RAISECOM

www.raisecom.com

RMON Function Configuration
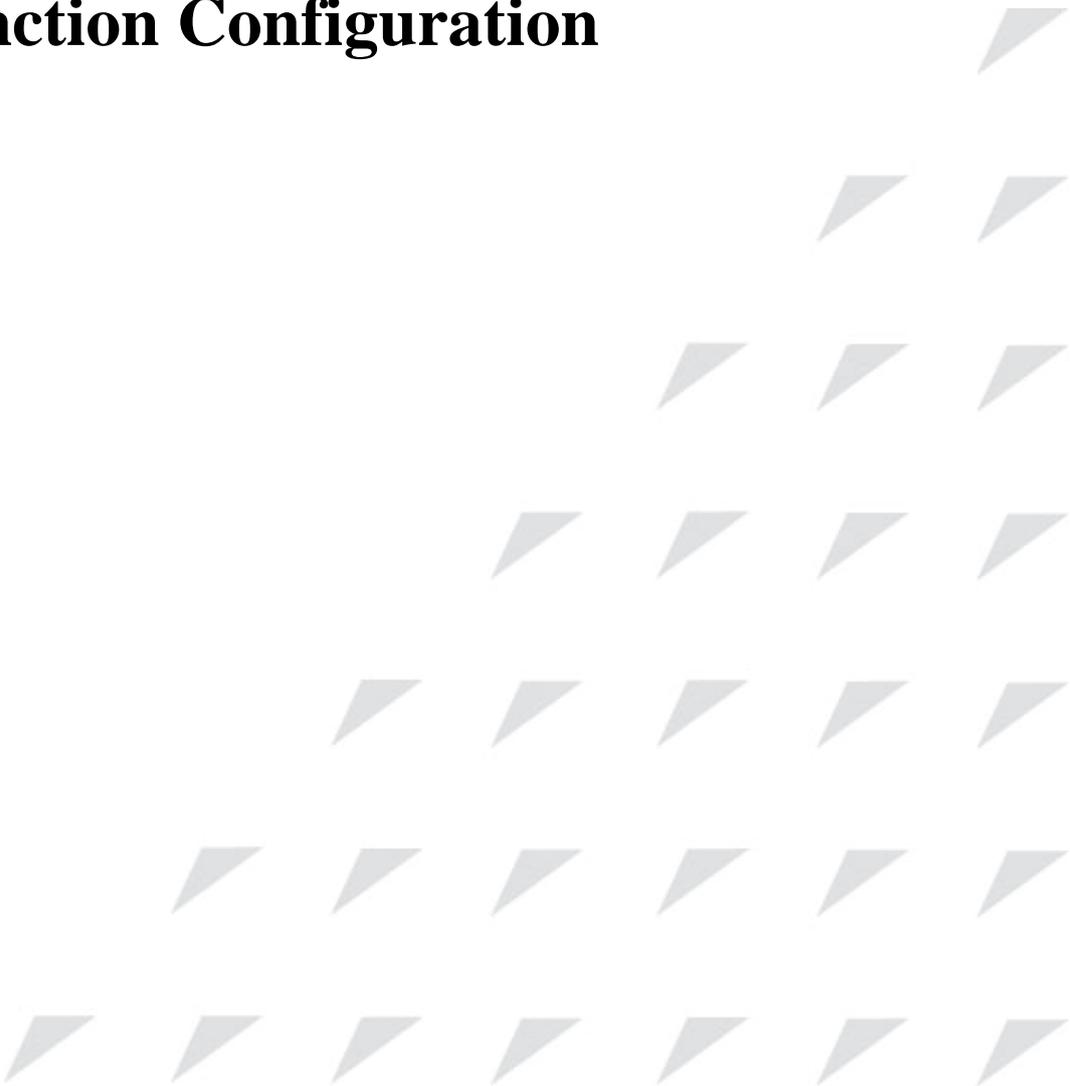
Legal Notices

Raisecom Technology Co., Ltd makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. **Raisecom Technology Co., Ltd** shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty.

A copy of the specific warranty terms applicable to your Raisecom product and replacement parts can be obtained from Service Office.

Restricted Rights Legend.

All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of **Raisecom Technology Co., Ltd.** The information contained in this document is subject to change without notice.

Copyright Notices.

Trademark Notices

RAISECOM is the trademark of Raisecom Technology Co., Ltd.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows® XP is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of

Microsoft Corporation.

Contact Information

Technical Assistance Center

The Raisecom TAC is available to all customers who need technical assistance with a Raisecom product, technology, or, solution. You can communicate with us through the following methods:

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road, Haidian District, Beijing 100085

Tel: +86-10-82883305

Fax: +86-10-82883056

World Wide Web

You can access the most current Raisecom product information on the World Wide Web at the following URL:

http://www.raisecom.com

Feedback

Comments and questions about how the … system software works are welcomed. Please review the FAQ in the related manual, and if your question is not covered, send email by using the following web page:

http://www.raisecom.com/en/xcontactus/contactus.htm.

If you have comments on the … specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Release Notes

Date of Release	Manual Version	Software Version	Revisions

Preface

About This Manual

This manual introduces primary functions of the configuration management software for RC series products.

Who Should Read This Manual

This manual is a valuable reference for sales and marketing staff, after service staff and telecommunication network designers. For those who want to have an overview of the features, applications, structure and specifications of … device, this is also a recommended document.

Relevant Manuals

《Raisecom NView System User Manual》

《Raisecom Nview System Installation and Deployment Manual》

《… User Manual》

《… Commands Notebook》

Organization

This manual is an introduction of the main functions of … EMS. To have a quick grasp of the using of the EMS of … , please read this manual carefully. The manual is composed of the following chapters

Chapter 1 Overview

This chapter briefly introduces the basic function of …

Chapter 2 Configuration Management

This chapter mainly introduces the central site configuration management function of the ….

Chapter 3 Performance Management

This chapter focuses on performance management function of ….

Chapter 4 Device Maintenance Management

This chapter introduces the device maintenance management function of ….

Appendix A Alarm Type

The alarm types supported by ….

Compliance

The RC series products developed by Raisecom are strictly complied with the following standards as well as ITU-T, IEEE, IETF and related standards from other international telecommunication standard organizations:

YD/T900-1997 SDH Equipment Technical Requirements - Clock

YD/T973-1998 SDH 155Mb/s and 622Mb/s Technical conditions of optical transmitter module and receiver module

YD/T1017-1999 Network node interface for the Synchronous Digital Hierarchy (SDH)

YD/T1022-1999 Requirement of synchronous digital hierarchy (SDH) equipment function

YD/T1078-2000 SDH Transmission Network Technique Requirements-Interworking of Network Protection Architectures

YD/T1111.1-2001 Technical Requirements of SDH Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Receiver Modules

YD/T1111.2- 2001 Technical Requirements of SHD Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Transmitter Modules

YD/T1179- 2002 Technical Specification of Ethernet over SDH

G.703 Physical/electrical characteristics of hierarchical digital interfaces

G.704 Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

G.707 Network node interface for the synchronous digital hierarchy (SDH)

G.774 Synchronous digital hierarchy (SDH) - Management information model for the network element view

G.781 Synchronization layer functions

G.783 Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks

G.784 Synchronous digital hierarchy (SDH) management

G.803 Architecture of transport networks based on the synchronous digital hierarchy (SDH)

G.813 Timing characteristics of SDH equipment slave clocks (SEC)

G.823 The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy

G.825 The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)

G.826 End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections

G.828 Error performance parameters and objectives for international, constant bit-rate synchronous digital paths

G.829 Error performance events for SDH multiplex and regenerator sections

G.831 Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)

G.841 Types and characteristics of SDH network protection architectures

G.842 Interworking of SDH network protection architectures

G.957 Optical interfaces for equipments and systems relating to the synchronous digital hierarchy

G.691 Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers

G.664 Optical safety procedures and requirements for optical transport systems

I.731 ATM Types and general characteristics of ATM equipment

I.732 ATM Functional characteristics of ATM equipment

IEEE 802.1Q Virtual Local Area Networks (LANs)

IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering

IEEE 802.3 CSMA/CD Access Method and Physical Layer Instruction

Chapter 1 RMON Function Configuration

16.1 RMON principle interview

RMON is a standard of network data monitoring using different network Agent and manage station systems designated by IETF, which can make SNMP monitoring remote equipments more effectively and forwardly. Therefore, network administrator can track network, network segment and the equipment faults more quickly. This way reduces the data stream between the manage station and the Agent and makes simple and powerful management to large network, which makes up the limitation that SNMPS is facing in the distributed connection that is becoming larger and larger.

We can use SNMP Agent in the switch side to monitor and manage the switch network situation. Now the 1, 2, 3, 9 group of RMON is realized, that is statistic group, history group, alarm group and event group.

- Statistics: Collects Ethernet, Fast Ethernet, and Gigabit Ethernet statistics on an interface.

- History: Collects a history group of statistics on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces for a specified polling interval.

- Alarm: Monitors a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified value (rising threshold), and resets the alarm at another value (falling threshold). Alarms can be used with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.

- Event: Determines the action to take when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.

16.2 RMON configuration

16.2.1 Default RMON configuration

Function	Default value
Static group	Enabled
History static group	No
Alarm group	No
Event group	No

16.2.2 RMON static group configuration

Configure the port's statistic function parameter, if the port's statistic function is disabled, use the command to enable it again; if it is enabled, use the command to change the corresponding parameter. By default all the port's statistic function is enabled, use command **no** to disable it.

Step	Command	Description

1	config	Enter global configuration mode
2	**rmon statistics** {**ip** *l3_interface* | **port** *port_list*} [**owner** *STRING*]	**ip** *l3_interface* set the statistics function of layer 3 interface, range is 0-14; **port** *port_list* set the statistics function for the physical port, range is 1-26; **owner** *STRING* set the owner name of current statistics group, default value is "monitorEtherStats".
3	**exit**	Exit from global configuration mode to enter privileged EXEC mode.
4	**show rmon statistics**	Show statistics group information.

To disable statistic group, use the command: **no rmon statistics {ip** *13_interface* \| **port** *port_list}*

⚠ Notice:

➢ Before RMON function is configured, SNMP Agent correct configuration must be made sure.

➢ When the statistic function of some port is disabled, it means not that data statistic is stopped, but that user can no longer acquire the port's statistic data.

16.2.3 RMON history statistic and configuration

Configure the port's statistic function parameter. If the port's history statistic function is disabled, use the command to enable it again; if it is enabled, use the command to change the corresponding parameters. All the ports, including three-layer port and physical port, are open by default, Use command **no** to disable it. When one port's history group function is disabled, data collection and statistic function can not go on, and all the history data collected before will be cleared.

Step	Command	Description
1	config	Enter global configuration mode
2	**rmon history** {**ip***l3_interface* | **port** *port_list*} [**shortinterval** *short-time*] [**longinterval** *long-time*] [**buckets** *queuesize*]	**ip** *l3_interface* Set the RMON history function of layer 3 interface, range is 0-14; **port** *port_list* set the RMON

	[**owner** *STRING*]	history function of physical port, range is 1-26;
		shortinterval *short-time:* the short time interval of history data collection of the port, range is 1-3600, default value is 2 seconds.
		longinterval *long-time* the long time interval of history data collection of the port, range is 1-3600, default value is 300 seconds (5 minutes);
		buckets *queuesize:* circular queue size for history data, range is 10-1000, default is 10.
		owner *STRING:* set the owner name of RMON history group, default name is "monitorHistory".
3	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
4	**show rmon history**	Show history statistics information

16.2.4 RMON alarm group configuration

Use command **no** to delete a warning to configure a MIB variable that is being monitored,

The MIB variable that is being monitored must be really exist, and it must be INTEGER type in ASN.1 expression, like type of INTEGER, Counter, Gauge and TimeTicker. If the variable does not exist or the type is incorrect when configured, return fault; in the alarm that has been successfully configured, if the variable is not collected in the late time, the warning will be shut up. Re-configuration is needed to monitor the variable again.

If the index number of trigger event is not configured, the default value will be 0, which means the event will not be triggered, because 0 is not a valid event number. If the index number of the event is not 0, but the event is not configured correspondingly in the event group, then the event will not be triggered successfully when the monitoring variable exceeds until the event is established.

Step	Command	Description

1	**config**	Enter global configuration mode
2	**rmon event** *number* [**log**] [**trap**] [**description** *string*] [**owner** *string*]	*number* event index number **log** whether log the information and send system log information **trap** whether send trap **description** *string*: description string **owner** *string* the owner of the event
3	**exit**	Exit from global configuration mode.
4	**show event** *number*	Show configuration information

Use command **no alarm** *number* to delete alarm.

16.2.5 RMON event group configuration

Step	Command	Description
1	`config`	Enter global configuration mode
2	`rmon event` *number* `[log] [trap]` `[description` *string*`] [owner` *string*`]`	Configure the event group function parameter of the port. *number* event index number `description` *string* description character string `owner` *string* owner of the event
3	`exit`	Quit global configuration mode and enter privileged EXEC mode
4	`show alarm` number	Show the configuration result number event index number

Use the command **no event** *number* to delete event.

16.2.6 Monitoring and maintenance

Command	Description
show rmon	Show all the RMON four group information
show rmon alarms	Show alarm information, including alarm number, name, threshold, sampling period and sampling value.
show rmon events	Show alarm information, including alarm number, name, threshold, sampling period and sampling value.
show rmon statistics	Show port information which has enabled statistics group.

Configure all the RMON groups' function to default state, that is the state when the switch has just been started

Step	Command	Description
1	**config**	Enter global configuration mode
2	**clear rmon**	Restore to the default state
3	exit	Quit global configuration mode and enter privileged EXEC mode.

16.2.7 Typical configuration example

1. Network requirement:

Agent connects the configuration terminal through console port, and connects remote NMS through Internet. In RMON Ethernet static table, set a table item, make performance statistic for Ethernet port, and record log when in a certain time the byte number that the port received exceeds the configured threshold.

2. Network figure
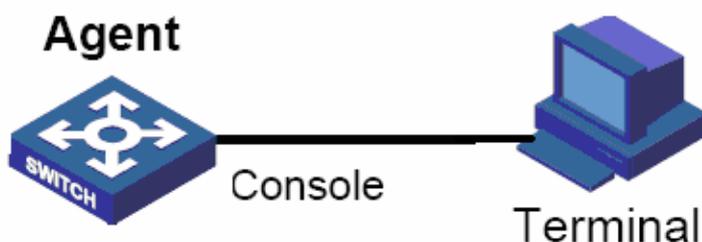
3. Configuration steps:

First, establish a event with the index number 1, and the description character stream is High-ifOutErrors for the event that sends out **log**, owner is system. Then, set a alarm, monitor MIB variable 1.3.6.1.2.1.2.2.1.20.1, examine if the variable is rising/falling every 20s, if it has rise 15, alarm will be triggered, the owner's name is the same with the event group.

```
Raisecom#config
Raisecom(config)#rmon event 1 log description High-ifOutErrors owner system
Raisecom(config)#rmon  alarm  10  1.3.6.1.2.1.2.2.1.20.1  interval  20  delta
rising-threshold 15 1 falling-threshold 0 owner system
Raisecom(config)#exit
Raisecom#show rmon alarm
Alarm 10 is active, owned by system
Monitors 1.3.6.1.2.1.2.2.1.20.1 every 20 seconds
Taking delta  samples, last value was 0
Rising threshold is 15, assigned to event 1
Falling threshold is 0, assigned to event 0
On startup enable rising and falling alarm
Raisecom#show rmon event
Event 1 is active, owned by system
Event generated at 0:0:0
Send TRAP when event is fired.
```