



RMON Configuration Guide, Cisco IOS Release 15M&T

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

RMON Events and Alarms 1

Finding Feature Information 1

Information About RMON Events and Alarms 1

Overview of RMON Events and Alarms 1

RMON Event and Alarm Notifications 2

HC Alarm MIB 2

How to Configure RMON Events and Alarms 3

Configuring RMON 3

Configuring RMON Event and Alarm Notifications 5

Configuration Examples for RMON Events and Alarms 6

Example: Configuring RMON 6

Example: Configuring RMON Event and Alarm Notifications 7

Additional References for RMON Events and Alarms 8

Feature Information for RMON Events and Alarms 9



RMON Events and Alarms

Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.

RMON delivers information in RMON groups of monitoring elements, each providing specific sets of data to meet common network-monitoring requirements.

This module describes the features of the RMON Alarm group and the RMON Events group, and explains how to configure RMON events and alarms.

- [Finding Feature Information, page 1](#)
- [Information About RMON Events and Alarms, page 1](#)
- [How to Configure RMON Events and Alarms, page 3](#)
- [Configuration Examples for RMON Events and Alarms, page 6](#)
- [Additional References for RMON Events and Alarms, page 8](#)
- [Feature Information for RMON Events and Alarms, page 9](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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.

Information About RMON Events and Alarms

- [Overview of RMON Events and Alarms, page 1](#)
- [RMON Event and Alarm Notifications, page 2](#)
- [HC Alarm MIB, page 2](#)

Overview of RMON Events and Alarms

Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data.

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 RMON Alarm group periodically takes statistical samples from variables in a probe and compares them with previously configured thresholds. If the monitored variable crosses a threshold, an event is generated. The RMON Alarm group provides information on the alarm type, the interval, and the start and stop thresholds.

The RMON Events group controls the generation and notification of events from a device. The RMON Events group provides information on the event type, the event description, and the time that the event was sent.

RMON Event and Alarm Notifications

RMON allows various network agents and console systems to exchange network monitoring data. 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 network 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 the same time. 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.

HC Alarm MIB

The High Capacity (HC) Alarm MIB (HC-ALARM-MIB) provides the capability to create alarms that monitor thresholds crossed by 64-bit MIB objects on an access server. The Remote Monitoring (RMON)-1 Alarm group and RMON-1 notification types are specific to 32-bit objects. The HC alarm MIB supports the polling of 64-bit RMON objects and is an extension of the RMON-1 Alarm group.

The RMON-1 Events group controls the generation and notification of events from a device. When an event is created, it is added to the RMON-1 Events group table. Each entry in this table describes parameters of an event that can be triggered by alarms. An entry may specify that a log entry must be created whenever an event occurs. The entry may also specify that a notification should occur through Simple Network Management Protocol (SNMP) trap messages.

The HC Alarm MIB defines two SNMP traps: hcRisingAlarm and hcFallingAlarm. The hcRisingAlarm trap is used when a rising-threshold value is crossed, and the hcFallingAlarm trap is used when a falling-threshold value is crossed.

High Capacity (HC) alarms are triggered when a monitored variable exceeds a set rising-threshold value or falls below a set falling-threshold value. HC alarms can be set on any HC MIB object on an access server.

Given below is a typical flow of how a 64-bit RMON object is monitored:

- 1 A user creates an event. The user defines the actions to be executed when an event occurs: creation of a log entry or notification by SNMP trap messages. The event is added to the RMON-1 Events group table.
- 2 A user creates an HC alarm. The user defines the MIB object that needs to be monitored by the alarm, the interval for monitoring, the rising-threshold value, and the falling-threshold value. The user also defines the events that are triggered when a rising-threshold value or falling-threshold value is crossed. The HC alarm is added to the HC alarm table.

- 3 The HC alarm monitors the MIB object according to the defined interval. If the counter value crosses the respective thresholds, the HC alarm is triggered.
- 4 When an HC alarm is triggered, the defined events are also triggered.
- 5 When an event is triggered, the actions defined in the events are executed. Either a log entry is created or an SNMP trap is generated.

How to Configure RMON Events and Alarms

- [Configuring RMON, page 3](#)
- [Configuring RMON Event and Alarm Notifications, page 5](#)

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: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 <code>interface <i>type number</i></code> Example: Device(config)# interface FastEthernet 1/0	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4 <code>rmon {native promiscuous}</code> Example: Device(config-if)# rmon native	Configures RMON on Ethernet interfaces in native or promiscuous mode. <ul style="list-style-type: none"> In the example, RMON is configured in the native mode.
Step 5 <code>exit</code> Example: Device(config-if)# exit	Exits the interface configuration mode and places the router in global configuration mode.
Step 6 <code>rmon queuesize <i>size</i></code> Example: Device(config)# rmon queuesize 128	(Optional) Configures the size of the queue that holds packets for analysis by the RMON process.
Step 7 <code>exit</code> Example: Device(config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 8 <code>show rmon</code> Example: Device# show rmon	Displays general RMON statistics.

Configuring 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 Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3 rmon event number [log] [trap community] [description string] [owner string] Example: Device(config)# rmon event number	Adds or removes an event (in the RMON event table) that is associated with an RMON event number.
Step 4 rmon alarm number variable interval {delta absolute} rising-threshold value [event-number] falling-threshold value [event-number] [owner string] Example: Device(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0 owner owner1	Configures an alarm on any MIB object.

Command or Action	Purpose
Step 5 <code>rmon hc-alarms <i>number variable interval</i> {<i>delta</i> <i>absolute</i>} <i>rising-threshold value</i> [<i>event-number</i>] <i>falling-threshold value</i> [<i>event-number</i>] [<i>owner string</i>]</code> Example: <pre>Device(config)# rmon hc-alarms 2 ifInOctets.2 20 delta rising- threshold 2000 2 falling-threshold 1000 1 owner own</pre>	(Optional) Configures an HC alarm on any MIB object.
Step 6 <code>exit</code> Example: <pre>Device(config)# exit</pre>	Exits the global configuration mode and enters the privileged EXEC mode.
Step 7 <code>show rmon alarms</code> Example: <pre>Device# show rmon alarm</pre>	Displays the RMON alarm table.
Step 8 <code>show rmon hc-alarms</code> Example: <pre>Device# show rmon hc-alarms</pre>	Displays the RMON HC alarm table.
Step 9 <code>show rmon events</code> Example: <pre>Device# show rmon events</pre>	Displays the RMON event table.

Configuration Examples for RMON Events and Alarms

- [Example: Configuring RMON, page 6](#)
- [Example: Configuring RMON Event and Alarm Notifications, page 7](#)

Example: Configuring RMON

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

```
Device> enable
```

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

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

```
Device# show rmon

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

Example: Configuring RMON Event and Alarm Notifications

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

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

The following example shows how to create 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 shows how to generate a Simple Network Management Protocol (SNMP) trap when the event is triggered.

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

```
Device# 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:

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

The following example shows how to configure 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

```
Device# 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:

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

The following example shows how to configure 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.2 value 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 the ifInOctets.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 device, use the **show rmon hc-alarms** command in privileged EXEC mode. The following is a sample output from the command:

```
Device# 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
```

Additional References for RMON Events and Alarms

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

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> RMON MIB HC-Alarm MIB 	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

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 RMON Events and Alarms

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 1 *Feature Information for Configuring RMON Support*

Feature Name	Releases	Feature Information
RMON Events and Alarms	Cisco IOS XE Release 2.1	<p>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.</p> <p>The following commands were introduced or modified: rmon alarm and rmon event.</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.