Configuring RMON Support

Last Updated: June 30, 2011

This module describes the Remote Monitoring (RMON) MIB agent specification and its usage in conjunction with Simple Network Management Protocol (SNMP) to monitor traffic using alarms and events.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring RMON Support

- RMON requires SNMP to be configured (you must be running a version of SNMP on the server that contains the RMON MIB).

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

Restrictions for Configuring RMON Support

- Full RMON packet analysis (as described in RFC 1757) is supported only on an Ethernet interface of Cisco 2500 series routers and Cisco AS5200 series universal access servers.
- A generic RMON console application is recommended in order to take advantage of the RMON network management capabilities.

Information About Configuring RMON Support

RMON Overview

RMON is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more flexibility in selecting network-monitoring probes and consoles with features that meet their particular networking needs.

The RMON specification defines a set of statistics and functions that can be exchanged between RMON-compliant console managers and network probes. RMON provides network administrators with comprehensive network-fault diagnosis, planning, and performance-tuning information.

The RMON feature identifies activity on individual nodes and allows you to monitor all nodes and their interaction on a LAN segment. Used in conjunction with the SNMP agent in a router, RMON allows you to view both traffic that flows through the router and segment traffic that is 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.

RMON Groups

RMON delivers information in RMON groups of monitoring elements, each providing specific sets of data to meet common network-monitoring requirements. Each group is optional so that you do not need to support all the groups within the Management Information Base (MIB). Some RMON groups require support of other RMON groups to function properly.

The table below summarizes the nine monitoring groups specified in the RFC 1757 Ethernet RMON MIB. For more information on gathering RMON statistics for these data types, refer to Configuring RMON Groups, page 9.

Note 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.

Table 1   *RMON Monitoring Groups*

RMON Group	Function	Elements
Statistics	Contains statistics measured by the probe for each monitored interface on this device.	Packets dropped, packets sent, bytes sent (octets), broadcast packets, multicast packets, CRC errors, runts, giants, fragments, jabbers, collisions, and counters for packets ranging from 64 to 128, 128 to 256, 256 to 512, 512 to 1024, and 1024 to 1518 bytes.
History	Records periodic statistical samples from a network and stores them for later retrieval.	Sample period, number of samples, items sampled.
Alarm	Periodically takes statistical samples from variables in the probe and compares them with previously configured thresholds. If the monitored variable crosses a threshold, an event is generated.	Includes the alarm table and requires the implementation of the event group. Alarm type, interval, starting threshold, stop threshold.
Host	Contains statistics associated with each host discovered on the network.	Host address, packets, and bytes received and transmitted, as well as broadcast, multicast, and error packets.
HostTopN	Prepares tables that describe the hosts that top a list ordered by one of their base statistics over an interval specified by the management station. Thus, these statistics are rate-based.	Statistics, host(s), sample start and stop periods, rate base, duration.
Matrix	Stores statistics for conversations between sets of two addresses. As the device detects a new conversation, it creates a new entry in its table.	Source and destination address pairs and packets, bytes, and errors for each pair.

RMON Group	Function	Elements
Filters	Enables packets to be matched by a filter equation. These matched packets form a data stream that might be captured or that might generate events.	Bit-filter type (mask or not mask), filter expression (bit level), conditional expression (and, or not) to other filters.
Packet Capture	Enables packets to be captured after they flow through a channel.	Size of buffer for captured packets, full status (alarm), number of captured packets.
Events	Controls the generation and notification of events from this device.	Event type, description, last time event sent.

RMON Event and Alarm Notifications

Thresholds allow you to minimize the number of notifications sent on the network. The RMON MIB defines two traps, the risingAlarm trap which is the rising-threshold value and fallingAlarm trap which is the falling-threshold value. Alarms are triggered when a problem exceeds a set rising-threshold value. No alarm notifications are sent until the agent recovers, as defined by the falling-threshold value. This means that notifications are not sent each time a minor failure or recovery occurs.

You can set an RMON alarm on any MIB object in the access server. You cannot disable all the alarms you configure at once. The delta value tests the change between MIB variables, which affects the alarmSampleType in the alarmTable of the RMON MIB. The absolute value tests each MIB variable directly, which affects the alarmSampleType in the alarmTable of the RMON MIB.

Refer to RFC 1757 to learn more about alarms and events and how they interact with each other.

RMON MIB

RMON MIB supports for polling of 64 bit counters and includes the following features:

- usrHistory group. This MIB group is similar to the RMON etherHistory group except that the group enables you 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. The table below details new partial probeConfig group objects.

Table 2   *partial probeConfig Group Objects*

Object	Description
probeCapabilities	The RMON software groups implemented.
probeSoftwareRev	The current version of Cisco IOS software running on the device.
probeHardwareRev	The current version of the Cisco device.
probeDateTime	The current date and time.

Object	Description
probeResetControl	Initiates a reset.
probeDownloadFile	The source of the image running on the device.
probeDownloadTFTPServer	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 software.
probeDownloadAction	Specifies the action of the commands that cause the device to reboot.
probeDownloadStatus	The state of a reboot.
netDefaultGateway	The router mapped to the device as the default gateway.
hcRMONCapabilities	Specifies the features mapped to this version of RMON.

In Cisco IOS Release 12.1, the RMON agent was rewritten to improve performance and add some new features. The table below highlights some of the improvements implemented.

Table 3   *RMON MIB Updates*

Prior to the RMON MIB Update in Cisco IOS Release 12.1	New Functionality in Cisco IOS Release 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 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.

HC Alarm MIB

The high-capacity (HC) Alarm MIB, which is an extension of RMON Alarm group table objects, supports polling of RMON variables up to 64 bit values. The HC-ALARM-MIB defines two traps, the hcRisingAlarm which provides the rising-threshold value and hcFallingAlarm which provides the falling-threshold value.

Refer to RFC 3434 to learn more about HC alarms.

How to Configure RMON Support

Configuring RMON

This task explains how to configure RMON and RMON queue size. In native mode, RMON monitors only those packets that are received by the interface. In promiscuous mode, RMON monitors all packets on the LAN segment.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **rmon** {**native** | **promiscuous**}
5. **exit**
6. **rmon queuesize** *size*
7. **exit**
8. **show rmon**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**rmon** {**native**	**promiscuous**} **Example:** `Router(config-if)# rmon native`	Configures RMON on Ethernet interfaces in native or promiscuous mode. • In the example, RMON is configured in the native mode.

	Command or Action	Purpose
Step 5	**exit** **Example:** Router(config-if)# exit	Exits the interface configuration mode and places the router in global configuration mode.
Step 6	**rmon queuesize** *size* **Example:** Router(config)# rmon queuesize 128	(Optional) Configures the size of the queue that holds packets for analysis by the RMON process.
Step 7	**exit** **Example:** Router(config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 8	**show rmon** **Example:** Router# show rmon	Displays general RMON statistics.

Configuring RMON Event and Alarm Notifications

The following tasks describe how to configure RMON event and alarm notifications.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **rmon event** *number* [**log**] [**trap** *community*] [**description** *string*] [**owner** *string*]
4. **rmon alarm** *number variable interval* {**delta** | **absolute**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *string*]
5. **rmon hc-alarms** *number variable interval* {**delta** | **absolute**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *string*]
6. exit
7. **show rmon alarms**
8. **show rmon hc-alarms**
9. **show rmon events**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.
		• Enter your password if prompted.
	Example:	
	Router> enable	
Step 2	**configure terminal**	Enters global configuration mode.
	Example:	
	Router# configure terminal	
Step 3	**rmon event number** [**log**] [**trap** *community*] [**description** *string*] [**owner** *string*]	Adds or removes an event (in the RMON event table) that is associated with an RMON event number.
	Example:	
	Router(config)# rmon event number	
Step 4	**rmon alarm** *number variable interval* {**delta** | **absolute**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *string*]	Configures an alarm on any MIB object.
	Example:	
	Router(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0 owner owner1	
Step 5	**rmon hc-alarms** *number variable interval* {**delta** | **absolute**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *string*]	(Optional) Configures an HC alarm on any MIB object.
	Example:	
	Router(config)# rmon hc-alarms 2 ifInOctets.2 20 delta rising-threshold 2000 2 falling-threshold 1000 1 owner own	
Step 6	exit	Exits the global configuration mode and enters the privileged EXEC mode.
	Example:	
	Router(config)# exit	

	Command or Action	Purpose
Step 7	**show rmon alarms**	Displays the RMON alarm table.
	Example:	
	`Router# show rmon alarm`	
Step 8	**show rmon hc-alarms**	Displays the RMON HC alarm table.
	Example:	
	`Router# show rmon hc-alarms`	
Step 9	**show rmon events**	Displays the RMON event table.
	Example:	
	`Router# show rmon events`	

Configuring RMON Groups

The following tasks explain how to configure RMON groups by gathering RMON statistics for data types.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **rmon collection history controlEntry** *integer* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]
5. **rmon collection host controlEntry** *integer* [**owner** *ownername*]
6. **rmon collection matrix controlEntry** *integer* [**owner** *ownername*]
7. **rmon collection rmon1 controlEntry** *integer* [**owner** *ownername*]
8. **exit**
9. **rmon capture-userdata**
10. **exit**
11. **show rmon history**
12. **show rmon hosts**
13. **show rmon matrix**
14. **show rmon statistics**
15. show rmon capture

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**rmon collection history controlEntry** *integer* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*] **Example:** `Router(config-if)# rmon collection history controlEntry 20 owner john`	(Optional) Enables RMON history gathering on an interface.
Step 5	**rmon collection host controlEntry** *integer* [**owner** *ownername*] **Example:** `Router(config-if)# rmon collection host controlEntry 40 owner own1`	(Optional) Enables RMON MIB host collection group of statistics on an interface.
Step 6	**rmon collection matrix controlEntry** *integer* [**owner** *ownername*] **Example:** `Router(config-if)# rmon collection matrix controlEntry 25 owner john`	(Optional) Enables RMON MIB matrix group of statistics on an interface.

	Command or Action	Purpose
Step 7	**rmon collection rmon1 controlEntry** *integer* [**owner** *ownername*] **Example:** Router(config-if)# rmon collection rmon1 controlEntry 30 owner john	(Optional) Enables all possible autoconfigurable RMON MIB statistic collections on an interface.
Step 8	**exit** **Example:** Router(config-if)# exit	Exits the interface configuration mode and places the router in global configuration mode.
Step 9	**rmon capture-userdata** **Example:** Router(config)# rmon capture-userdata	Disables the packet zeroing feature that initializes the user payload portion of each RMON MIB packet.
Step 10	**exit** **Example:** Router(config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 11	**show rmon history** **Example:** Router# show rmon history	Displays the RMON history table.
Step 12	**show rmon hosts** **Example:** Router# show rmon hosts	Displays the RMON hosts table.
Step 13	**show rmon matrix** **Example:** Router# show rmon matrix	Displays the RMON matrix table and values associated with RMON variables.

	Command or Action	Purpose
Step 14	**show rmon statistics** **Example:** Router# show rmon statistics	Displays the RMON statistics table.
Step 15	show rmon capture **Example:** Router# show rmon capture	Displays the contents of the router's RMON capture table.

Configuration Examples for RMON Support

Configuring RMON Example

The following example shows how to configure RMON with a queuesize of 100 packets in promiscuous mode:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 0/0
Router(config-if)# rmon promiscuous
Router(config-if)# exit
Router(config)# rmon queuesize 100
```

The following is a sample output from the **show rmon** command. All counters are from the time the router was initialized:

```
Router# show rmon
145678 packets input (34562 promiscuous), 0 drops
145678 packets processed, 0 on queue, queue utilization 15/100
```

Configuring RMON Event and Alarm Notifications Example

The following example shows how to enable the **rmon event**global configurationcommand:

```
Router> enable
Router# configure terminal
Router(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner
ownerA
```

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 ownerA 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.

The following is a sample output from the **show rmon events** command:

```
Router# show rmon events
Event 1 is active, owned by ownerA
 Description is High ifOutErrors
 Event firing causes log and trap to community rmonTrap, last fired 00:00:00
```

The following example shows how to configure an RMON alarm using the **rmon alarm** global configuration command:

```
Router> enable
Router# configure terminal
Router(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-
threshold 0 owner ownerA
```

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 rise or fall of the variable. 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.

The following is sample output from the **show rmon alarms** command

```
Router# show rmon alarms
Alarm 2 is active, owned by owner_a
 Monitors ifEntry.20.1.20 every 20 seconds
 Taking delta samples, last value was 0
 Rising threshold is 15, assigned to event 12
 Falling threshold is 0, assigned to event 0
 On startup enable rising or falling alarm
```

The following example shows how to configure an RMON HC alarm using the **rmon hc-alarms** global configuration command:

```
Router> enable
Router# configure terminal
Router(config)# rmon hc-alarms 2 ifInOctets.2 20 delta rising-threshold 2000 2 falling-
threshold 1000 1 owner own
```

This example configures RMON HC alarm number 2. The alarm monitors the MIB variable ifInOctets.2 once every 20 seconds until the alarm is disabled, and checks the change in the rise or fall of the variable. If the ifInOctets.2value shows a MIB counter increase of 2000 or more, such as from 100000 to 103000, the alarm is triggered. The alarm in turn triggers event number 2, which is configured with the **rmon event** command. Possible events include a log entry or a Simple Network Management Protocol (SNMP) trap. If theifInOctets.2 value changes by 1000 (falling threshold is 1000), the alarm is reset and can be triggered again.

To display the contents of the RMON HC alarm table of the router, use the **show rmon hc-alarms** command in privileged EXEC mode. The following is sample output:

```
Router# show rmon hc-alarms
Router#show rmon hc-alarms
 Monitors ifInOctets.1 every 20 second(s)
 Taking absolute samples, last value was 0
 Rising threshold Low is 4096, Rising threshold Hi is 0,
               assigned to event 0
 Falling threshold Low is 1280, Falling threshold Hi is 0,
               assigned to event 0
 On startup enable rising or falling alarm
```

Configuring RMON Tables Example

The following example shows how to enable the RMON collection matrix group of statistics with an ID number of 25 and specifies john as the owner:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 0/0
Router(config-if)# rmon collection matrix controlEntry 25 owner john
```

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

```
Router# show rmon matrix
Matrix 1 is active and owned by john
Monitors controlEntry
Table size is 25, 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
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
CNS commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Network Management Command Reference 3.0*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
• RMON MIB • HC-Alarm MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1757	*Remote Network Monitoring Management Information Base*
RFC 2021	*Remote Network Monitoring Management Information Base Version 2 using SMIv2*
RFC 3434	*Remote Monitoring MIB Extensions for High Capacity Alarms*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring RMON Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4   ***Feature Information for Configuring RMON Support***

Feature Name	Releases	Feature Information
HC Alarm MIB	12.2(33)SXI 12.2(33)SRE	The HC Alarm MIB feature provides an extension to the RMON-1 Alarm group table objects which was used to support counter 32 objects for threshold capabilities. The HC Alarm MIB adds support to threshold capabilities for counter 64 objects. The following commands were introduced: **rmon hc-alarms**, **show rmon hc-alarms**.
Remote Monitoring MIB Update	12.0(5)T	The RMON Rewrite feature updated the Remote Monitoring MIB to improve performance and available features. The following commands were introduced: **rmon capture-userdata**, **rmon collection history**, **rmon collection host**, **rmon collection matrix**, **rmon collection rmon1**, **show rmon capture**, **show rmon filter**, **show rmon hosts**, **show rmon matrix**.
RMON Events and Alarms	11.2 Cisco IOS XE Release 2.1	The RMON Events and Alarms feature introduces the ability to combine 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. In Cisco IOS XE Release 2.1, this feature was introduced on Cisco ASR 1000 series routers. The following commands were introduced: **rmon alarm**, **rmon event**, **rmon queuesize**.

Feature Name	Releases	Feature Information
RMON Full	11.2	The RMON Full feature identifies activity on individual nodes and helps monitor all nodes and their interaction on a LAN segment. Used in conjunction with the SNMP agent in a router, RMON can be used to view both traffic that flows through the router and segment traffic not necessarily destined for the router.
RMON MIB enhancement to support 64 bit counters	12.2(33)SXI 12.2(33)SRE	RMON MIB enhancement to support 64 bit counters features provides support for the ability to poll 64 bit counters.