RMON Configuration Guide, Cisco IOS Release 15SY

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

CONTENTS

RMON Events and Alarms 1

- Finding Feature Information 1
- Prerequisites for Configuring RMON Support 1
- Restrictions for Configuring RMON Support 2
- Information About RMON Events and Alarms 2
  - Overview of RMON Events and Alarms 2
  - RMON Groups 2
  - RMON Event and Alarm Notifications 4
  - RMON MIB 4
  - HC Alarm MIB 5
- How to Configure RMON Events and Alarms 6
  - Configuring RMON 6
  - Configuring RMON Event and Alarm Notifications 8
  - Configuring RMON Groups 10
- Configuration Examples for RMON Events and Alarms 13
  - Example: Configuring RMON 13
  - Example: Configuring RMON Event and Alarm Notifications 13
  - Configuring RMON Tables Example 15
- Additional References for RMON Events and Alarms 15
- Feature Information for RMON Events and Alarms 16

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
- Prerequisites for Configuring RMON Support, page 1
- Restrictions for Configuring RMON Support, page 2
- Information About RMON Events and Alarms, page 2
- How to Configure RMON Events and Alarms, page 6
- Configuration Examples for RMON Events and Alarms, page 13
- Additional References for RMON Events and Alarms, page 15
- Feature Information for RMON Events and Alarms, page 16

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.

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.
- Even though the Switched Port Analyzer (SPAN) is specified as the source interface, broadcast and multicast traffic that flow through other interface ports are also captured by the SPAN destination interface.
- Traffic between different VLANs can be captured by the SPAN destination interface.

Information About RMON Events and Alarms

- Overview of RMON Events and Alarms, page 2
- RMON Groups, page 2
- RMON Event and Alarm Notifications, page 4
- RMON MIB, page 4
- HC Alarm MIB, page 5

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 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 10.

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

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.

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.

Object	Description
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 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 (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 6
- Configuring RMON Event and Alarm Notifications, page 8
- Configuring RMON Groups, page 10

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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(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:** `Device(config-if)# rmon native`	Configures RMON on Ethernet interfaces in native or promiscuous mode. • In the example, RMON is configured in the native mode.
Step 5	**exit** **Example:** `Device(config-if)# exit`	Exits the interface configuration mode and places the router in global configuration mode.
Step 6	**rmon queuesize** *size* **Example:** `Device(config)# rmon queuesize 128`	(Optional) Configures the size of the queue that holds packets for analysis by the RMON process.
Step 7	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

	Command or Action	Purpose
Step 8	**show rmon** **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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

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

	Command or Action	Purpose
Step 9	**show rmon events** **Example:** `Device# show rmon events`	Displays the RMON event table.

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.

	Command or Action	Purpose
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.
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.

	Command or Action	Purpose
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.
Step 14	**show rmon statistics** **Example:** `Router# show rmon statistics`	Displays the RMON statistics table.

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

Configuration Examples for RMON Events and Alarms

- Example: Configuring RMON, page 13
- Example: Configuring RMON Event and Alarm Notifications, page 13
- Configuring RMON Tables Example, page 15

Example: Configuring RMON

The following example shows how to configure RMON with a queuesize 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.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 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
```

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 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
• 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

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 4 Feature Information for Configuring RMON Support

Feature Name	Releases	Feature Information
RMON Events and Alarms	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. The following commands were introduced or modified: **rmon alarm** and **rmon event**.

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.