Contents

1 Configuring RMON

1.1 Introduction

1.1.1 Overview

The Remote Network Monitoring (RMON) protocol is a network management protocol that is built on the Simple Network Management Protocol (SNMP) architecture. RMON provides statistics and alarm functions for a managing device to remotely monitor and manage devices. he statistics function means that a managed device can trace and calculate different types of traffic information on a network segment that is connected to the port of the device regularly or continuously. For example, the device can trace and calculate the total number of packets or the total number of excessively long packets received on a network segment in a period. The alarm function means that a managed device can monitor specified management information base (MIB) variables and automatically record an event and send Trap messages to the managing device when one of the variables reaches the alarm threshold, for example, the port rate or the ratio of broadcast packets reaches a specified value.

Both RMON and SNMP are used for remote network management. Compared with SNMP, RMON has the following advantages:

- RMON notifies the managing device of alarm variable abnormality in Trap messages by using the SNMP Trap message sending mechanism. Though the Trap function is also defined in SNMP, this function is used to notify the managing device of the function running status of a managed device and physical state change of an interface. SNMP and RMON have different monitored objects, trigger conditions, and report content.
- Compared with SNMP, RMON can monitor remote network devices more effectively and actively, thus providing an efficient means of monitoring subnet running. According to RMON, a managed device can automatically send Trap messages when a value reaches the alarm threshold. This frees the managing device from frequently obtaining and comparing values of MIB variables and thus reduces the communication between the managing device and managed device. As a result, large interconnected networks are being managed simply yet effectively.

1.1.2 Principles

RMON defines different RMOM groups, and Orion_B26Q devices support the statistics group, history group, alarm group, and event group. The four groups are as follows:

1. Statistics Group

A statistics group is used to monitor and calculate traffic data on an Ethernet interface. The traffic data consists of cumulative values and is calculated from the time of entry creation to the current time. Statistical objects include discarded packets, broadcast packets, CRC errors, over-small or over-large packets, and conflicts. The statistical results are saved in the Ethernet statistical table for the administrator to view at any time.

2. History Group

A history group is used to collect network traffic periodically and records cumulative values of the traffic and bandwidth usage in each period. The data is saved in the history control table for the administrator to process. A history group includes two sub-groups:

- The HistoryControl sub-group is used to configure control information such as sampling interval and sampling data sources.
- The EthernetHistory sub-group provides the administrator with history data of a specific network segment, including traffic, error packets, broadcast packets, usage, and hit times.

3. Alarm Group

The alarm group is used to monitor specified MIB objects. When the value of an MIB object exceeds the set upper limit or lower limit, an alarm is triggered and processed as an event.

4. Event Group

An event group is used to define processing methods of events. When a monitored MIB object reaches the alarm condition, an event is triggered. The event can be processed with one of the following methods:

- None: The event is ignored.
- Log: The event related information is recorded in a log table for the administrator to view at any time.
- Snmp-trap: The Trap message is sent to the network management station to notify the occurrence of the event.
- Log-and-trap: The event-related information is recorded in a log table and the Trap message is sent to the network management station.

5. Working Process of RMON

RMON allows multiple monitor authorities to collect data with the following two methods: use the special RMON probe to collect data so that the NMS can obtain all MIB information from the RMON probe; embed the RMON agent into a network device (for example, switch or router) so that the device possesses the function of an RMON probe. The NMS uses basic commands of SNMP to exchange data with the network device and collect network management information. Limited by the device resources, this method does not obtain all data of the RMON MIB. Generally, only four groups of information are collected.

Through the RMON agent running on the managed network device, the NMS can obtain information such as traffic, error statistics, and performance statistics on the network segment that is connected to the port of this network device, to remotely manage this network device. Figure 1-1 shows the communication network between the NMS and RMON agent.

- RMON Ethernet statistics function

  Make the statistics of network traffic on the Ethernet interface from the time of entry creation to the current time.

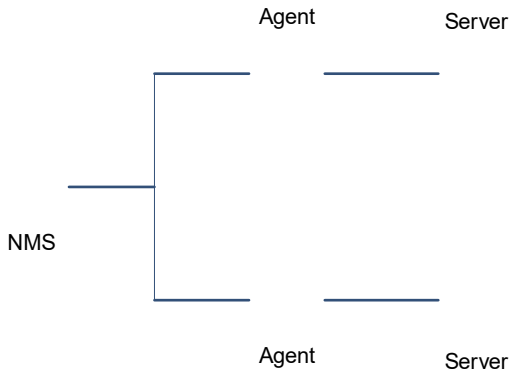
- RMON history statistics function

  Record cumulative statistical values of traffic on the Ethernet interface in each period.

- RMON alarm function

Monitor changes of alarm variable values periodically. If an alarm variable value exceeds the specified upper or lower limit, corresponding event is triggered, for example, a Trap message is sent or a LogTable entry record is created. Continuous excess of an upper or a lower limit triggers an event only once and the event can be triggered again by excess of the opposite limit.

Figure 1-1Communication Network Between the NMS and RMON Agent



1.1.3 Protocols and Standards

- STD 0059 / RFC 2819: Remote Network Monitoring Management Information Base
- RFC4502: Remote Network Monitoring Management Information Base Version 2
- RFC 3919: Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)
- RFC 3737: IANA Guidelines for the Registry of Remote Monitoring (RMON) MIB Modules
- RFC 3434: Remote Monitoring MIB Extensions for High Capacity Alarms
- RFC 3395: Remote Network Monitoring MIB Protocol Identifier Reference Extensions
- RFC 3287: Remote Monitoring MIB Extensions for Differentiated Services
- RFC 3273: Remote Network Monitoring Management Information Base for High Capacity Networks
- RFC 2896: Remote Network Monitoring MIB Protocol Identifier Macros
- RFC 2895: Remote Network Monitoring MIB Protocol Identifier Reference

1.2 Configuration Task Summary

RMON configuration includes the following tasks:

- Configuring the Ethernet Statistics Function
- Configuring the History Statistics Function
- Configuring the Alarm Function

1.3 Configuring the Ethernet Statistics Function

1.3.1 Overview

With the Ethernet statistics function of RMON, you can learn the cumulative statistical values of traffic generated on the monitored Ethernet interface from the time of entry creation to the current time.

1.3.2 Restrictions and Guidelines

- To calculate and monitor a specified interface, you must configure the Ethernet statistics function on this interface.
- After the statistics entry is created on the specified interface, the statistics group calculates the traffic of this interface. That is, make the statistics of variables defined by the Ethernet statistics table and record the cumulative values of variables that are generated from the creation time of the RMON statistics table to the current time.
- This function cannot be configured in the batch interface configuration mode.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure statistical items of RMON.

rmon collection stats *collection-stats-table-index* [**owner** *owner-name*]

The Ethernet statistics function is not configured on an Ethernet interface by default.

1.4 Configuring the History Statistics Function

1.4.1 Overview

With the history statistics function of RMON, you can learn the cumulative statistical values of traffic generated in each period and the bandwidth utilization on the monitored interface.

1.4.2 Restrictions and Guidelines

- The history group makes the statistics of variables defined by the history statistics function and records cumulative values of variables in each period.
- To collect network statistics on a specified interface, you must configure the history control function on the interface. This function cannot be configured in the batch interface configuration mode.
- It is not allowed to modify parameters of the configured history statistics function.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

Interface *interface type interface number*

(4) Configure the history statistics function of an Ethernet interface.

rmon collection history *collection-history-table-index* [**buckets** *bucket-number*] [**interval** *period-time*] [**owner** *owner-name*]

The history statistics function is not configured on an Ethernet interface by default.

1.5 Configuring the Alarm Function

1.5.1 Overview

The alarm function of RMON monitors whether the values of alarm variables vary within the valid range periodically.

1.5.2 Restrictions and Guidelines

- If alarm variables are MIB variables defined by the RMON statistical group or history group, the RMON statistics function or history statistics function must be configured on the monitored Ethernet interface. Otherwise, the alarm table fails to be created.
- The alarm function is implemented by the alarm table and event table. After an alarm event is triggered, the SNMP agent must be configured so that Trap messages can be sent to the managing device. For more information about SNMP agent configuration, see "Configuring SNMP" in *NMS and Monitoring Configuration Guide*.
- Configured event table parameters, including event type, Trap community name, event description, and event creator, can be modified.
- Configured alarm table parameters, including alarm variable, sampling type, table creator, sampling interval, upper/lower limit, and event, can be modified.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure an event table.

rmon event *event-table-index* [**description** *description-string*] [**log**] [**owner** *owner-name*] [**trap** *community*]

No RMON event is configured by default.

(4) Configure the alarm function.

rmon alarm *alarm-table-index alarm-variable sampling-interval* { **absolute** | **delta** } **rising-threshold** *ampling-rising-threshold-value* [*event-number*] **falling-threshold** *falling-threshold-*[*event-number*] [**owner** *owner-name*]

The RMON alarm function is not configured by default.

1.6 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Table 1-1Monitoring

Command	Purpose
show rmon	Displays all RMON configurations.
show rmon stats	Displays the Ethernet statistics table information.
show rmon history	Displays the history control table information.
show rmon alarm	Displays the alarm table information.
show rmon event	Displays the event table information

1.7 Configuration Examples

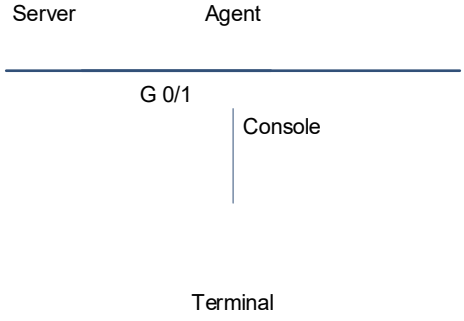
1.7.1 Configuring the Ethernet Statistics Function

1. Requirements

The RMON agent is connected to a server. The network administrator uses the RMON statistics group to calculate the performance of received packets on GigabitEthernet 0/1. Thus, the network administrator can understand the data of packets received on an interface at any time by viewing data, and take timely actions to process network abnormalities.

2. Topology

Figure 1-1Topology of the RMON Ethernet Statistics Function



3. Procedure

Configure a statistics table instance on GigabitEthernet 0/1 of the device on which the RMON agent is deployed to make the statistics of traffic on this interface.

```
Orion_B26Q> enable
Orion_B26Q# configure terminal
Orion_B26Q(config)# interface gigabitEthernet 0/1
Orion_B26Q(config-if-GigabitEthernet 0/1)# rmon collection stats 1 owner admin
```

4. Verification

Run the **show rmon stats** command to display Ethernet statistics information.

```
Orion_B26Q# show rmon stats
ether statistic table:
                  index = 1
                  interface = GigabitEthernet 0/1
                  owner = admin
                  status = 1
                  dropEvents = 0
                  octets = 25696
                  pkts = 293
                  broadcastPkts = 3
                  multiPkts = 0
                  crcAlignErrors = 0
                  underSizePkts = 0
                  overSizePkts = 0
                  fragments = 0
                  jabbers = 0
                  collisions = 0
                  packets64Octets = 3815
                  packets65To127Octets = 1695
                  packets128To255Octets = 365
                  packets256To511Octets = 2542
                  packets512To1023Octets = 152
                  packets1024To1518Octets = 685
```

5. Configuration Files

Agent configuration file

```
hostname Orion_B26Q
!
interface GigabitEthernet 0/1
 rmon collection stats 1 owner admin
!
end
```

6. Common Errors

The parameters of configured statistics entries are reconfigured or modified.

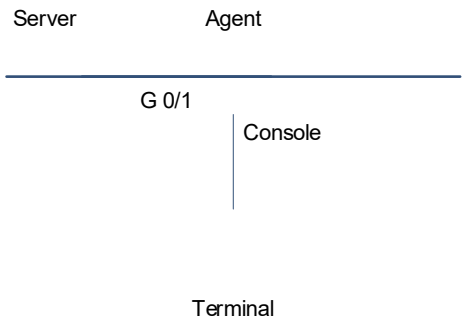
1.7.2 Configuring the History Statistics Function

1. Requirements

The RMON agent is connected to a server. The network administrator uses the history group to make the statistics of received packets on GigabitEthernet 0/1 every minute so as to monitor the network and master emergencies.

2. Topology

Figure 1-1Topology of the History Statistics Function



3. Procedure

Configure a history control table on GigabitEthernet 0/1 of the device on which the RMON agent is deployed to make the statistics of traffic on this interface periodically.

```
Orion_B26Q> enable
Orion_B26Q# configure terminal
Orion_B26Q(config)# interface gigabitEthernet 0/1
Orion_B26Q(config-if-GigabitEthernet 0/1)# rmon collection history 1 buckets 5
interval 300 owner admin
```

4. Verification

Run the **show rmon history** command to display history group statistics.

```
Orion_B26Q# show rmon history
rmon history control table:
                    index = 1
                    interface = GigabitEthernet 0/1
                    bucketsRequested = 5
                    bucketsGranted = 5
                    interval = 60
                    owner = admin
                    stats = 1

rmon history table:
                    index = 1
                    sampleIndex = 786
                    intervalStart = 6d:18h:37m:38s
```

```
dropEvents = 0
octets = 2040
pkts = 13
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0

index = 1
sampleIndex = 787
intervalStart = 6d:18h:38m:38s
dropEvents = 0
octets = 1791
pkts = 16
broadcastPkts = 1
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0

index = 1
sampleIndex = 788
intervalStart = 6d:18h:39m:38s
dropEvents = 0
octets = 432
pkts = 6
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0

index = 1
```

```
                    sampleIndex = 789
                    intervalStart = 6d:18h:40m:38s
                    dropEvents = 0
                    octets = 432
                    pkts = 6
                    broadcastPkts = 0
                    multiPkts = 0
                    crcAlignErrors = 0
                    underSizePkts = 0
                    overSizePkts = 0
                    fragments = 0
                    jabbers = 0
                    collisions = 0
                    utilization = 0

                    index = 1
                    sampleIndex = 790
                    intervalStart = 6d:18h:41m:38s
                    dropEvents = 0
                    octets = 86734
                    pkts = 934
                    broadcastPkts = 32
                    multiPkts = 23
                    crcAlignErrors = 0
                    underSizePkts = 0
                    overSizePkts = 0
                    fragments = 0
                    jabbers = 0
                    collisions = 0
                    utilization = 0
```

5. Configuration Files

Agent configuration file

```
hostname Orion_B26Q
!
interface GigabitEthernet 0/1
 rmon collection history 1 buckets 5 interval 300 owner admin
!
end
```

6. Common Errors

The parameters of configured history control entries are reconfigured or modified.

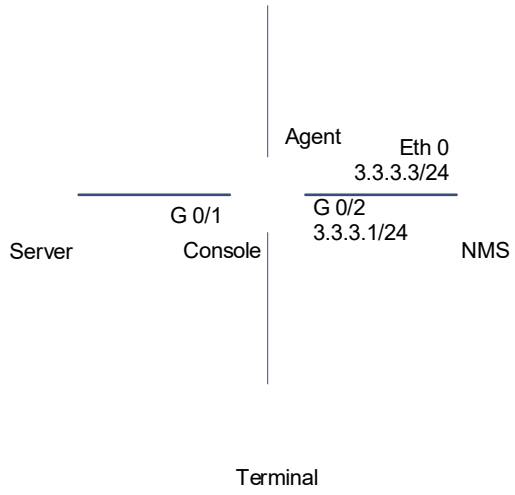
1.7.3 Configuring the Alarm Function

1. Requirements

The RMON agent is configured on a terminal device and connected to the NMS device for communication. The port GigabitEthernet 0/1 is connected to the server and must be monitored the number of received packets with unknown protocols. The sampling interval is 60 seconds. When the absolute collection value is smaller than 10, only a log record is generated. When the absolute sampling value is greater than 100, a log record is generated and a notification is sent to the NMS in a Trap message.

2. Topology

Figure 1-1Topology of the Alarm Function



3. Notes

- Run SNMPv1 on the NMS, configure a community name public1, set the attribute to RW, and set the Trap message receiving address to 3.3.3.3.
- Monitor the number of packets with unknown protocols, received on GigabitEthernet0/1, and check whether the OID value is 1.3.6.1.2.1.2.2.1.15.3, sampling method is relative sampling, and sampling interval is 60 seconds. Check whether event 1 or event 2 is triggered when the relative sampling value is greater than 100 or smaller than 10. For event 1, a Trap message is sent and a log record is generated. For event 2, a log record is generated.

4. Procedure

Set the IP address of GigabitEthernet0/2 on the agent to 3.3.3.1.

```
Orion_B26Q> enabel
Orion_B26Q# configure terminal
Orion_B26Q(config)# interface gigabitEthernet 0/1
Orion_B26Q(config-if-GigabitEthernet 0/1)# ip address 3.3.3.1 255.255.255.0
Orion_B26Q(config-if-GigabitEthernet 0/1)# exit
```

Configure an event group to process alarms.

```
Orion_B26Q(config)# snmp-server community public1 rw
Orion_B26Q(config)# snmp-server host 3.3.3.3 trap public1
Orion_B26Q(config)# rmon event 1 description rising-threshold-event log trap
public owner admin
Orion_B26Q(config)# rmon event 2 description falling-threshold-event log owner
admin
```

Configure the alarm function.

```
Orion_B26Q(config)# rmon alarm 1 1.3.6.1.2.1.2.2.1.15.3 60 delta rising-threshold
100 1 falling-threshold 10 2 owner admin
```

5. Verification

Run the **ping** command to verify that the agent and NMS are mutually reachable via L3 routes.

```
Orion_B26Q# ping 3.3.3.3
Sending 5, 100-byte ICMP Echoes to 3.3.3.3, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms.
```

Run the **show rmon event** command to display the event table information.

```
Orion_B26Q# show rmon event
rmon event table:
                   index = 1
                   description = rising-threshold-event
                   type = 4
                   community = public
                   lastTimeSent = 0d:0h:0m:0s
                   owner = admin
                   status = 1

                   index = 2
                   description = falling-threshold-event
                   type = 2
                   community =
                   lastTimeSent = 6d:19h:21m:48s
                   owner = admin
                   status = 1

rmon log table:
                   eventIndex = 2
                   index = 1
                   logTime = 6d:19h:21m:48s
                   logDescription = falling-threshold-event
```

Run the **show rmon alarm** command to display the alarm table information.

```
Orion_B26Q# show rmon alarm
```

```
rmon alarm table:
          index: 1,
          interval: 60,
          oid = 1.3.6.1.2.1.2.2.1.15.3
          sampleType: 2,
          alarmValue: 0,
          startupAlarm: 3,
          risingThreshold: 100,
          fallingThreshold: 10,
          risingEventIndex: 1,
          fallingEventIndex: 2,
          owner: admin,
          stauts: 1
```

6. Configuration Files

Agent configuration file

```
hostname Orion_B26Q
!
interface GigabitEthernet 0/1
 ip address 3.3.3.1 255.255.255.0
!
rmon alarm 1 1.3.6.1.2.1.2.2.1.15.3 60 delta rising-threshold 100 1 falling-
threshold 10 2 owner admin
rmon event 1 description rising-threshold-event log trap public1 owner admin
rmon event 2 description falling-threshold-event log owner admin
!
snmp-server host 3.3.3.3 traps public1
snmp-server community public1 rw
!
end
```

7. Common Errors

- The entered object OID is improper. For example, the variable corresponding to this OID does not exist or the OID type is not an integer or unsigned integer.
- The upper limit is smaller than or equal to the lower limit.