



Configuring RMON Support

This chapter describes the Remote Monitoring (RMON) MIB agent specification, and how it can be used in conjunction with SNMP to monitor traffic using alarms and events.

For a complete description of the RMON commands mentioned in this chapter, refer to the “RMON Commands” chapter in the “System Management” part of the Release 12.1 *Cisco IOS Configuration Fundamentals Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

Configuring RMON Support

The Remote Monitoring (RMON) option identifies activity on individual nodes and allows you to monitor all nodes and their interaction on a LAN segment. Used in conjunction with the Simple Network Management Protocol (SNMP) agent in a router, RMON allows you to view both traffic that flows through the router and segment traffic not necessarily destined for the router. Combining RMON alarms and events (classes of messages that indicate traffic violations and various unusual occurrences over a network) with existing MIBs allows you to choose where proactive monitoring will occur.



Note

Full RMON packet analysis (as described in RFC 1757) is supported only on an Ethernet interface of the Cisco 2500 series and Cisco AS5200 series universal access servers. RMON requires that SNMP be configured (you must be running a version of SNMP on the server that contains the RMON MIB). A generic RMON console application is recommended in order to take advantage of RMON’s network management capabilities. This feature supports RFCs 1757 and 2021.

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.

All Cisco IOS software images ordered without the explicit RMON option include limited RMON support (RMON alarms and event groups only). Images ordered with the RMON option include support for all nine management groups (statistics, history, alarms, hosts, hostTopN, matrix, filter, capture, and event). As a security precaution, support for the capture group allows capture of packet header information only; data payloads are not captured.

In Cisco IOS 12.1, the RMON agent has been rewritten to improve performance and add some new features. The command line interface (CLI) has been enhanced with some new RMON commands. Table 16 highlights some of the improvements implemented:

Table 16 *Benefits of RMON MIB Update*

Prior to the RMON MIB Update in Cisco IOS 12.1	New functionality in Cisco IOS 12.1
RMON configurations do not persist across reboots. Information is lost after a new session on the RMON server.	RMON configurations persist across reboots. Information is preserved after a new session on the RMON server.
Packet analysis applies only on the Media Access Control (MAC) header of the packet.	Complete packet capture is performed with analysis applied to all frames in packet.
Only RMON I MIB objects are used for network monitoring.	RMON I and selected RMON II objects are used for network monitoring.

New RMON MIB features include.

- `usrHistory` group. This MIB group is similar to the RMON `etherHistory` group except that the group enables the user to specify the MIB objects that are collected at each interval.
- `partial probeConfig` group. This MIB group is a subset of the `probeConfig` group implemented in read-only mode. These objects implement the simple scalars from this group. Table 17 details new `partial probeConfig` group objects:

Table 17 *partial probeConfig Group Objects*

Object	Description
<code>probeCapabilities</code>	The RMON software groups implemented.
<code>probeSoftwareRev</code>	The current version of Cisco IOS running on the device.
<code>probeHardwareRev</code>	The current version of Cisco device.
<code>probeDateTime</code>	The current date and time.
<code>probeResetControl</code>	Initiates a reset.
<code>probeDownloadFile</code>	The source of the image running on the device.
<code>probeDownloadTFTPServer</code>	The address of the server that contains the Trivial File Transfer Protocol (TFTP) file that is used by the device to download new versions of Cisco IOS.
<code>probeDownloadAction</code>	Specifies the action of the commands that cause the device to reboot.
<code>probeDownloadStatus</code>	The state of a reboot.
<code>netDefaultGateway</code>	The router mapped to the device as the default gateway.
<code>hcRMONCapabilities</code>	Specifies the features mapped to this version of RMON.

Configuring RMON Alarm and Event Notifications

To enable RMON on an Ethernet interface, use the following command in interface configuration mode:

Command	Purpose
<code>rmon {native promiscuous}</code>	Enables RMON.

In native mode, RMON monitors only the packets normally received by the interface. In promiscuous mode, RMON monitors all packets on the LAN segment.

The default size of the queue that holds packets for analysis by the RMON process is 64 packets. To change the size of the queue, use the following command in global configuration mode:

Command	Purpose
<code>rmon queuesize size</code>	Changes the size of the RMON queue.

To set an RMON alarm or event, use one of the following commands in global configuration mode:

Command	Purpose
<code>rmon alarm number variable interval {delta absolute} rising-threshold value [event-number] falling-threshold value [event-number] [owner string]</code>	Sets an alarm on a MIB object.
<code>rmon event number [log] [trap community] [description string] [owner string]</code>	Adds or remove an event in the RMON event table.

You can set an alarm on any MIB object in the access server. To disable an alarm, you must enable the **no** form of this command on each alarm you configure. You cannot disable all the alarms you configure at once. Refer to RFC 1757 to learn more about alarms and events and how they interact with each other.

Configuring RMON Groups

RMON tables can be created for buffer capture, filter, hosts, and matrix information. The buffer capture table details a list of packets captured off of a channel or a logical data or events stream. The filter table details a list of packet filter entries that screen packets for specified conditions as they travel between interfaces. The hosts table details a list of host entries. The matrix table details a list of traffic matrix entries indexed by source and destination MAC addresses.

RMON statistics can be gathered for these data-types by using the following commands in interface configuration mode:

Command	Purpose
<code>rmon collection history {controlEntry integer} [owner ownername] [buckets bucket-number] [interval seconds]</code>	Enables an RMON history group of statistics on an interface.
<code>rmon collection host {controlEntry integer} [owner ownername]</code>	Enables an RMON host collection group of statistics on an interface.

Command	Purpose
<code>rmon collection matrix {controlEntry integer} [owner ownername]</code>	Enables an RMON matrix group of statistics on an interface.
<code>rmon collection rmon1 {controlEntry integer} [owner ownername]</code>	Enables all possible autoconfigurable RMON statistic collections on an interface.

To specifically monitor the above features, use the **show rmon capture**, **filter**, **hosts**, and **matrix** commands listed below.

Monitoring and Verifying RMON Configuration

To display the current RMON status, use one or more of the following commands in EXEC mode:

Command	Function
<code>show rmon</code>	Displays general RMON statistics.
or	
<code>show rmon task</code>	
<code>show rmon alarms</code>	Displays the RMON alarm table.
<code>show rmon capture</code>	Displays the RMON buffer capture table and current configuration. Available on Cisco 2500 series and Cisco AS5200 only.
<code>show rmon events</code>	Displays the RMON event table.
<code>show rmon filter</code>	Displays the RMON filter table. Available on Cisco 2500 series and Cisco AS5200 only.
<code>show rmon history</code>	Displays the RMON history table. Available on Cisco 2500 series and Cisco AS5200 only.
<code>show rmon hosts</code>	Displays the RMON hosts table. Available on Cisco 2500 series and Cisco AS5200 only.
<code>show rmon matrix</code>	Display the RMON matrix table and values associated with RMON variables. Available on Cisco 2500 series and Cisco AS5200 only.
<code>show rmon statistics</code>	Display the RMON statistics table. Available on Cisco 2500 series and Cisco AS5200 only.
<code>show rmon topn</code>	Display the RMON top-n hosts table. Available on Cisco 2500 series and Cisco AS5200 only.

RMON Configuration Examples

Alarm and Event Examples

The following example enables the **rmon event** command:

```
rmon event 1 log trap eventtrap description "High ifOutErrors" owner sdurham
```

This example creates RMON event number 1, which is defined as *High ifOutErrors*, and generates a log entry when the event is triggered by an alarm. The user *sdurham* owns the row that is created in the event table by this command. This example also generates a Simple Network Management Protocol (SNMP) trap when the event is triggered.

The following example configures an RMON alarm using the **rmon alarm** command:

```
rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0 owner
jjohnson
```

This example configures RMON alarm number 10. 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 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.

show RMON Examples

To display the RMON buffer capture table and current configuration, enter the **show rmon capture** command (Cisco 2500 series and Cisco AS5200 only). A sample configuration follows:

```
show rmon capture
```

```
Buffer 1 is active, owned by John Smith
Captured data is from channel 1
Slice size is 128, download size is 128
Download offset is 0
Full Status is full, full action is wrapWhenFull
Granted -1 octets out of -1 requested
Buffer has been on since 18:59:48, and has captured 522 packets
Current capture buffer entries:
Packet 3271 was captured 2018256 ms since buffer was turned on
Its length is 184 octets and has a status type of 0
Packet ID is 3721, and contains the following data:
03 00 00 00 00 0100 A0CC 3C9D DF00 A6F0 03
Packet 3722 was captured 2018452 ms since buffer was turned on
Its length is 64 octets and has a status type of 0
Packet ID is 3722, and contains the following data:
01 80C2 0000 0000 6009 FDFE D300 2642 03
```

To view values associated with RMON variables, enter the **show rmon matrix** command (Cisco 2500 series and Cisco AS5200 only). The following is a sample output:

```
show rmon matrix
```

```
Matrix 1 is active and owned by
Monitors ifEntry.1.1
Table size is 42, last time an entry was deleted was at 11:18:09
Source addr is 0000.0c47.007b, dest addr is ffff.ffff.ffff
Transmitted 2 pkts, 128 octets, 0 errors
Source addr is 0000.92a8.319e, dest addr is 0060.5c86.5b82
Transmitted 2 pkts, 384 octets, 1 error
```

For an explanation of the fields in the above examples, see the respective command descriptions in the “RMON Commands” chapter of the Release 12.1 *Cisco IOS Configuration Fundamentals Command Reference*.

