



RMON Configuration Guide, Cisco IOS XE 16 (Cisco ASR 920 Series)

| | |
|--|----------|
| Configuring RMON Support | 2 |
| Finding Feature Information | 2 |
| Information About Configuring RMON Support | 2 |
| How to Configure RMON Support | 3 |
| Configuration Examples for RMON | 5 |
| Additional References | 5 |
| Feature Information for Configuring RMON Support | 6 |

Revised: April 5, 2022

Configuring RMON Support

The Remote Monitoring (RMON) MIB agent specification can be used 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 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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <https://cfnng.cisco.com/>. An account on Cisco.com is not required.

Information About Configuring RMON Support

The 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 SNMP agent in a device, 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 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 the RMON network management capabilities.

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

All Cisco IOS XE 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.

RMON MIB features include the following:

- **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. The table below details new partial probeConfig group objects.

Table 1: partial probeConfig Group Objects

| Object | Description |
|-------------------|---------------------------------------|
| probeCapabilities | The RMON software groups implemented. |

| Object | Description |
|-------------------------|--|
| probeSoftwareRev | The current version of Cisco IOS XE running on the device. |
| probeHardwareRev | The current version of the Cisco device. |
| probeDateTime | The current date and time. |
| 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 XE 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 another Cisco device as the default gateway. |
| hcRMONCapabilities | Specifies the features mapped to this version of RMON. |

How to Configure RMON Support

Setting an RMON alarm or event

Perform the following steps to set an RMON alarm or event:

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | rmon alarm <i>number variable interval {absolute delta } rising-threshold value [event-number] falling-threshold value [event-number] [owner string]</i> Example: <pre>Device(config)# rmon alarm 10 ifEntry.20.1 20 delta rising-threshold 15 1 falling-threshold 0 owner owner2</pre> | Sets an alarm on a MIB object. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 4 | rmon event <i>number</i> [log] [trap community] [description string] [owner string] Example: <pre>Device(config)# rmon event 1 log trap eventtrap description "High ifOutErrors" owner owner2</pre> | Adds or removes an event in the RMON event table. |
| Step 5 | end Example: <pre>Device(config)# end</pre> | Returns to privileged EXEC mode. |

Troubleshooting Tips

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.

The RMON MIB defines two traps, the risingAlarm and fallingAlarm traps generated when an RMON alarmEntry risingThreshold or fallingThreshold event occurs. Thresholds allow you to minimize the number of notifications sent on the network. Alarms are triggered when a problem exceeds a set rising threshold value. No more 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.

Monitoring and Verifying an RMON Configuration

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

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | show rmon Example: <pre>Device# show rmon</pre> | Displays general RMON statistics. |
| Step 3 | show rmon alarms Example: <pre>Device# show rmon alarms</pre> | Displays the RMON alarm table. |
| Step 4 | show rmon events Example: | Displays the RMON event table. |

| | Command or Action | Purpose |
|--|---------------------------------|---------|
| | Device# show rmon events | |

Configuration Examples for RMON

Example: Configuring Alarms and Events

The following example shows how to add an event (in the RMON event table) that is associated with an RMON event number, using the **rmon event** global configuration command:

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

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 “owner_a” 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 example shows how to configure an RMON alarm using the **rmon alarm** global configuration command:

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

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.

Additional References

The following sections provide references related to the Configuring RMON Support feature.

MIBs

| MIB | MIBs Link |
|------------------------------|---|
| Remote Monitoring (RMON) MIB | To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | http://www.cisco.com/techsupport |

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 2: Feature Information for Configuring RMON Support

| Feature Name | Releases | Feature Information |
|------------------------|----------|--|
| RMON Events and Alarms | | The Remote Monitoring (RMON) MIB agent specification can be used in conjunction with Simple Network Management Protocol (SNMP) to monitor traffic using alarms and events. |

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.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2017–2019 Cisco Systems, Inc. All rights reserved.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.