



CHAPTER 53

Configuring RMON

This chapter describes how to configure Remote Network Monitoring (RMON) on your Catalyst 4500 series switch. RMON is a standard monitoring specification that defines a set of statistics and functions that can be exchanged between RMON-compliant console systems and network probes. RMON provides you with comprehensive network-fault diagnosis, planning, and performance-tuning information.



Note

For complete syntax and usage information for the commands used in this chapter, see the *Cisco IOS Configuration Fundamentals Command Reference*

http://www.cisco.com/en/US/docs/ios/fundamentals/command_reference/cf_book.html

and related publications at this location:

<http://www.cisco.com/en/US/products/ps6350/index.html>

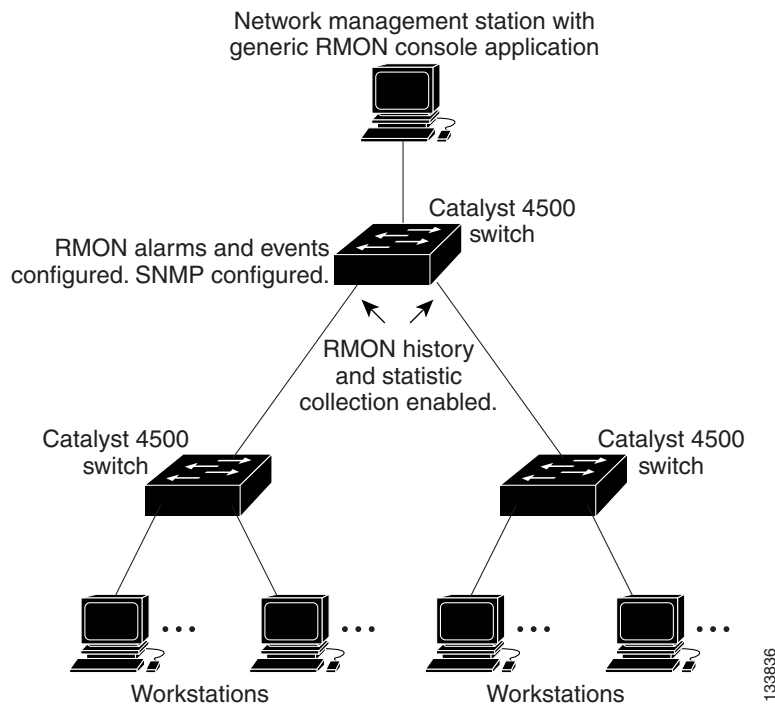
This chapter consists of these sections:

- [About RMON, page 53-1](#)
- [Configuring RMON, page 53-2](#)
- [Displaying RMON Status, page 53-6](#)

About RMON

RMON is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. You can use the RMON feature with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switches on all connected LAN segments.

Figure 53-1 Remote Monitoring Example



The switch supports these RMON groups (defined in RFC 1757):

- Statistics (RMON group 1)—Collects Ethernet, Fast Ethernet, and Gigabit Ethernet statistics on an interface.
- History (RMON group 2)—Collects a history group of statistics on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces for a specified polling interval.
- Alarm (RMON group 3)—Monitors a specific MIB object for a specified interval, triggers an alarm at a specified value (rising threshold), and resets the alarm at another value (falling threshold). Alarms can be used with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.
- Event (RMON group 9)—Determines the action to take when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.

Because switches supported by Cisco IOS Release 12.2(31)SG use hardware counters for RMON data processing, the monitoring is more efficient, and little processing power is required.

Configuring RMON

This section describes how to configure RMON on your switch. It contains this configuration information:

- [Default RMON Configuration, page 53-3](#)
- [Configuring RMON Alarms and Events, page 53-3](#)
- [Configuring RMON Collection on an Interface, page 53-4](#)

Default RMON Configuration

RMON is disabled by default; no alarms or events are configured.

Only RMON 1 is supported on the switch.

Configuring RMON Alarms and Events

You can configure your switch for RMON by using the command-line interface (CLI) or an SNMP-compatible network management station. We recommend that you use a generic RMON console application on the network management station (NMS) to take advantage of RMON's network management capabilities. You must also configure SNMP on the switch to access RMON MIB objects. For more information, see [Chapter 51, "Configuring SNMP."](#)

To enable RMON alarms and events, perform this task:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>rmon alarm number variable interval {absolute delta} rising-threshold value [event-number] falling-threshold value [event-number] [owner string]</code>	<p>Sets an alarm on a MIB object.</p> <ul style="list-style-type: none"> For <i>number</i>, specify the alarm number. The range is 1 to 65535. For <i>variable</i>, specify the MIB object to monitor. For <i>interval</i>, specify the time in seconds the alarm monitors the MIB variable. The range is 1 to 4294967295 seconds. Specify the absolute keyword to test each MIB variable directly; specify the delta keyword to test the change between samples of a MIB variable. For <i>value</i>, specify a number at which the alarm is triggered and one for when the alarm is reset. The range for the rising threshold and falling threshold <i>values</i> is -2147483648 to 2147483647. (Optional) For <i>event-number</i>, specify the event number to trigger when the rising or falling threshold exceeds its limit. (Optional) For owner string, specify the owner of the alarm.

	Command	Purpose
Step 3	<code>rmon event number [description string] [log] [owner string] [trap community]</code>	<p>Adds an event in the RMON event table that is associated with an RMON event number.</p> <ul style="list-style-type: none"> For <i>number</i>, assign an event number. The range is 1 to 65535. (Optional) For description string, specify a description of the event. (Optional) Use the log keyword to generate an RMON log entry when the event is triggered. (Optional) For owner string, specify the owner of this event. (Optional) For <i>community</i>, enter the SNMP community string used for this trap.
Step 4	<code>end</code>	Returns to privileged EXEC mode.
Step 5	<code>show running-config</code>	Verifies your entries.
Step 6	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

To disable an alarm, use the **no rmon alarm number** global configuration command on each alarm you configured. You cannot disable at once all the alarms that you configured. To disable an event, use the **no rmon event number** global configuration command. To learn more about alarms and events and how they interact with each other, see RFC 1757.

You can set an alarm on any MIB object. The following example configures RMON alarm number 10 by using the **rmon alarm** command. The alarm monitors the MIB variable *ifEntry.20.1* once every 20 seconds until the alarm is disabled and checks the change in the variable's rise or fall. If the *ifEntry.20.1* value shows a MIB counter increase of 15 or more, such as from 100000 to 100015, the alarm is triggered. The alarm in turn triggers event number 1, which is configured with the **rmon event** command. Possible events can include a log entry or an SNMP trap. If the *ifEntry.20.1* value changes by 0, the alarm is reset and can be triggered again.

```
Switch(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1
falling-threshold 0 owner jjohnson
```

The following example creates RMON event number 1 by using the **rmon event** command. The event is defined as *High ifOutErrors* and generates a log entry when the event is triggered by the alarm. The user *jjones* owns the row that is created in the event table by this command. This example also generates an SNMP trap when the event is triggered.

```
Switch(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
jjones
```

Configuring RMON Collection on an Interface

You must first configure RMON alarms and events to display collection information.

To collect group history statistics on an interface, perform this task:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>interface interface-id</code>	Specifies the interface on which to collect history, and enter interface configuration mode.
Step 3	<code>rmon collection history index</code> [<code>buckets bucket-number</code>] [<code>interval seconds</code>] [<code>owner ownername</code>]	Enables history collection for the specified number of buckets and time period. <ul style="list-style-type: none"> For <i>index</i>, identify the RMON group of statistics. The range is 1 to 65535. (Optional) For buckets <i>bucket-number</i>, specify the maximum number of buckets desired for the RMON collection history group of statistics. The range is 1 to 65535. The default is 50 buckets. (Optional) For interval <i>seconds</i>, specify the number of seconds in each polling cycle. (Optional) For owner <i>ownername</i>, enter the name of the owner of the RMON group of statistics. <p>To disable history collection, use the no rmon collection history index interface configuration command.</p>
Step 4	<code>end</code>	Returns to privileged EXEC mode.
Step 5	<code>show running-config</code>	Verifies your entries.
Step 6	<code>show rmon history</code>	Displays the contents of the switch history table.
Step 7	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

To collect group Ethernet statistics on an interface, perform this task:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>interface interface-id</code>	Specifies the interface on which to collect statistics, and enter interface configuration mode.
Step 3	<code>rmon collection stats index</code> [<code>owner ownername</code>]	Enables RMON statistic collection on the interface. <ul style="list-style-type: none"> For <i>index</i>, specify the RMON group of statistics. The range is from 1 to 65535. (Optional) For owner <i>ownername</i>, enter the name of the owner of the RMON group of statistics. <p>To disable the collection of group Ethernet statistics, use the no rmon collection stats index interface configuration command.</p>
Step 4	<code>end</code>	Returns to privileged EXEC mode.
Step 5	<code>show running-config</code>	Verifies your entries.
Step 6	<code>show rmon statistics</code>	Displays the contents of the switch statistics table.
Step 7	<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Displaying RMON Status

To display the RMON status, use one or more of the privileged EXEC commands in [Table 53-1](#):

Table 53-1 *Commands for Displaying RMON Status*

Command	Purpose
<code>show rmon</code>	Displays general RMON statistics.
<code>show rmon alarms</code>	Displays the RMON alarm table.
<code>show rmon events</code>	Displays the RMON event table.
<code>show rmon history</code>	Displays the RMON history table.
<code>show rmon statistics</code>	Displays the RMON statistics table.