, allows you to view traffic that flows through the switch as well as segment traffic not necessarily destined for the switch. Combining RMON alarms and events with existing MIBs allows you to choose where proactive monitoring will occur.

RMON can be very data and processor intensive. Users should measure usage effects to ensure that router performance is not degraded by RMON and to minimize excessive management traffic overhead. Native mode is less intensive than promiscuous mode.

The Cisco 6400 supports both RMON and ATM RMON.

For a complete description of the RMON MIB agent specification, and how it can be used in conjunction with SNMP to monitor traffic using alarms and events, see the “Configuring RMON Support” section of the “Cisco IOS System Management” part of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For a complete description and configuration information for ATM RMON on the NSP, see the “Configuring ATM Accounting and ATM RMON” chapter of the *ATM Switch Router Software Configuration Guide*.

Alarms

Alarms on the NSP help to monitor equipment and identify the cause of physical system problems within the central office (CO). There are three levels of alarms: minor, major, and critical, and there are many sources of alarm conditions. Temperature thresholds are the only alarm source that you can configure, but alarms can be triggered by card failure, SONET APS failures, and NRP failures.

Configuring Temperature Threshold Alarms

The Cisco 6400 includes environmental monitoring hardware and a digital thermometer that measures the temperature of the intake airflow and the temperature at the hottest part of the chassis. Temperature thresholds for each alarm type and location are automatically set, based on empirically determined values that vary depending on the number and type of boards inserted in the chassis. In addition to the automatically set thresholds, you can set your own thresholds for minor and major temperature alarms. You can also disable the minor and major temperature alarms. You cannot, however, change the threshold for or disable critical alarms.

To set thresholds for the minor and major temperature alarms at the two monitored locations, use the following command in global configuration mode:

Command	Purpose
`Switch(config)# facility-alarm [intake-temperature | core-temperature] [minor ˚C | major ˚C]`	Specifies thresholds for the intake and core major and minor alarms in degrees Celsius.

To disable the minor or major temperature alarms for either monitored location, use the **no** form of the **facility-alarm** command.

Example—Setting the Threshold

In the following example, the major core temperature alarm is set to 35˚C:

```
Switch(config)# facility-alarm core-temperature major 35
```

Example—Disabling the Alarm

In the following example, the minor intake temperature alarm is disabled:

```
Switch(config)# no facility-alarm intake-temperature minor
```

Verifying Temperature Alarms

To check the temperature thresholds, use the **show facility-alarm status** EXEC command, described in the next section.

Displaying Alarm Status and Thresholds

To display the status of current major and minor alarms and the settings of all user-configurable alarm thresholds, use the following EXEC command:

Command	Purpose
`Switch# show facility-alarm status`	Display all alarm thresholds and the status of current alarms.

Example

```
Switch# show facility-alarm status
Thresholds:
Intake minor 40 major 50 Core minor 55 major 53
SOURCE:Network Clock TYPE:Network clock source, priority level 2 down
SEVERITY:Minor ACO:Normal
SOURCE:NSP EHSA TYPE:Secondary failure SEVERITY:Minor ACO:Normal
SOURCE:ATM2/0/1 TYPE:Sonet major line failure SEVERITY:Major ACO:Normal
SOURCE:ATM6/0/1 TYPE:Sonet major line failure SEVERITY:Major ACO:Normal
SOURCE:ATM7/0/1 TYPE:Sonet major line failure SEVERITY:Major ACO:Normal
SOURCE:ATM6/1/0 TYPE:Sonet major line failure SEVERITY:Major ACO:Normal
SOURCE:ATM6/1/1 TYPE:Sonet major line failure SEVERITY:Major ACO:Normal
SOURCE:ATM7/1/1 TYPE:Sonet major line failure SEVERITY:Major ACO:Normal
```

Clearing Alarms

You can use the **clear facility-alarm** EXEC command to reset the external alarm relays and stop an auditory alarm indication. However, the alarm cause and LED indication may still be in effect, and the alarm can be viewed with the **show facility-alarm status** EXEC command until the alarm is cleared at the source. To clear the source of an alarm, you must specify the source as either the secondary CPU, one of the power entry modules (PEMs), or any device installed in the specified slot or subslot.

Clearing the source of an alarm is useful for:

- Removing a card from the chassis permanently or for an extended period of time
- Replacing a card with a different type of card in the same slot or subslot

The Cisco 6400 remembers the type of card originally installed in each slot or subslot, and removing a card activates an alarm.

To clear the specified alarm, reset the alarm contacts, and remove the source of the alarm, use the following EXEC command:

Command	Purpose
Switch# **clear facility-alarm** [**minor** | **major** | **critical**] [**source** {**sec-cpu** | **pem** {**0** | **1**} | **cardtype** {*slot* | *slot/subslot*}}]	Clears all alarms of the specified level, or clears the specified alarm source.

Note If all interfaces on an NLC or NRP are shut down prior to card removal (using the **shutdown** interface command), the Cisco 6400 will not generate an alarm.

Example—Clearing All Alarms

The following example shows how to clear all current external alarm relays:

```
Switch# clear facility-alarm
```

Example—Clearing a Specified Alarm Source

Suppose you have an NRP-1 in slot 2. Removing the NRP-1 and inserting an OC-12 NLC will generate an alarm. The following example shows how to clear the alarm:

```
Switch# clear facility-alarm source cardtype 2
```

Verifying Cleared Alarms

To verify that you cleared the alarms, use the **show facility-alarm status** EXEC command.