RAISECOM

www.raisecom.com

RC581 Configuration User Manual

Raisecom ROS 3.0
Apr-01-2006

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.

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:

Add: 1120, Haitai Tower, 229 Fourth North Loop Middle Road, Haidian District, Beijing 100083

Tel: +86-10-82884499 Ext.878 (International Department)

Fax: +86-10-82885200, +86-10-82884411

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 NView iEMS 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 NView iEMS specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Preface

About This Manual

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

Who Should Read This Manual

Sales and marketing engineers, after service staff and telecommunication network design engineers could use this manual as a valuable reference. If you want to get an overview on features, applications, architectures and specifications of Raisecom RC series integrated access devices, you could find useful information in this manual as well.

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 System Overview

Audience

This guide is compiled only for those professionals who need to configure the RC581 series demarcations. It mainly introduces the functional modules' theories and features as well as the configuration guide for the modules.

Structure

This guide includes the following parts:

Chapter 2: Summarization

Systematically introduce the functional features of RC581 series demarcations.

Chapter 3: Command-line of system

Introduce how to use the command line to configure the RC581 series demarcations.

Chapter 4: Command-line configuration.

Introduce the function and configuration methods of RC581 series Ethernet demarcations.

Chapter 5: Bandwidth management function configuration

Introduce the bandwidth management function and configuration methods for the RC581 series demarcations.

Chapter 6: Physical layer interface configuration

Introduce the configuration of physical layer interface for the RC581 series demarcations.

Chapter 7: Layer 3 interface configuration

Introduce the configuration of Layer 3 interface for the RC581 series demarcations.

Chapter 8: RMON configuration

Introduce the basic RMON conceptions and configurations for the RC581 series demarcations.

Chapter 9: ARP management configuration

Introduce the basic ARP conceptions and configurations for the RC581 series demarcations.

Chapter 10: SNMP configuration

Introduce the basic SNMP conceptions and configurations for the RC581 series demarcations.

Chapter 11: System log configuration

Introduce the basic conceptions and configuration methods of system log configuration for the RC581 series demarcations.

Chapter 12: System clock

Introduce the system clock configuration methods for the RC581 series demarcations.

Chapter 13: Malfunction location command

Introduce the using of malfunction location command for the RC581 series demarcations.

Chapter 14: VLAN configuration

Introduce the basic VLAN principles and the configuration methods for the RC581 series demarcations.

Chapter 15: ACL and network security configuration

Introduce the using and configuration methods for the RC581 series demarcations.

Chapter 16: QoS configuration

Introduce basic QoS principles and configurations for the RC581 series demarcations.

Chapter 17: Customer network

Introduce the basic theories and configuration of user network for the RC581 series demarcations.

Chapter 18: OAM

Introduce the basic OAM principles and configuration methods for the RC581 series demarcations.

ABBREVIATION

VLAN: Virtual LAN

QoS: Quality of Service

CoS: Class of Service

ToS: Type of Service

DSCP: Differentiated Services Code Point

WRR: Weighted Round Robin

ICMP: Internet Control Message Protocol

IGP: Interior Gateway Protocol

InARP: Inverse ARP

MBZ: Must be Zero

MIB: Management Information Base

PDU: Protocol Data Unit

Reference

< RAISECOM Series Switch Command Notebook >

Chapter 2 Summarization

Base on standardized layer 2 protocol

- ✧ 802.1Q(tag VLAN: 4096)

Management function

- ➢ Support SNMP(RFC1157)、SNMP V2 and SNMPV3;
- ➢ Support management by using CONSOLE;
- ➢ Support remote management by using TELNET
- ➢ Support automatic configuration, can download configuration files from network management server automatically for updating.
- ➢ Support rmon 1, 2 , 3, 9 group;
- ➢ Support RC-OAM

Bandwidth management

- ✧ Bandwidth management based on ports

Layer 3 functions

- ✧ Support double Ip4 protocol stack

Chapter 3 Command line of system

Software & hardware environment

The hardware environment for running the ROS-LITE is: RC581 series Ethernet demarcation platform.

Software environment is: ROS-LITE3.0

Command line mode

Mode	Description	Login mode	Mode identifier
User EXEC	User can configure the terminal settings and the displaying	Login the demarcation and input the username and password	Raisecom>
Privileged EXEC(enable)	In this mode, user can configure the basic information for the demarcation, such as the system time, demarcation name and so on. Running information can not be configured here.	Input **enable** and the relevant password under the User EXEC	Raisecom#
Global configuration	User can configure all the running parameters for the demarcation under this mode	Input **config** under the Privilege EXEC	Raisecom(config)#
Interface configuration	User can configure the demarcation's Ethernet physical interface parameters under this mode	Input **interface port** *portid* command under the Global configuration mode	Raisecom(config-port)#

User network mode	Under this mode, user can configure the user network Layer 3 setttings, display the user network information and user network tools	Input **user-network diagnostics** command under the Global configuration mode	Raisecom(config-usrnet)#

Acquire help

Command	Description
help	Get a short system help both in English and in Chinese.
*abbreviated-command-entry***?**	Get a list for all the available commands that match a particular string prefix(*abbreviated-command-entry*). For example: ISCOM2826> **en?** **english enable**
abbreviated-command-entry<**Tab**>	Complement an incomplete command. For example. Raisecom#**show ser**<Tab> Raisecom#**show service**
?	List all the commands under this mode. For example Raisecom#**?**
command **?**	List all the key words, options and brief help information for a command Raisecom#**show ?**

User history commands

About 20 history commands are reserved in the default demarcation. User can input

Raisecom>**terminal history** *<0-20>* to configure number for the system's reserved history commands.

Use the edit attribute

up arrow: last entered command;

down arrow: the next entered command;

left arrow: left move a character;

right arrow: right move a character;

backspace: delete a character in front of the cursor

Ctrl+d: delete a character at the cursor

Ctrl+a: move the cursor to the beginning of the command line.

Ctrl+e: move the cursor to the end of the command line

Ctrl+k: delete all the characters on the right side the cursor

Ctrl+w: delete all the characters on the left side of the cursor

Ctrl+u: delete the row all

Ctrl+z: exit from other modes to privileged EXEC

Chapter 4 System Command configuration

This chapter mainly depicts the basic configuration, user management and hardware environment monitoring.

Basic system command and configuration

chinese: System help information will display in Chinese

english: System help information will display in English

clear: Clear up the information

list: Show all the command list under each mode

clock set: Edit the system time

Configuration file and boot file management

Configuration setting

- The configuration file name of the current system under default situation is: startup_config.conf
- User can use **write** to write the configuration file into the system's flash file, the configuration will be renewed automatically after the system is rebooted.
- User can use **erase** command to delete the file;
- In order to renew the saved configuration file startup_config.conf, user can use **upload** and **download** based on TFTP protocol or FTP protocol to download or upload the configuration file from server.
- User can use **show startup-config** command to display the saved configuration information.
- User can use the **show running-config** command to view the system's current configuration information;

Startup file

- the program file, the system's current program file is: system_boot.z;
- The program file can be uploaded or downloaded from servers by using the **upload** or **download** commands based on TFTP protocol or FTP protocol.
- User can use **dir** to view the files in the flash system;
- User can use **show version** to view the software version;

User management

The system's default user name is: raisecom, password is: raisecom

If user wants to add a new user, the following steps should be followed:

Command	Description
user *USERNAME* **password** { **no-encryption | md5 }** *PASSWORD*	·*USERNAME* username; ·**Password** password keyword; ·{ **no-encryption | md5}** use none encryption password or md5 encryption password ·*PASSWORD* password information
user *USERNAME* **privilege** *<1-15>*	·*USERNAME* username; ·**Privilege** privilege keyword; ·*<1-15>* user privilege;
Write	Save the configuration
show user	view the user information

Hardware environment monitoring

System can display the chassis temperature and 1.2/1.5/1.8/3.3 volt's actual value, and can also monitor the chassis's temperature and 3.3v volts. System will send alarm when the temperature and 3.3v voltage operates abnormally.

Temperature monitor

1. Startup the temperature alarm function

Command	Description
config	Enter the Global configuration mode
alarm temperature	Startup the temperature alarm function
exit	Back to the privilege EXEC
show hardware	Show the hardware environment monitoring information

User can use **no alarm temperature** command to shut down the alarm function. This function is enabled under default situation.

2. Set the temperature alarm threshold value

The temperature units can be Celsius or Fahrenheit for configuration and displaying.

Command	Description

config	Enter the Global configuration mode
alarm temperature threshold Celsius low <0-30> **high** <30-70>	Configure the temperature alarm threshold value, the unit is Celsius
exit	Back to the privilege EXEC
show hardware	Show the hardware environment monitoring information

Command	Description
config	Enter the Global configuration mode
alarm temperature threshold Fahrenheit low <32-86> **high** <86-158>	Configure the temperature alarm threshold value, the unit is Fahrenheit
exit	Back to the privilege EXEC
show hardware	Show the hardware environment monitoring information

User can use **no alarm temperature threshold** to set the alarm threshold value back to the default value: 70 for high Celsius; 5 for low Celsius.

Volt monitor

1. enable the volt alarm function

Command	Description
config	Enter the Global configuration mode
alarm volt	enable the volt alarm function
exit	Back to privilege EXEC
show hardware	Show the hardware environment monitoring information

User can use the **no alarm volt** to disable the volt alarm function. This function is enabled under the default situation.

2. Configure the volt alarm threshold

The temperature unit is mV for configuration and displaying

Command	Description
config	Enter the Global configuration mode
alarm volt threshold low <3000-3300> **high** <3300-3600>	Configure the volt alarm threshold with the unit: mV
exit	Back to privilege EXEC
show hardware	Show the hardware environment

monitoring information

User can use **no alarm volt threshold** to set the volt alarm threshold to the default value: 3460mV for high value, 3140mv for low value.

Chapter 5 Bandwidth management and configuration

Sometimes user needs to limit the bandwidth for certain purpose. Under such situation, user can configure the ports' bandwidth to limit the bandwidth within a certain range, the data excluding the configuration will be discarded. The default situation is that: each port rate is autonegotiate with no bandwidth limitation.

Configure the bandwidth based on ports

Configure the port egress bandwidth limitation

Command	Description
config	Enter the Global configuration mode
rate-limit port *port-list* **egress** *rate*	Configure the physical port bandwidth limitation *port-list is* physical port number, the range can be from 1-2. User can use "," and "-" to input multiple ports. *Rate* is the bandwidth value, the unit is kbps, and range is from 1-1048576. The actual valued could be different from that configured. Egress is the data transmission direction.
exit	Back into the privilege EXEC
show rate-limit port-list [*port-list*]	Show the port bandwidth limitation *port-list* is the physical port number,

User can use **no rate-limit port** *port-list* **egress** to delete port bandwidth limitation under the global configuration mode.

Example

Configure the port 1 and port 2 egress bandwidth as 1Mbps.

Raisecom#config

Raisecom(config)#rate-limit port-list all egress 1000

SUCCESS !

Actual egress rate: 1000

Raisecom(config)#exit

Raisecom#sh rate-limit port-list

E-Rate: Egress Rate

Port E-Rate(Kbps)

---

1 1000

2 1000

Chapter 6 Physical port configuration

This chapter includes the following parts:

- ✧ Port rate and duplex mode configuration
- ✧ Port 802.3x flowcontrol configuration
- ✧ Port enable and shut down configuration
- ✧ Port fault-pass, fault-return and local loopback configuration

Port rate and duplex mode configuration

Gigabit Ethernet port is always configured as 1000Mbps and full duplex mode. When the rate (duplex mode) is configured as autonegotiation, the duplex mode (rate) will be configured as autonegotiation as well. The default situation is that all the ports are configured as autonegotiation.

Command	Description
config	Enter the Global configuration mode
interface port *port-number*	Enter the Ethernet physical port configuration mode. *port_numbe* is physical port number, range is from 1-2.
speed {auto | 10| 100 |1000 } **duplex** { full | half }	Port rate and duplex mode configuration. Auto means the port rate and duplex mode are both set as auto negotiation. 10 means the port rate is configured as 10Mbps. 100 means the port rate is configured as 100Mbps. 1000 means gigabit Ethernet port configuration. Full means the duplex mode is configured as full duplex mode. Half means the duplex mode is configured as half duplex mode.
exit	Back into the Global configuration mode
exit	Back into the privilege EXEC
show interface port *port-number*	Show the port status *port_number* is the physical port number, range is from 1-2.

User can use **speed auto** commands to configure the Ethernet physical port rate and duplex mode back to the default configuration which is autonegotiation.

Example: The port 1 rate will be configured as 10Mbps, duplex mode is configured as full duplex mode.

Raisecom#**config**

RAISECOM(config)#**interface port** 1

RAISECOM(config-port)#**speed** *10*

RAISECOM(config-port)# **duplex** full

RAISECOM(config-port)#**exit**

RAISECOM(config)#**exit**

Raisecom#**show interface port** *1*

R: Receive Direction

S: Send Direction

Port Admin Operate Speed/Duplex Flowcontrol(R/S)

---

1 enable down 10/full off/off

802.3x port flowcontrol configuration

The port flowcontrol at the egress and ingress directions should be configured simultaneously, which means egress or ingress should be configured as on or off simultaneously. The defaults situation is that the flowcontrol for all the ports is disabled.

Command	Description
config	Enter the Global configuration mode
interface port *port-number*	Enter the Ethernet physical interface configuration mode. *port_number* is the physical port number, the range is 1-2.
flowcontrol { **on** | **off** }	Configure the flowcontrol as on or off for the physical port **on** means enable the port flowcontrol **Off** means shut down the port flowcontrol
exit	Back to the Global configuration mode
exit	Back to the privilege user mode
show interface port *port-number*	Show the port flowcontrol status *port_number* is the physical port number, range is

1-2.

Example: enable the flowcontrol for the port 1

Raisecom#**config**

RAISECOM(config)# **interface port** *1*

RAISECOM(config-port)#**flowcontrol on**

RAISECOM(config-port)#**exit**

RAISECOM(config)#**exit**

Raisecom#**show interface port** *1*

R: Receive Direction

S: Send Direction

Port Admin Operate Speed/Duplex Flowcontrol(R/S)

---

1 enable down auto on/on

Ports enable and shut down configuration

User sometimes needs to shut down the port for certain purpose. The default situation is that all the ports are enabled.

Command	Description
config	Enter the Global configuration mode
interface port *port-number*	Enter the Ethernet physical port or batch configuration mode. *port_number* is the physical port number, range is 1-2.
{ **shutdown | no shutdown** }	Shut down or enable the physical port **shutdown** means shut down the physical port **no shutdown** means enable the physical port
exit	Back to the global configuration mode
exit	Back to the privilege EXEC mode
show interface port *port-number*	Show the port status *port_number* is the physical port number, range is 1-2.

Example: shut down port 2.

Raisecom#**config**

RAISECOM(config)# **interface port** 2

RAISECOM(config-port)#**shut down**

RAISECOM(config-port)#**exit**

RAISECOM(config)#**exit**

Raisecom#**show interface port** *2*

R: Receive Direction

S: Send Direction

Port Admin Operate Speed/Duplex Flowcontrol(R/S)

---

2 enable down auto off/off

Port fault-pass, fault-return and loopback configuration

1. Enable the port fault-pass function

Command	Description
config	Enter the global configuration mode
interface port *port-number*	Enter the Ethernet physical interface or batch configuration mode.
fault-pass {enable|disable}	Enable or shut down the physical interface fault-pass function
exit	Back to the global configuration mode
exit	Back to the privilege EXEC
show interface port *port-number* **detail**	Show the interface status detailed information

2. Enable the fault-return function for the optical interface

Command	Description
config	Enter the global configuration mode
interface port *port-number*	Enter the Ethernet physical interface or batch configuration mode.
fault-return {enable|disable}	Enable or shut down the fault-return function

	for the optical interface
exit	Back to the global configuration mode
exit	Back to the privilege EXEC
show interface port *port-number* **detail**	Show the interface status

The fault-return function is only supported by the optical interface.

3. Enable the loopback function

Command	Description
config	Enter the global configuration mode
interface port *port-number*	Enter the Ethernet physical interface mode or batch configuration mode. *port_number* is the physical port number, the range is 1-2.
loopback [**timeout** < 0-30>]	Enable the loopback function for the physical port < 0-30>:duration, the units is minute.
exit	Back to the global configuration mode.
exit	Back to the privilege EXEC
show interface port *port-number* **detail**	view the port status *port_number* is the physical port number, range is 1-2.

If the duration is 0, that means the loopback function will not stop after it starts. User can use the command **no loopback** to cease the loopback function.

Example:

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)#fault-pass enable

Raisecom(config-port)#fault-return enable

Raisecom(config-port)#loopback

Raisecom#show interface port 2 detail

Port 2:

Administer: Disable

Operate: Down

Speed/Duplex: 100M/full

Flowcontrol(R/S): off/off

Fault pass enable: Enable

Fault pass status: Normal

Loopback enable: Enable

Loopback lasting time: 0 (forever)

Optical module type: Unknown

SD status: SD

Fault return enable: Enable

Fault return status: Down

Chapter 7 Layer-3 interface configuration

The layer 3 interface for RC581 is based on VLAN virtual interface configuration. In order to create a layer 3 interface, user can use **ip address** command to configure the IP address for the interface and specify the associated VLAN ID and management port. User can also use **no ip address** to delete a layer 3 interface. VLAN configuration can be referred to chapter 14.

RC581 supports only one virtual layer-3 interface. Each virtual layer-3 interface corresponds to a VLAN ID and multiple management port. After generating the layer-3 interface, this static VLAN will operate as a managing VLAN. If this static VLAN dose not exists, then this layer-3 will not work properly.

The default situation is that all the interfaces are management ports.

The process to create a layer-3 interface and IP address configuration is as follows:

Steps	Command	Description
1	**config**	Enter the global configuration mode
2	**ip address** *ipaddress* [*mask*] *<1-4094>* **[port** {*1-2*}**]**	Configure the layer-3 IP address and the associated static VLAN ID
3	**exit**	Back to the privilege EXEC
4	**show interface ip**	Show the layer-3 interface information

Chapter 8 RMON configuration

RMON introduction

RMON is designated by IETF as a standard without using network Agent and management system for data monitoring, it can be more efficient and more positive to monitor the remote devices, network administer can also track the network, network segment and problem device rapidly; This method reduces the data flow between the administration site and agent, make it possible for user to manage huge scale network conveniently, while making up to the SNMP limitation when facing the extending distributed internet.

User can use the SNMP Agent in the demarcation to monitor and manage all the network status. Four group functions are available currently: statistic group, history group, alarm group and event group.

- Statistic group collects the statistical information at the port, including the received packet number and the size distribution statistics.
- History group is similar with statistic group, but it collects statistic information within a designated period.
- Alarm group monitors a designated management information base (MIB) within a specified period, a high threshold value and a low threshold value are configured to trigger an event when the monitored objects reach the threshold value.
- The event group cooperates with the alarm group, when the alarm triggers an event, the event group is used to record the relevant event information, such as sending trap, writing into LOG and etc.

The RMON relevant command operations include configuration commands and displaying information commands:

- Statistic group configuration
- History statistic group configuration
- Alarm group configuration
- Event group configuration
- Displaying results

RMON configuration

Statistic group configuration:

User can configure the statistic function parameters for the port, if the port status is disabled, user can use command to enable it; if the port status is enabled, user can use the command to edit the relevant parameters. The default situation is that the statistic function of all the ports (including the

layer-3 interfaces and physical ports) is enabled. User can use **no** command to shut down.

Note that when the port's statistic function is shut down, it does not mean that it would not operate the data statistic any more, it means the user will not obtain the statistic data any longer from this port.

Command	Description
config	Enter the global configuration mode
rmon statistics {**ip** | **port** *port_list*} [**owner** *STRING*]	**ip** configure the statistic function for the layer-3 interface; **port** *port_list* configure the statistic function for the physical port, range is 1-2; **owner** *STRING* configure the owner's name for this statistic group, the default situation is "monitorEtherStats"
exit	Back to the privilege user mode
show rmon statistics	Show the information obtained from the statistic group

In order to shut down the statistic group, user can use **no rmon statistics** {**ip** | **port** *port_list*}.

Example:

Enable the statistic group function for port 1-2, the ower's name is raisecom.

Raisecom#config

Raisecom(config)#rmon statistics port 1-2 owner raisecom

Raisecom(config)#exit

Raisecom#show rmon statistics port

Example:

Enable the statistic group function for layer-2 interface, the ower's name is config.

Raisecom#config

Raisecom(config)# rmon statistics ip owner config

Raisecom(config)#exit

Raisecom#show rmon statistics ip

History group configuration:

Configure the history statistic function parameters for the port, if the history statistic function is disabled for this interface, user can use command to enable it; otherwise, user can edit the relevant parameters by using this command. The default situation is that the history statistic function for all the ports (including the layer-3 interfaces and physical ports) is enabled; use can also use **no** command to shut down this function. When the port's history group statistic function is shut down, no data will be collected any more, and the previous collected history data will be cleared up.

Command	Description
config	Enter the global configuration mode
rmon history {**ip** | **port** *port_list*} [**shortinterval** *short-time*] [**longinterval** *long-time*] [**buckets** *queuesize*] [**owner** *STRING*]	**Ip** configure the statistic function for the layer-3 interfaces;; **port** *port_list* configure the statistic function for the physical port, range is 1-2; **shortinterval** *short-time* the short intervals for collecting history statistic at the port, range is 1-600 seconds, the default value is 30 seconds. **longinterval** *long-time* the long intervals for collecting history statistic at the port, range is 600-3600 seconds, the default value is 1800 seconds. **buckets** *queuesize* save the port history data's circulation queue size, range is 10-1000, the default value is 10. **owner** *STRING* configure the owner's name for this statistic group, the default value is "monitorHistory".
exit	back to the privilege EXEC
show rmon history	Show the information obtained from the history statistic group

In order to shut down the history group, user can use the command **no rmon history** {**ip** | **port** *port_list*}

Example:

Configure the history group function for the physical port 1-2, the ower's name is raisecom.

Raisecom#config

Raisecom(config)#rmon history port 1-2 owner raisecom

Raisecom(config)#exit

Raisecom#show rmon history port

Example:

Configure the history group function for the layer-3 interface

Raisecom#config

Raisecom(config)# rmon history ip

Raisecom(config)#exit

Raisecom#show rmon history ip

Alarm group configuration:

User can monitor a MIB variable according to the configuration; user can also delete an alarm by using the relevant **no** command.

The monitored MIB variable should actually exist, and also should be the INTEGRE type following the ASN.1 grammar, such as the type of INTEGER, Counter, Gauge, Time Ticks and etc. if the variable does not exist or the type is not correct while configuration, failure is returned; If the variable can not be collected any more in the alarms that already been configured successfully, this alarm will be shut down accordingly, user must reconfigure to monitor the variable.

If there is no index number for the triggered event, the default value is 0, which means it will not be triggered, because 0 is not an effective event index number. If the event index number is not 0, and the associated event is not configured in the event group, when the monitored variable overflows, no event will be triggered successfully until this event is created.

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**rmon alarm** *Number MIBVAR* [**interval** *time*] {**delta** | **absolute**} **rising-threshold** *value [event-number]* **falling-threshold** *value [event-number]* **owner** *string*	● *Number* Alarm index number, range is <1-512〉; ● *MIBVAR specify the MIB object that will be monitored.* ● *time* unit is second, monitor the period of MIB object.; ● **delta** specify the two times sampling difference of MIB variables. ● **absolute** directly sampling MIB variable ● **rising-threshold** *value* upper bound ● *event-number the event number of which get to the upper bound.* ● **falling-threshold** *value* lower bound. ● *event-number the event number of which get to the lower bound.* ● **owner** *string* specify the owner of Alarm.
3	**exit**	Exit the global configuration mode.
4	**show alarm** *number*	Show the configuration results

If user wants to delete the alarm, can use the command **no alarm** *number*.

Example:

Configure an alarm, monitor MIB variable 1.3.6.1.2.1.2.2.1.20.1, every 20 seconds for each time, check the rise or down of this variable. If the value raises 15, the alarm will be triggered; the name of the owner is system.

Raisecom#config

Raisecom(config)#**rmon alarm 10** 1.3.6.1.2.1.2.2.1.20.1 **intterval 20 delta rising-threshold 15 1 falling-threshold 0 owner** system

Raisecom(config)#exit

Raisecom#show rmon alarm 10

Config the event group

Set the relevant configuration parameters for a particular event; use **no** command to delete an event.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rmon event** *number* [**log**] [**trap**] [**description** *string*] [**owner** *string*]	● *number index number* ● **log** whether write the log information and send syslog ● **trap** whether to send trap ● **description** *string*:*describe string* ● **owner** *string* the owner of the event
3	**exit**	Exit the global configuration mode
4	**show event** *number*	Show configuration results.

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

Example:

Create the event with an index number 1, the group number of the trap is eventtrap, description string is High-ifOutErrors, owner is system.

Raisecom#config

Raisecom(config)#**rmon event** 1 **trap** eventtrap **description** High-ifOutErrors **owner** system

Raisecom(config)#exit

Raisecom#show rmon event 1

Set back to default status:

Set all the function of RMON group to default status, which is the status when the demarcation startups.

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**clear rmon**	Return back to the default status
3	**exit**	Exit the global configuration mode

Show RMON configuration information and the results

show rmon	Show all four groups information of RMON.
show rmon alarms	Show alarm information, including alarm number, name, threshold value, sampling period and sampling value.
show rmon events	Show event information, including event number, name, description, log/trap etc.
show rmon history	Show port information of history group that are opened already.
show rmon statistics	Show the port information of statistics functions that are opened already.

Chapter 9 ARP management

ARP address table introduction

In the procedure of IP packet transmission, software of the demarcation needs to search its physical address based on the IP address of the destination host.

The mapping relationship between IP address and MAC address is saved in the ARP address mapping table in the demarcation.

The ARP mapping table includes two type terms:

- ✧ Dynamic term: use ARP protocol to study MAC address. If it is not used, it will age.
- ✧ Static term: manually added by the user, it will not age.

ARP (address resolution protocol) is a main resolution for the map between IP address and Ethernet MAC address.

ARP modules are necessary for the inter-transmission among computer host network layers in LAN.

If host A wants to send IP message to host B, it will use host B's IP address to search the relevant physical address in its own mapping table. If the physical address is found, the IP message will be transmitted; If it is not found, host A will send ARP request to host B so that the mapping between host B's IP address and MAC address will be added.

Normally, when host A sends packets to host B, host B will sends packets to host a after a while, this means host B may send request to host A for packeting. In order to reduce the transmitted data, host A would keep its own mapping between IP address and MAC address in the ARP request packet. Therefore, when host B received the packet request from host A, it will keep the mapping information in its own mapping table, which will then make it more convenient for host B to send packets to host A.

In some special situation, user can use static MAC address configuration command to operate ARP address mapping table.

ARP configuration

Add static ARP address

Static ARP address term has the following features:

Static ARP address must be added manually, and also must be deleted manually, it will not age.

Below is the configuration command for adding static mapping terms of ARP address mapping table.

Command	Description
arp *ip-address mac-address*	Add a static term to ARP address mapping table.

arp add *ip-address mac-address* is used to add a ARP static mapping term. *Ip-address* demonstrates ip address; mac-address demonstrates IP address associated Ethernet MAC address. The format of MAC address is HHHH.HHHH.HHHH. For example: 0050.8d4b.fd1e.

Delete ARP address mapping term:

Command	Description
no arp *ip-address*	Delete a term in the ARP address-mapping table.

no arp add *ip-address* is used to delete a mapping from ARP address mapping table, including static term and dynamic term.

ARP dynamic address mapping timeout terms configuration

Command	Description
arp aging-time *sec*	Configure the existing time of ARP dynamic table.

This command is used to configure the timeout of ARP dynamic term, if the time value exceeds the timeout, the ARP dynamic term will be deleted automatically. The range of timeout is 0-2147483, if timeout is set as 0, ARP dynamic table will not age.

Clear ARP address mapping table

Command	Description
clear arp	Clear all the terms in ARP address mapping table.

Use *clear arp* command to delete all the terms in MAC address table

Show ARP address mapping table

Command	Description
show arp	Show all the terms in ARP address mapping table.

User can use this command to view all the terms in the ARP address mapping table. The table contents include the IP address, MAC address and term types for each term.

Chapter 10 SNMP configuration

SNMP protocol instruction

Simple Network Management Protocol (SNMP for short) is the most comparatively used protocol in computer networks currently. It is also a standard protocol for managing the internet.

SNMP consists of two parts: agents and network-management systems (NMS). *NMS* is the station running the client program which executes applications that monitor and control the managed devices, such as the current frequently used IBM NetView and Sun NetManager; *agent* is a network-management software module that resides in the managed device. It has the running information of local device that exits in the form of MIB (management information base).

When SNMP agent receives the request packets like Get-Request, Get-Next-Request, Get-Bulk-Request or Set-Request packet (all of them are about MIB variables) from NMS, agent will read or write MIB variables that are requested by NMS and then generates operational response packets based on these requests.

On the other hand, when SNMP Agent receive device status, such as getting cold or getting hot , it will generate a Trap packet and send it to NMS to report these events initiatively.

RC581 SNMP Agent supports SNMPv1,SNMPv2 and SNMPv3.

SNMP configuration

SNMP management has two parts: one part is access which is the response from SNMP agent to NMS request packet; the second part is TRAP. All of these two parts are based on particular use or group. This chapter introduce SNMP configuration:

- ✧ SNMP user configuration
- ✧ Access priority setting
- ✧ TRAP configuration

SNMP user configuration

SNMPv3 uses user-based security model. No matter NMS sends request packets toSNMP Agent, or SNMP Agent sends Trap packets to NMS, the communication between NMS and SNMP Agent are based on a particular user. SNMP NMS and agent maintain a local SNMP user table, this user table records all the names, user associated engine IDs, and other information like whether if the password needs to be authenticated, key for that and etc. No matter which end gets request messages from other end, the receiving end will search the user table and the encryption information, and then

resolve it from the content of message and give a proper response. The configuration of SNMP user is that to create an *authpassword* using command line, and then add a user in the demarcation's local SNMP user table.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server user** *username* [**remote** *engineid*] [**authentication**{**md5** | **sha**} *authpassword*]	Use password format to add a SNMP user.
3	**exit**	Back to privileged EXEC mode
4	**show snmp user**	Show configuration information

Except the *username*, all the other are optional: ***engineid*** is the user associated SNMP engine ID, default is local engine ID; **md5** | **sha** is option of authentication algorithm. If without the input of [**authentication**{**md5** | **sha**} *authpassword*], do not authenticate as default; authpassword is authentication password.

Example 1:

Add a user guestuser 1, local engine ID, and use md5 authentication algorithm, euthentication password is *raisecom*:

Raisecom(config)#**snmp-server user** *guestuser1* **authentication md5** *raisecom*

Example 2:

Add a user *guestuser2*, local engine ID, do not authenticate.

Raisecom(config)#**snmp-server user** *guestuser2*

Example 3:

Delete user *guestuser2*,local engine ID:

Raisecom(config)#**no snmp-server user** *guestuser2*

Access privilege configuration

SNMP protocol has several access control model.

1. Access control based on group

In order to protect itself and MIB from the unauthorized access, SNMP uses the conceptions of community. The management station in any particular community should use the community's name for all the Get and Set operations of agent, otherwise, the requests will not be responded. That is to

say, SNMPv1 and SNMPv2 take community name as the authorization solutions; the SNMP packets that do not match the authorized community name will be discarded.

Actually, community uses various strings to mark different SNMP communities. Different communities can have read-only or read-write priority. The community with read-only priority can only search the device's information; however the community with read-write priority can not only search the device information but can also configures the device.

The demarcation uses following commands to set the SNMP community name:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server community** *community-name* [**view** *view-name*] { **ro** | **rw** }	configure the group name and access priority
3	**exit**	Back to privileged EXEC mode
4	**show snmp community**	Show configuration information

Community-name is the community name, **view-name** is the name of view, **ro** demonstrates that the network management station which the community use can be used to look up the MIB variable in designated view; **rw** demonstrates that the network management station which the community use can look up the MIB variable in designated view of the demarcation, and also has the priority to configure the writeable MIB variable in designated view.

Example 1:

Raisecom(config)#**snmp-server community** raisecom **rw**

This command is used to define the community name as Raisecom. This command does not specify the view, so this community corresponds to the default view internet. When this community is configured, the network management station that uses this community can search all the MIB variables corresponding to the internet view, and also has the priority to configure the writeable MIB variable in the view.

Example 2:

Raisecom(config)#**snmp-server view** mib2 1.3.6.1.2.1 **included**

Raisecom(config)#**snmp-server community** guest **view** mib2 **ro**

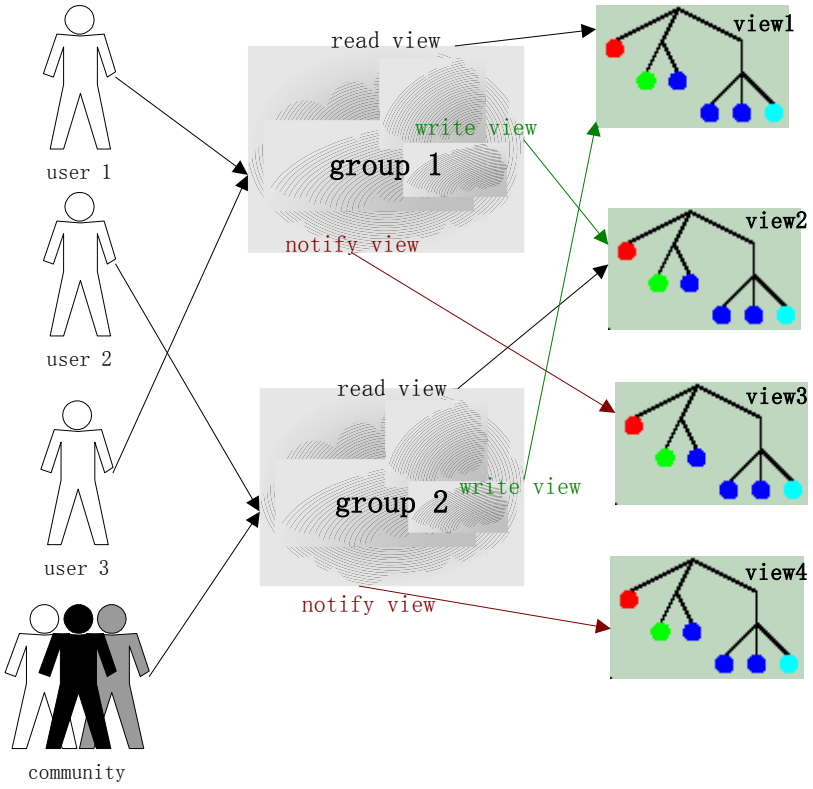
The first command defines view mib2, and this view includes the MIB tree under note 1.3.6.1.2.1

The second command defines group guest, and network management system that uses group name guest can search the MIB variable of mib2 view in the demarcation.

2. Access control based on the user

SNMPV3 uses usm (user-based security model). Usm proposes the conception of access group:

One or more users corresponds to an access group, each access group set corresponding read, write and notification view, the user in the access group has corresponding privilege in the view. The access group that has the user who sends requests like Get and Set should has the corresponding privilege; otherwise, the request will not be responded.



SNMPV3 access control model

From the figure above, we can see that if NMS want to access the demarcation, we should not only configure the user, but should also make sure which user belongs to which access group, the view privilege that the access group owns, and each view. The configuration procedure (including the user configuration) is shown in the following table.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server user** *username* [**remote** *engineid*] [**authentication**{**md5** | **sha**} *authpassword*]	Add a user
3	**snmp-server view** *view-name oid-tree* [*mask*] {**included** | **excluded**}	Define the view and its range of MIB.

4	**snmp-server group** *groupname* **user** *username* { **v1sm	v2csm	usm**}	Make sure the user belongs to which access group.
5	**snmp-server access** *groupname* **[read** *readview***] [write** *writeview***] [notify** *notifyview***] [context** *contextname* **[**{**exact	prefix**}**]]** { **v1sm	v2csm	usm**} { **noauthnopriv	authnopriv** }	Define the access priority of access group
6	**exit**	Back to privileged EXEC mode
7	**show snmp group** **show snmp access** **show snmp view** **show snmp user**	Show configuration information

- View configuration information

view-name denotes the configured name of view ,*oid-tree* denotes OID tree, **included** means that the scale of the view includes all the MIB variables at OID tree, **excluded** means that the scale of the view includes all the MIB variables at OID tree.

mask is the mask of OID subtree, each of its bit corresponds to one term in the subtree. If the bit of the mask is 1, view should be in accordance with the corresponding term in subtree; if bit of the mask is 0, view does not need to match any term. The maximum length of mask is 16 bytes, which means, it supports the subtree with 128 depth. For example: a view OID subtree is 1.3.6.1.2.1, mask is 1.1.1.1.0.1, then actual subtree in this view is 1.3.6.1.x.1 (x can be arbitrary), which is the first term of all the nodes at 1.3.6.1. The default view of the demarcation is Internet, the scale of the view includes all the MIB variables at the tree 1.3.6. All default bits of mask are 1.

- Configuration introduction of access control group.

Groupname is the name of access group; *readview* is the read view, the default setting is internet; *writeview* is the write view, default is null; *notifyview* is the notify view, default setting is null; *contextname* is the name of context or its prefix; **exact|prefix** stands for the matched type of the context: **exact** means the input should be fully matched with the name of context, **prefix** means that the first several letters should be matched with the name of context; v1sm|v2csm|usm is the security model, it stands for SNMPv1 security model, SNMPv2 security model based on the group, and SNMPv3 security model based on the user respectively; **noauthnopriv|authnopriv** is the security level, it stands for no authentication with no encryption, and authentication without encryption respectively. When deleting an access group, the name of accesss group, name of context, security mode and security level should be specified.

If the security model is v1sm or v2csm, security level is noauthnopriv automatically, so the model

doesn't has the option {**noauthnopriv | authnopriv**}, meanwhile, there is not the option for **[context** *contextname* **[{exact | prefix}]].**

Example 1:

Create an access group "guestgroup", security model is usm, security level is authentication without encryption, readable view is mib2, both writable view and notifyview are null as default:

Raisecom(config)#**snmp-server access** *guestgroup* **read** *mib2* **usm authnopriv**

Example 2:

Delete access group guestgroup:

Raisecom(config)#**no snmp-server access** *guestgroup* **usm authnopriv**

- Configuration mapping between user and access group

Groupname is the name of access group;*username* is username;**v1sm | v2csm | usm** is security model.

Example 1:

Map the *guestuser1* who has the security level usm to access group *guestgroup*.

Raisecom(config)#**snmp-server group** *guestgroup* **user** *guestuser1* **usm**

Example 2:

Delete the map from *guestuser 1* with security level usm to access group *guestgroup*.

Raisecom(config)#**no snmp-server group** *guestgroup* **user** *guestuser1* **usm**

TRAP configuration

To configure Trap, user should configure the IP address of target host that receives the Trap, and also need to configure the username of the trap that is sent by SNMPv3, SNMP version, security level (whether need to be authenticated or encrypted) and etc.

The demarcation needs following commands to configure parameters for target host.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server host** *A.B.C.D* version {1|2c} NAME [**udpport** *<1-65535>*] [bridge] [config] [interface] [rmon] [snmp] [ospf]	Configure the target host of SNMPv1/v2 Trap.

	snmp-server host *A.B.C.D* version 3 { noauthnopriv | authnopriv } NAME [**udpport** *<1-65535>*] [bridge] [config] [interface] [rmon] [snmp] [ospf]	Configure SNMPv3 Trap target host
3	**exit**	Back to privilege EXEC mode.
4	**show snmp host**	Show configuration situation

Example 1:

Add a host computer address of host_1, ip address is *172.20.21.1*, user name is raisecom, SNMP version is v3, authentication but no encryption, with trap.

Raisecom(config)#**snmp-server host** *172.20.21.1* version 3 authnopriv raisecom

Example 2:

Delete host computer address host_1

Raisecom(config)#**no snmp-server host** *172.20.21.1*

Other configuration

- Configure the identification and contact information for the network administrators

The identification and contact information for network administrator is a variable of MIB system group; the function is to configure the identification and contact information for network administrator.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server contact** *sysContact*	Set the mark and contact method of network administrators
3	**exit**	Back to privilege EXEC mode
4	**show snmp config**	Show the configuration

Example:

Raisecom(config)#snmp-server contact service@raisecom.com

- Permit or deny sending trap

Trap is mainly used to provide important events to network management station (NMS). The demarcation will send a trap message that is failed to authenticate when trap receives a request with

wrong group name and is set as allowed to send snmp trap.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server enable traps**	Allow the send trap operation by the demarcation
	no snmp-server enable traps	Deny the send trap operation by the demarcation
3	**exit**	Back to privilege EXEC
4	**show snmp config**	Show configuration information

Use snmp-server enable traps command to all trap.

Use **no snmp-server enable traps** command to deny the demarcation to send trap.

- Set the position of the demarcation

The position information of the demarcation "sysLocation" is a variable MIB, which is used to describe the physical location of the demarcation.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server location** *sysLocation*	Set the position of the demarcation
3	**exit**	Back to privilege EXEC mode
4	**show snmp config**	Show configuration information

Example: set the physical position information of the demarcation as HaiTaiEdifice8th.

Raisecom(config)#snmp-server location HaiTaiEdifice8th

Show SNMP configuration information

Command	Description
show snmp community	Show all the community name, the corresponding view name and privilege
show snmp host	Show all the IP address of trap target host
show snmp config	Show the local SNMP engine ID, the identification of network administrator and contact information, the position of the demarcation and TRAP on-off switch.
show snmp view	Show all view names and their scale.
show snmp access	Show all the names of access groups and the related attributes.

show snmp group	Show all the mappings between user and access group.
show snmp user	Show all the users, and all the relevant authentication and encryption protocol information.
show snmp statistics	Show SNMP packet statistics information

Chapter 11 System log configuration

System log introduction

The system information and some debugging information will be sent into log for processing. Based on the configuration of system log, the process is able to decide the destination that the log information will be sent to: log file, console, TELNET, log host.

The general format of system log is:

timestamp module-level- Message content

Example: FEB-22-2005 14:27:33 CONFIG-7-CONFIG:USER " raisecom " Run " logging on "

System log configuration

The configuration for system log includes:

- The enable and disable of system log
- Time stamp configuration of system log.
- The configuration of log rate.
- Log information output configuration
- Display log.

The enable and disable for system log

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging on**	Start system log
3	**exit**	Back to privilege EXEC
4	**show logging**	Display configuration information

Example:

Raisecom#**config**

Configuration mode, one conmmand input per times. End with CTRL-Z.

CONFIG-I:Configured from console ...

Raisecom(config)#**logging on**

set sucessfully!

Raisecom(config)#**exit**

Raisecom#**show logging**

Syslog logging:Enable, 0 messages dropped, messages rate-limited 0 per second

Console logging:Enable, level=informational, 0 Messages logged

Monitor logging:Disable, level=informational, 0 Messages logged

Time-stamp logging messages: date-time

Log host information:

Target Address Level Facility Sent Drop

The time-stamp setting of log information

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging time-stamp { standard | relative-start | null }**	Set time stamp: **standard :standard time format** mmm-dd-yyyy hh-mm-ss,"FEB-22-2005 14:27:33" **relative-start :**demarcation starting time hh-mm-ss,for example"29:40:6"stands for 29 hours 40 minutes 6 seconds **null:there is no time stamp in the log**
3	**exit**	Back to privilege EXEC
4	**show logging**	Show configuration information

Example:

Raisecom(config)#**logging time-stamp relative-start**

set successfully!

Log rate configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging rate <1-65535>**	Set the number of the log that will be sent per second.
3	**exit**	Back to privilege EXEC mode

Log information output configuration

1. Log information sent to console or TELNET

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging {console |monitor} {<0-7> | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings}**	Log information is sent to console or TELENT.
3	**exit**	Back to privilege EXEC
4	**show logging**	Display configuration information

2. Set logging host

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging host A.B.C.D { local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7} { <0-7> | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings }**	Set logging host
3	**exit**	Back to privilege EXEC
4	**show logging**	Show configuration information

The meaning for each term:

local0-local7 device name for logging host

·**<0-7>** the log level

·**alerts** need immediate action (level=1)

·**critical** critical status (level=2)

·**debugging** debugging status (level=7)

·**emergencies** the system is not available (level=0)

·**errors** error condition (level=3)

·**informational** informational events (level=6)

·**notifications** the events in the critical conditions (level=5)

·**warnings** warning events (level=4)

Example:

Raisecom(config)#**logging console warnings**

set console logging information successfully

Raisecom(config)#**logging host 10.168.0.16 local0 warnings**

set log host logging information successfully

Raisecom(config)#**ex**

Raisecom#**show logging**

Syslog logging: enable, 0 messages dropped, messages rate-limited 0 per second

Console logging: enable, level=warning ,18 Messages logged

Monitor logging: disable, level=info ,0 Messages logged

Time-stamp logging messages: enable

Log host Information:

Target Address Level Facility Sent Drop

10.168. 0. 16 warning local0 1 0

3. Open log file

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging file**	Set logging host
3	**exit**	Back to privilege EXEC
4	**show logging file**	Show logging file

Show log configuration

Step	Command	Description

1	**show logging**	Show configuration information
2	**show logging file**	Show the contents of logging file

Chapter 12 System clock

System clock

There are two methods to set the system clock: the first one is to use SNTP protocol to synchronize the system time with that of SNTP host, the SNTP protocol synchronized time is the Greenwich time, system will adjust the local time according to the system time zone; the second one is to configure the time manually, the manually configured time is the local time. System clock configuration includes:

- ✧ Configure SNTP synchronized time
- ✧ Manually configure system time.
- ✧ Set summer time.

SNTP synchronized time

Step	Command	Description
1	**config**	Enter global configuration mode
2	**sntp server** A.B.C.D	Start SNTP services
3	**exit**	Configure SNTP server address
4	**show sntp**	Back to privilege EXEC

Manually configure system time

Step	Command	Description
1	**clock timezone** {+|-} <0-11> <0-59>	Set system time zone: ·+ east hemisphere time zone ·- west hemisphere time zone ·<0-11> time zone offset hours ·<0-59> time zone offset minutes Default setting is Beijing local time, which is east hemisphere time 8 o'clock.
2	**clock set** *<1-24> <0-60> <0-60> <2000-2199> <1-12> <1-31>*	Set system time, they are: hour, minute, second, year, month, day
3	**show clock**	Show configuration information

Example: set the local time zone offset as to offset towards west for 10 hours and 30 minutes. Local time is 2005-3-28 time is 11:14, 20 seconds am.

Raisecom#**clock timezone** – 10 30

set sucessfully!

Raisecom#**clock set** *11 14 20 2005 3 28*

set sucessfully!

Raisecom#**show clock**

Current system time: Mar-28-2005 11:15:05

Timezone offset: -10:30:00

Note: *when configuring the time manually, if the system uses summer time, for example, the summer time is from the second Sunday of each April at2 am to the second Sunday of each September at 2 am, in this time period, clock should move one hour ahead, that means the time offset 60 minutes, then the time between 2 o'clock and 3 o'clock on the second Sunday of each April does not exist. The result from setting time manually in this time period is failed.*

Set summer time

Sun rises early in summer, so the daytime seems very long. In order to save resource and fully utilize the daytime, many countries in the world use the legalized manner to set the time one hour ahead when summer comes, or half an hour or a couple of hours; when winter comes, people need to set the time back. This is called "summer time", a legalized time.

When the summer time is enabled, all time that use SNTP synchronized time will be turned as local summer time. The summer time configuration is as follows:

Step	Command	Description
1	**clock summer-time enable**	The start of summer time, some country does not use summer; can also use this command to close.
2	**clock summer-time recurring {**<1-4>| last**} {** sun | mon | tue | wed | thu | fri | sat **} {**<1-12> | MONTH **}** <0-23> <0-59> **{**<1-4> | last**} {** sun | mon | tue | wed | thu | fri | sat **} {**<1-12> | MONTH **}** <0-23> <0-59> <1-1440>	Set the starting and ending time of summer time. ·**<1-4>** which week of the month to start summer time. ·**last** the summertime begins from the last week of the month. ·***week day*** which day in the weed to start the summertime ·**<1-12>** the starting month ·**MONTH** summer time starting month, input month in English. ·**<0-23>** summer time starting hour ·**<0-59>** summer time starting minute ·**<1-4>** the ending time is which week of the month. ·**last** summertime ends at the last week of the month. ·***week day*** summer time ends at which day of the week. ·**<1-12>** summer time ending month ·**MONTH** summertime ending month, input the month in English. ·**<0-23>** summer time ending hour ·**<0-59>** summer time ending minute ·**<1-1440>** summertime excursion minutes
3	**show clock summer-time recurring**	Display summertime

		configuration

For example, set summer time as: From the second Sunday of each April at 2 am to the second Sunday of the each September at 2 am. In this time period, set the clock one hour ahead.

Raisecom#**clock summer-time enable**

set sucessfully!

Raisecom#**clock summer-time recurring 2 sun 4 2 0 2 sun 9 2 0 60**

set sucessfully!

Raisecom#**show clock summer-time-recurring**

Current system time: Jan-01-2004 08:40:07

Timezone offset: +08:00:00

Summer time recuuring: Enable

Summer time start: week 02 Sunday Apr 02:00

Summer time end: week 02 Sunday Sep 02:00

Summer time Offset: 60 min

Chapter 13 Trouble shooting command

Trouble shooting

When troubles occur somewhere in the system, user can use trouble shooting commands to solve the problem. The content includes the following commands:

- ✧ Memory usage information
- ✧ Port driving pool usage information
- ✧ Process and stack status
- ✧ Port UP/DOWN statistical information
- ✧ Information collection for trouble shooting

Memory usage information

Step	Command	Description
1	**show memory**	Check memory usage information

Example:

```
Raisecom#show memory
FREE LIST:
  num         addr          size
  --- ---------- ----------
    1   0x27db148            9120
    2   0x3483100           16904
    3   0x27ddd50             160
    4    0x916220        32017512
    5   0x3e00000         2077144
SUMMARY:
 status      bytes       blocks      avg block    max block
 ------ --------- -------- ---------- ----------
current
free    34120840            5        6824168     32017512
alloc   23460160        62554            375            -
cumulative
alloc   23591248        64754            364            -
```

Port driving pool usage information

Step	Command	Description
1	**show buffer [port** <1-2>**]**	Check the port driving port usage information

Example

Raisecom(config)# **show buffers port 2**

Port 2

Total mBlks: 500 Free mBlks: 500 DATA: 0

HEADER: 0 SOCKET: 0 PCB: 0

RTABLE: 0 HTABLE: 0 ATABLE: 0

SONAME: 0 ZOMBIE: 0 SOOPTS: 0

FTABLE: 0 RIGHTS: 0 IFADDR: 0

CONTROL: 0 OOBDATA: 0 IPMOPTS: 0

IPMADDR: 0 IFMADDR: 0 MRTABLE: 0

Process and stack status

Step	Command	Description
1	**show processes**	Check the process and stack status

Example:

Raisecom#**show processes**

Task Information:

Total time elapse is 0(ticks) 0 m 0 ms

Task STATUS: RDY- ready; SUP- suspended; POS-pend on sem;

TSD- task delay;DTS-dead task

taskid task Name stk(B) prio status Ecode Rtime(sws /ticks%)

3bfe9e0 tExcTask 7744 0 POS 3d0001 (0 / 0.0%)

3bfc058 tLogTask 4760 0 POS 0 (0 / 0.0%)

348bd78 tWdbTask 7656 3 POS 0 (0 / 0.0%)

2c71c38 tED 8024 20 POS 3d0002 (0 / 0.0%)

6c9a38 tStpTm 2796 30 TSD 0 (0 / 0.0%)

2a055c0 tSch 8056 30 TSD 0 (0 / 0.0%)

29e5188 tRmonTm 1896 30 TSD 0 (0 / 0.0%)

2a4aa00 tStpRecv 4832 35 POS 0 (0 / 0.0%)

34e22d0 tNetTask 9792 50 POS 3d (4 / 0.0%)

2e7d9d8 tDPC 15928 50 POS 0 (0 / 0.0%)

2e2a988 tARL.0 15928 50 POS 0 (0 / 0.0%)

2da6710 tLINK.0 15912 50 3d0004 (3 / 0.0%)

```
2db3bd0     tCOUNTER.0     15896     50            3d0004   (      3 /   0.0%)
27d9500      tScrnBg_0     13888     50       RDY  30067   (     28 /   0.0%)
27d1c78      tScrnBg_1     16192     50       POS      0   (      0 /   0.0%)
27ca4e0      tScrnBg_2     16192     50       POS      0   (      0 /   0.0%)
27c2d48      tScrnBg_3     16192     50       POS      0   (      0 /   0.0%)
27bb5b0      tScrnBg_4     16192     50       POS      0   (      0 /   0.0%)
27b3e18      tScrnBg_5     16192     50       POS      0   (      0 /   0.0%)
2a6ba58       tRndpRecv     7944     51       POS      0   (      0 /   0.0%)
2a632d0       tRtdpRecv     7912     51       POS      0   (      1 /   0.0%)
2907680        tCcomTm      840     55       TSD      0   (      2 /   0.0%)
348df68         tSntpS     4344     56       POS      0   (      0 /   0.0%)
2a7c008         tDhcpS    19464     56                0   (      0 /   0.0%)
2a6f480         tLoopD     3944     60       TSD      0   (     10 /   0.0%)
2906408          tCcom     3848     60       POS      0   (      2 /   0.0%)
2a1e7f0          tRmon    32632     75       TSD 81000c   (     15 /   0.0%)
2a11358      tPortStats     3632     75       TSD      0   (      6 /   0.0%)
2a0aeb8       tLinkTrap     8040     75       TSD      0   (      2 /   0.0%)
2a06868       tColdTrap     3944     75       TSD      0   (      1 /   0.0%)
2a23a38          tIgmpTm     2848    100       TSD      0   (      0 /   0.0%)
2a22c20       tIgmpSnoop     3816    100       POS      0   (      0 /   0.0%)
2a21a08            tSnmp    11816    100       POS      0   (      0 /   0.0%)
2a16590          tIpBind     3904    100       TSD 81000c   (      1 /   0.0%)
2a08b78          tEndStat     7832    100            3d0004   (      0 /   0.0%)
29e2558        tRmonAlrm     7976    100       POS      0   (      2 /   0.0%)
27aea90 tTelnetdOut0       3336    100       POS      0   (      0 /   0.0%)
27ad878    tTelnetdIn0     3384    100       POS      0   (      0 /   0.0%)
27ac610 tTelnetdOut1       3336    100       POS      0   (      0 /   0.0%)
27ab3f8    tTelnetdIn1     3384    100       POS      0   (      0 /   0.0%)
27aa190 tTelnetdOut2       3336    100       POS      0   (      0 /   0.0%)
27a8f78    tTelnetdIn2     3384    100       POS      0   (      0 /   0.0%)
27a7d10 tTelnetdOut3       3336    100       POS      0   (      0 /   0.0%)
27a6af8    tTelnetdIn3     3384    100       POS      0   (      0 /   0.0%)
27a5890 tTelnetdOut4       3336    100       POS      0   (      0 /   0.0%)
27a4678    tTelnetdIn4     3384    100       POS      0   (      0 /   0.0%)
```

```
27a3460      tTelnetd     3640   100     POS          0   (      0 /   0.0%)
3489320      tSyslog      7968   105     POS          0   (      0 /   0.0%)
2daaac8      tx_cb       15912   110     POS          0   (      0 /   0.0%)
348f558      tSntpCLsn    4760   150     TSD          0   (      1 /   0.0%)
2a52d20      tRelay       3880   151     POS          0   (      0 /   0.0%)
2da0958      rx0         15888   200          3d0004   (     29 /   0.0%)
2cc1c98      tArlAging    1896   200     TSD          0   (      0 /   0.0%)
2b38248      tSnmpTm      3856   200     POS          0   (      0 /   0.0%)
2c25d60      tRosInit     5912   250     POS    81000e   (      0 /   0.0%)
27af260      tIdle         568   251     RDY          0   (    281 /   0.0%)
```

The schedule-list above includes: task ID, task name, the size of the stack, priority, status, and error code, degree of execution and CPU occupation rate.

UP/DOWN statistical information

Step	Command	Description
1	**show diags link-flap**	Check the port UP/DOWN statistic information

Example:

```
Raisecom#show diags l
Port       Total          Last Min
-----------------------------
19         2              0
21         2              2
```

The example above means that from the time when the device startups: port 19 up/down for twice, no up/down happened within this minute; port 21 up/down for twice, and up/down twice happened twice with this minute.

Information gathering for trouble shooting

Step	Command	Description
1	**show tech-support**	Check the information collection for trouble shooting.

This command displays the information collection for trouble shooting, includes:

- Version information(show version)
- Current configuration information(show running-config)
- Current CPU occupation rate(show cpu-utilization)
- Memory usage information(show memory)
- Port driving pool usage information(show buffer)
- Process information(show processes)
- Flash file(dir)
- Current system time(show clock)
- Port status information(show interface port)

- Port statistics information(show interface port statistics)
- Port Up/Down statistics information(show diags link-flap)
- SNMP statistics information(show snmp statistics)
- Spanning tree information(show spanning-tree)
- Static VLAN information(show vlan static)
- ARP information(show arp)
- trunk information(show trunk)
- TCP connection status.

Chapter 14 VLAN configuration

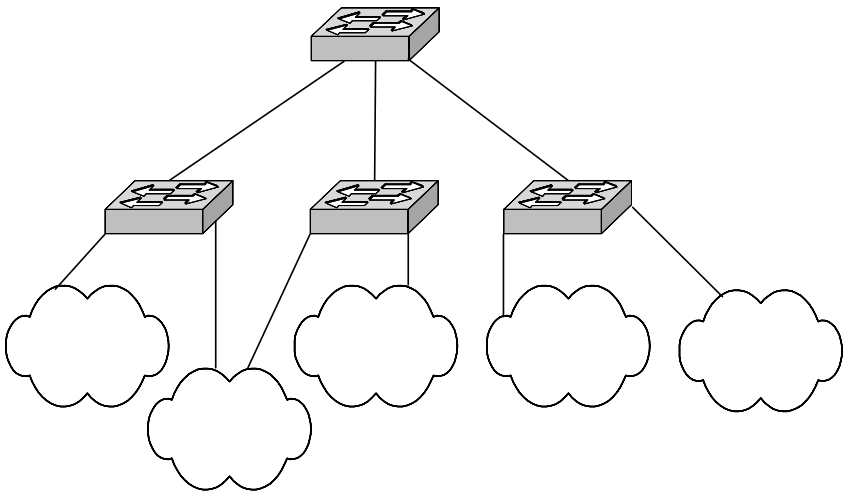
This chapter introduces how to configure VLAN on the demarcation, including the following contents:

- ✧ VLAN summary:
- ✧ VLAN configuration list:
- ✧ Monitor and maintenance

VLAN summary

VLAN is Virtual Local Area Networks. From the function point of view, VLAN and LAN have the same characteristics. But there is no physical limitation for VLAN members. For example, the users connected to the same demarcation can belong to different VLAN, users connected to different demarcations can also belong to the same VLAN. The broadcast area and multicast area relates to the relevant VLAN members. Broadcast, multicast and unicast of the VLAN will not be sent to other VLANs. Different VLANs can communicate with each other by using Layer-3 switch or routers. These above characteristics make it convenient for user to manage the network. User can distribute VLANs according to the different members' functions so that the network bandwidth utility and security can improve a lot. Below is a typical VLAN topology figure:

VLAN topology:



In the actual network application, vlan always corresponds to an IP subnet, as the figure above, VLAN 1 is corresponding to 10.0.0.0/24 network, VLAN 2 is corresponding to 20.0.0.0/24 network. Though they are isolated at layer two, but at layer three, they can communicate with each other.

Q-in-Q summary

In the structure of IP data network, demarcation is always used as access device. When using LAN as access, an important problem that should be concerned is the isolation among different users.

Many carriers now required the end to end security; they hope to allocate VLAN for each user. However, the faced problem is that the default VLAN resource is only 4096. By using the Q-in-Qb technology, user can break through the VLAN number limitation for the construction ability of

metropolitan Ethernet, that means the construction ability of VLAN layer-2 is expanded, then layer-2 VPN in metropolitan area network can also be achieved, which can provide appropriate service to the metropolitan Ethernet.

The theory of Q-in-Q is that: a private Tag is carried on the data that transmitted in private network, which is defined as CVLAN Tag; the data will then be added with another public network VLAN tag when they go into the backbone of service provider, which is defined as SPVLAN Tag (or Outer tag); when the data arrive at the destination, the SPVALN Tag will be peeled off, offering a simple layer-2 VPN tunnel for the user.

SPVLAN Tag is embedded after the Ethernet source MAC address and destination MAC address. It also includes a 12-bit SPVLAN ID, support 4096 VLAN. SPVLAN CoS region includes 3 bits, support 8 level precedence. In the network based on Q-in-Q, carriers allocate a SPVLAN ID for each VLAN, and then map users' CVLAN ID samples onto these SPVLAN ID. In this way, user's C-VLAN ID can be protected.

Raisecom's Q-in-Q technique provides the following advantages when setting solutions for small area metropolitan network and enterprise network.

- provides 4096×4096 VLAN ID, be able to solve the limitation problem of public VLAN ID resource;
- User can set there own private VLAN ID that will not conflict with publish VLAN ID;
- Provides a comparatively simple layer-2 VPN solution scheme;
- Provides user with higher independency, user do not need to change their original configurations when service provider updates the network.

VLAN configuration list

VLAN configuration includes following contents:

- Create and delete VLAN;
- VLAN name configuration;
- VLAN active attribute configuration;
- VLAN mode of the port and relevant attributes;
- Monitor and maintenance.

Demarcation-mode configuration

When user needs to configure the switching mode for the device, they should follow the steps below:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**switch-mode {transparent | vlan}**	Configure the switch mode for the device
3	**exit**	Back to the privilege EXEC mode
4	**show vlan**	Show VLAN configuration status

Under the situation of transparent mode, configuration of static VLAN and port VLAN are not actually effective (data switching will not be affected). Under the situation of transparent, the system will keep the records but does not perform the command configuration below:

- vlan
- pvid
- vlan accept-frame
- vlan double-tag
- vlan egress default
- vlan ingress-filtering

When the VLAN mode is turned to forwarding mode, the configuration above will be performed by system.

Under the VLAN forwarding mode, the configuration above will take effect directly.

Create and delete VLAN

When user wants to create new VLAN, they need to follow the steps below:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**vlan** *<1-4094>* **port** {*1-2*} **[untag port** {*1-2*}**]** [*0-7*]	Create VLAN, and enter its configuration mode
3	**exit**	Back to privilege EXEC mode
4	**show vlan**	Show VLAN configuration status

When user needs to delete a VLAN, they need to follow the steps below:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**no vlan** (*all*|{*1-4094*})	Delete VLAN
3	**exit**	Back to global configuration mode
4	**show vlan**	Shw VLAN configuration status

The example below show how to create VLAN 3 and use *show* command to view the configuration status:

Raisecom#(config)#**vlan** *3* **port** *1,2*

Raisecom#(config)#**exit**

Raisecom#**show vlan**

Demarcation mode: Vlan

Core tag type: 0x9100

VLAN Ports Untag Port Priority

---

3 1,2 n/a -----

Port VLAN relevant attributes configuration

1. PVID with the relevant configuration

Under the default situation, PVID is 1, the override function is closed. When user needs to revise PVID or (and) enable override function, they need to follow the steps below:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**interface port** *port-number*	Enter the Ethernet physical interface configuration mode
3	**pvid** <1-4094> [**override**]	Configure PVID or(and) startup override function
4	**exit**	Back to privilege EXEC
5	**exit**	Back to privilege EXEC
6	**show interface port** [{1-2}] **switchport**	Show port VLAN configuration status

User can execute *no pvid override* to shut down override without revising PVID. User can also use *no pvid* to set it back to defaults situation.

2. Configure the accept data

The defaults situation is that, all the datagram is permit for receiving. When user needs to revise the accepted data type, the following steps should be followed:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**interface port** *port-number*	Enter the Ethernet physical interface configuration mode.
3	**vlan accept-frame {***tag*|*untag* **}**	Configure the accepted datagram with tag or without tag
4	**exit**	Back to privilege EXEC
5	**exit**	Back to privilege EXEC
6	**show interface port** [{1-2}] **switchport**	Show port VLAN configuration status

User can execute the command *no vlan accept-frame* to set it back to default configuration.

3. Ingress-filter configuration

The default situation is that, the ingress datagram will not be discarded. If user need to filter the ingress datagram, can follow the steps below:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**interface port** *port-number*	Enter Ethernet physical interface configuration mode
3	**vlan ingress-filtering {***unknown-vlan* | *not-member***}**	Configure the ingress discarding VLAN not exist or not-member of VLAN datagram
4	**exit**	Back to privilege EXEC
5	**exit**	Back to privilege EXEC
6	**show interface port** [{1-2}] **switchport**	Show port VLAN configuration status

User can execute the command to set it back to default configuration.

4. Egress-filter configuration

The default situation is that, the egress datagram without VLAN will not be revised. If user needs revise it, can follow the steps below:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**interface port** *port-number*	Enter the Ethernet physical interface configuration mode
3	**vlan egress default {***tag* | *untag***}**	Configure add TAG or not to the egress port without VLAN
4	**exit**	Back to privilege EXEC
5	**exit**	Back to privilege EXEC
6	**show interface port** [{1-2}] **switchport**	Show the port VLAN configuration status

User can execute the command *vlan egress default unmodify* to set back to default configuration.

Q-in-Q enable and disable

The default situation is that Q-in-Q function is disabled. If user wants to startup Q-in-Q function, they need to follow the steps below:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**interface port** *port-number*	Enter the Ethernet physical interface configuration mode
3	**vlan double-tag**	Enable Q-in-Q function
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege EXEC
6	**show vlan**	Show VLAN configuration status

If user wants to disable the Q-in-Q function, they need to follow the steps below:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**interface port** *port-number*	Enter the Ethernet physical interface configuration mode
3	**no vlan double-tag**	Disable Q-in-Q function
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege EXEC
6	**show vlan**	Show VLAN configuration status

The example below shows how to enable the Q-in-Q function, and use *show* command to view the configuration status:

Raisecom#**config**

Raisecom(config)#**interface port** 2

Raisecom(config-port)# **vlan double-tag**

Raisecom#**show interface port** 2 **switchport**

Port 2:

PVID: 1

PVID override: Disabled

Double tag: Enabled

Vlan accept-frame: All

Vlan ingress filtering: None

Egress default : Unmodify

Outer Tag TPID value configuration

The default situation is that: the outer Tag TPID value is 0x9100, if user wants to revise the value, the steps below should be followed:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**mls double-tagging tpid HHHH**	Configure outer Tag TPID value as **HHHH** (HHHH is a four bits hexadecimal)
3	**exit**	Back to privilege EXEC

4	**show vlan**	Show VLAN configuration status

If user wants to recover the outer Tag TPID to default value, the steps below shouldbe followed:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**no mls double-tagging tpid**	Recover the outer Tag TPID vaule to default value(0x9100)
3	**exit**	Back to global configuration mode
4	**show vlan**	Show VLAN configuration mode

The example below shows how to configure the outer Tag TPID value as 0x8100 and use *show* command to view the configuration status:

Raisecom#(config)# mls double-tagging tpid 8100

Raisecom#(config)#exit

Raisecom#show vlan

Demarcation mode: Vlan

Core tag type: 0x8100

VLAN Ports Untag Port Priority

---

1 1,2 n/a --

3 1,2 1,2 ---

Monitor and maintenance

In order to perform monitor and maintenance, user can use the two *show* commands to view the VLAN configuration:

Command	Description
show vlan [{*1-4094*}]	Show VLAN configuration information
show interface port [{*1-2*}] **swithport**	Show physical interface VLAN configuration

User can use *show vlan* to view the created VLAN based on CLI or SNMP, including those VLANs managed by layer-3 interface:

Raisecom#show vlan

Demarcation mode: Vlan

Core tag type: 0x8100

VLAN Ports Untag Port Priority

---

1 1,2 n/a --

3 1,2 1,2 --

User can also use show interface port [{*1-2*}] swithport to view the port VLAN attributes based on CLI or SNMP configuration:

Raisecom#show interface port demarcationport

Port 1:

PVID: 1

PVID override: Disabled

Double tag: Enabled

Vlan accept-frame: All

Vlan ingress filtering: None

Egress default : Unmodify

Port 2:

PVID: 1

PVID override: Disabled

Double tag: Disabled

Vlan accept-frame: All

Vlan ingress filtering: None

Egress default : Unmodify

Chapter 15 ACL and network security configuration

ACL introduction

In order to filter the data packet, network device needs to configure a series of matching rules to identify the objects that needed to be filtered out. When the given objects are identified, network device can permit or deny the data packets based on previously defined policies. ACL (Access Control List, ACL) is used to realize those functions. ACL can be applied to Layer-3 management interface.

Based on a series of matching rules, ACL can classify the data packet. The conditions can be source address, destination address, and port number of the data packet. It is comprise of a series of judgment sentence. When an ACL is active, the demarcation will check each data packet based on the judgment conditions. Demarcation will then decide whether to transmit or discard the data packet.

The access classification configuration can be set as permit or deny. If the access type is deny, all the data packet that match this condition will be discarded, all the others will be transmitted; if the access type is set to permit, the data packet that match the given condition will be transmitted, all the others will be discarded.

Configure IP access control list

The demarcation can define 400 IP access control lists at the most(range of the number ID is 0～199). It will define the classification rules and process the data packets according to the source IP, destination IP, used TCP or UDP port number and etc., which are in the datagram's IP header. The structure of IP header can be referred to RFC791 and relevant documents.

Command	Description
config	Enter the global configuration mode
ip-access-list *list-number* {**deny** | **permit**} *protocol* {*source-address mask* | **any**} [*source-protocol-port*] {*destination-address mask* | **any**} [*destination-protocol-port*]	**ip-access-list** configure the IP address access control list *list-number* IP index number for the address control list, range is 0-199 **deny**|**permit** means deny|permit access *protocol* associated protocol type *source-address mask* | **any** is the source IP address and its mask, the format is *A.B.C.D* dotted decimal; if **any** is any, that denotes arbitrary address. *source-protocol-port* is TCP/UDP source port *destination -address mask* | **any** is destination address with its mask, the format is *A.B.C.D* dotted decimal; if **any** is any, that denotes arbitrary address. *destination -protocol-port* is the TCP/UDP destination port
exit	Back into the privilege EXEC
show ip-access-list *list-number*	Show IP access control list relevant information *list-number* is the index number for the address control list, range is 0-199.

User can use the command **no ip-access-list** *list-number* to delete IP access control list, *list-number*

is the list index number to be deleted.

Example:

The source IP address is 192.168.1.0 network section, destination IP address is in any network section, protocol type is IP, access type is deny.

Source IP address is 10.168.1.19, mask is 255.255.255.255, source protocol port is 80, destination address is any, any port, protocol type is TCP; access type is deny.

The source IP address is 10.168.1.19, mask is 255.255.255.255, destination address is 10.168.0.0 network section, protocol type is TCP, and access type is permit.

raisecom#config

raisecom(config)#ip-access-list 0 deny ip 192.168.1.0 255.255.255.0 any

raisecom(config)#ip-access-list 1 deny tcp 10.168.1.19 255.255.255.255 80 any

raisecom(config)#ip-access-list 2 permit tcp 10.168.1.19 255.255.255.255 80 10.168.0.0 255.255.0.0 80

raisecom(config)#exit

raisecom#show ip-access-list

Src Ip: Source Ip Address

Dest Ip: Destination Ip Address

List	Access	Protocol	Ref.	Src Ip:Port	Dest Ip:Port
0	deny	IP	0	192.168.1.0:0	0.0.0.0:0
1	deny	TCP	0	10.168.1.19:80	0.0.0.0:0
2	permit	TCP	0	10.168.1.19:80	10.168.0.0:80

Use ACL on layer-3 interface

The step for using ACL on layer-3 interface is as follows:

- Define access control list

As in paragraph 15.2

- configure using ACL

The ACL on the third layer interface are made up of several “permit|deny” commands. For these commands, the ranges of designated data packet are different. There are problems in the matching sequence when matching a data packet to an access control rule. The matching sequences of ACL are based on the sequence of filtering rules: the later it is in the sequence, the higher priority it has. If there are conflicts in the rules, high priority will be the complied.

Command	Description
config	Enter the global configuration mode
[no] ip ip-access-list {**all**| *acllist*}	Configure the filter based on layer-3 interface **ip-access-list** means the filter is based on IP access control list *acllist* | **all** is the range of series number of the filter based on access control list, **all** means all the configured access control list

exit	Back into the privilege EXEC
show ip ip-access-list	Show all the filter status for the configured layers

Example:

1. The demarcation only permit the IP packet access from 10.0.0.0/8 network segment. raisecom#config

raisecom(config)# ip-access-list 2 deny ip any any

raisecom(config)# ip-access-list 3 permit ip 10.0.0.0 255.0.0.0 any

raisecom(config)#interface ip 0

raisecom(config-ip)# ip ip-access-list 2,3

raisecom(config-ip)#exit

raisecom(config)#exit

Chapter 16 QoS configuration

This chapter introduces QOS function and its configuration methods. User can realize the control of some sort of particular data flow by using the QoS function. It also provide end-to-end service quality assurance for customers' business.

QoS Introduction

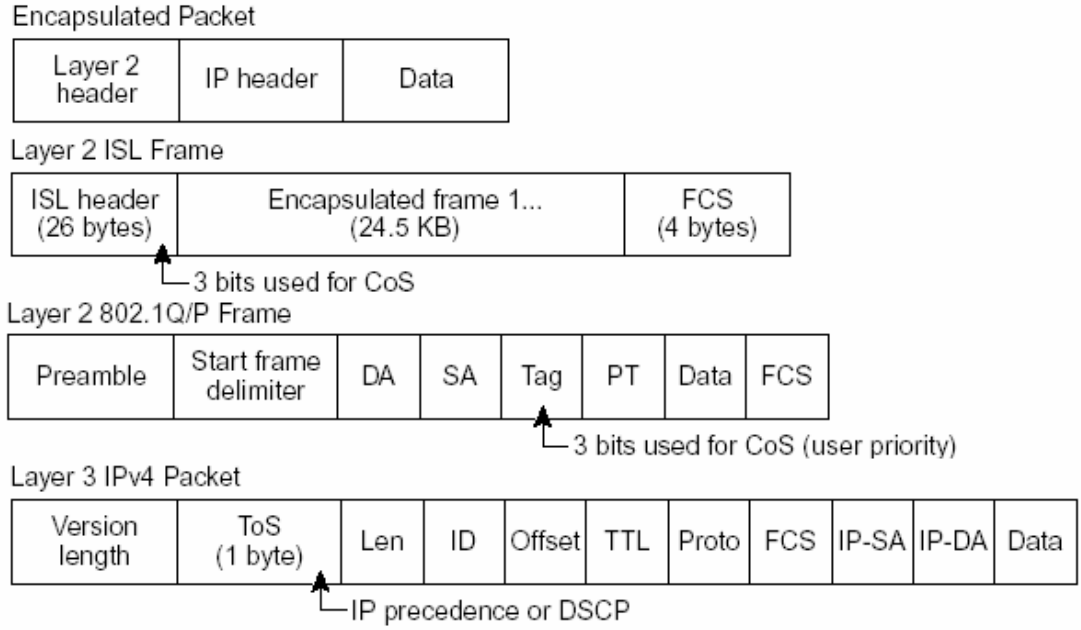
Generally speaking, based on store-forwarding mechanism, the Internet (ipv4 standard) only provide best-effort service to customers, and it can not guarantee the feature of real time, the integrity and the order of arrivals for data transmission, that is to say, it can not guarantee the quality of service. For the user, their requests of different distribute multimedia service applications are different, so they require the network to distribute and control the resource based on requirements. Network service quality (QoS) is then applied to process some sorts of data packets that have the higher priority, or to make the network predictable by using a specified management scheduling policy. In this way, the bandwidth management will be more effective.

The QoS mechanism on RC581 is based on 802.1P, 8092.1Q standards and is to classify data packets on the layer-2.

802.1Q standard defines the VLAN principles, though there is no definition for service quantity structure in this standard, it sets basement for achieving QoS because of the mechanism that can modify the priority of received frame.

802.1P standard defines the priority mechanism. The message with lower priority will not be sent until the message with higher priority been sent.

In the layer-2 802.1Q frame header, there is two-byte TAG control information segment, , the first three higher bits of it have CoS (Class of Service) value, this value is from 0-7, as shown in the following figure:



The eight kinds of priorities defined by CoS can be considered as the classification for the following eight data packets:

000	Routine
001	Priority
010	Intermediate
011	Flash
100	Flash Override
101	Critical
110	Internet Control Network Control

Generally speaking, the highest priority 7 is applied to important network data traffic like route information etc; priority 6 or 5 is applied to interactive video, and music data that are sensitive to time delay; priority 4-1 are applied to multimedia data or important enterprise-level data information; priority 0 is applied to the best-effort sending information as default. So, user can classify the output data flow based on CoS value or apply different operations.

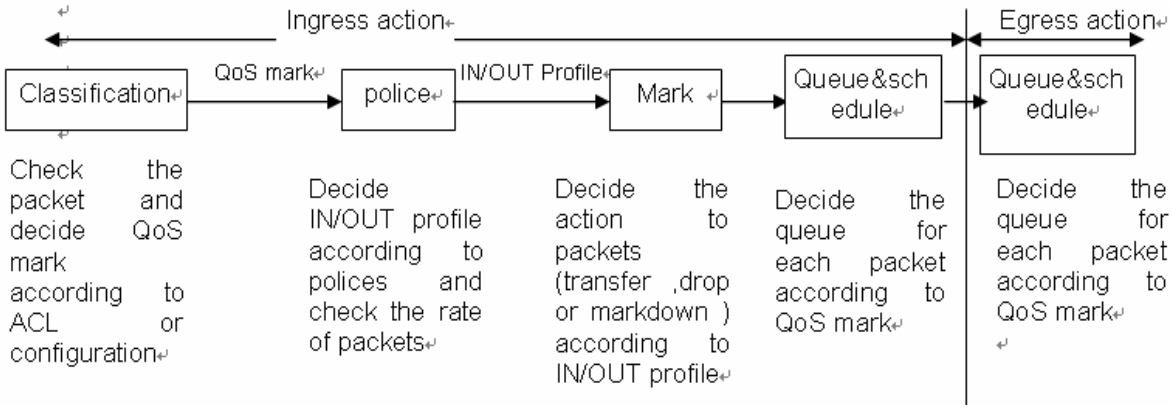
Below is the basic model for QoS:

The action at ingress port includes traffic classification, policing and marking:

- Classifying: used to differentiate the data traffic. This process will generate an interior DSCP value for the data packet to identify all the QoS characteristic operations for all the packets.
- Policing: by comparing the interior DSCP and configured policy, it will decide inputting or outputting profile, and also decides the bandwidth for the data packet. The decided result will be sent to marker.
- Marking: if the data-packet is out-profile, evaluate the policing and the configuration information, and decides how to process the packet (transmit the packet, or mark down the DSCP value and then transmit, or discard the packet)

The actions at output port include queuing and scheduling:

- Queuing: evaluate interior DSCP, an decides to put the data packet into which output queue. DSCP value will be mapped to an interior COS value to select an out queue.
- Scheduling: based on WRR (weighted round robin) and the threshold value, provides service for output queue.



Classification

Classification is a process of checking the domain value of data packet and then to classify the data traffic. Only global QoS is enabled, the classification can be enabled. QoS is disabled as the default situation.

User can specify particular domain in the frame or packet to classify incoming traffic, to non-IP traffic, the classification process as follows:

- Use port default value: if the frame does not include CoS value, distribute default CoS value to the incoming frame, then use CoS-to-DSCP mapping table to generate interior DSCP value.
- For the CoS value of trust incoming frame (configure the port as CoS trust): use the configurable CoS-to-DSCP mapping table to generate interior DSCP value. For non-IP traffic, it does not make any sense to configure it to DSCP trust and Ip priority, it will use port default CoS value.

For IP traffic:

- Trust the IP DSCP value of the input packet (configure the port as DSCP trust): use the DSCP value of the IP packet as the interior DSCP value.
- Trust the CoS value of the input packet: use CoS-to-DSCP mapping table to generate DSCP value.

Mapping table

In the process of QOS, the demarcation describes the interior DSCP precedence for all the data flow:

- In the process of classification, QoS uses configured mapping table (CoS-to-DSCP,IP-precedence-to-DSCP), the interior DSCPA is obtained according to the received COS or IP precedence.
- Before the traffic enters into scheduling, QoS uses DSCP-to-CoS map table and based on interior DSCP value to obtain CoS value, then select the output queue by using the CoS-to-egress-queue mapping.

CoS-to-DSCP and DSCP-to-CoS mapping table has their own default value.

Queuing and scheduling

RC581 aims at different packets to execute two kinds of processing:

- Based on the defined rule, recreate CoS value for message output, but it do not change the CoS value itself;
- This policy is only effective when the rule is set to up to TOS value, that is to change the CoS value of the message according to TOS value;

RC581 supports four kinds of precedence output queuing with the value 0-3, the highest precedence is 3; RC581 also supports two kinds of queuing schedule scheme: strict priority scheduling and control-forwarding weight value scheduling.

RC581 also supports the management of layer 2 message frame that does not have TAG. Each port has its own default priority, which is CoS value. when some particular port received a message without TAG, the demarcation will take port default priority as the current CoS value for the message and set scheduling for it. When the message is output from the demarcation, it will recover the packet format before the input.

Configure QOS list

The configuration for QoS includes the following contents:

- QoS enable and disable
- Configure QoS trust status and CoS default value.
- Configure QoS map table
- Configure QoS class map
- Configure QoS policing map
- Configure QoS classification
- Apply the policy on the port
- Set the scheduling mode for egress queue.
- Monitor and monitor

QOS Default setting

Attributes	Default configuration
QoS enable	disabled
Port trust status	UNTRUST
Port default CoS	0
Port default DSCP	0
Queue scheduling policing	Strict priority scheduling SP

CoS-DSCP default mapping relationship:

CoS value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

DSCP-COS default mapping relationship:

DSCP value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS value	0	1	2	3	4	5	6	7

After QoS is enabled, default mapping relationship between interior COS and the queue:

Interior CoS value	0	1	2	3	4	5	6	7
Queue ID	1	1	2	2	3	3	4	4

QOS enable and disable

The default QoS function is disabled on the demarcation. Apply the following commands under global configuration mode to enable the QoS setting:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**mls qos**	Enable QOS
3	**exit**	Back to privilege EXEC
4	**show mls qos**	Show QOS configuration status

In order to disable QOS, apply **no mls qos** command under global configuration mode.

In order to check whether the configuration is correct or not, use show command:

Raisecom#show mls qos

QoS: Enable

When the QoS has not been enabled, some functions are still effective, for instance, port default CoS, port default DSCP, queue scheduling mode, but all the packets are mapped to queue 1. We suggest user disable the flow control function before the enabling the QoS.

Configure QoS trust status and CoS default value

Under the default situation, the trust status for each port is UNITRUST, default CoS value is 0, default DSCP value is 0. The following steps are for the configuration under port mode:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port 1**	Enter port configuration mode
3	**mls qos default-cos** *cos-value*	Set default CoS value
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege EXEC
6	**show mls qos port**	Show QoS port configuration mode

Configuration example:

Raisecom#config

Raisecom(config)#inter port 1

Raisecom(config-port)#mls qos default-cos 2

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom# show mls qos port

In order to check whether the configuration is correct or not, use show command Raisecom#sh mls qos port

Port Id Trust state Default CoS

---

1 Untrusted 2

2 Untrusted 0

In order to recover default configuration for the port, use no command:

Configure QoS mapping table:

1. COS-DSCP mapping table:

COS-DSCP mapping table map the CoS value of ingress packet to a DSCP value, QoS uses it to describe the priority of data flow.

Default mapping relationship is:

CoS value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

If user wants to modify the mapping relationship, use following steps for configuration:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**mls qos map cos-dscp** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Set new mapping relationship
3	**exit**	Back to privilege EXEC
4	**show mls qos maps cos-dscp**	Show COS-DSCP mapping table for QoS

Configuration example:

Configure the **cos-dscp** mapping as **2 3 4 5 6 7 8 9:**

Raisecom#config

Raisecom(config)# **mls qos map cos-dscp 2 3 4 5 6 7 8 9**

Raisecom(config)#exit

Raisecom# show mls qos maps cos-dscp

In order to check whether the configuration is correct or not, use show command:

Raisecom#show mls qos maps cos-dscp

Cos-dscp map:

cos: 0 1 2 3 4 5 6 7

---

dscp: 2 3 4 5 6 7 8 9

In order to recover the relationship from COS-DSCP mapping table as default, use no command:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**no mls qos map cos-dscp**	Recover to default map relationship
3	**exit**	Back to privilege EXEC mode
4	**show mls qos maps cos-dscp**	Show COS-DSCP map table of QoS

In order to check whether the configuration is correct or not, use show command:

Raisecom#show mls qos maps cos-dscp

Cos-dscp map:

cos: 0 1 2 3 4 5 6 7

---

dscp: 0 8 16 24 32 40 48 56

2、DSCP-COS map table:

DSCP-COS mapping table maps the dscp value of ingress packet to a CoS value, Qos uses it to describe the priority of data flow. The default mapping is:

DSCP value	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS value	0	1	2	3	4	5	6	7

If user wants to modify this kind of mapping relationship, use the following steps:

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**mls qos map dscp-cos** *dscplist* **to** *cos*	Configure new mapping relationship
3	**exit**	Back to privilege EXEC mode
4	**show mls qos maps dscp-cos**	Show the DSCP-COS mapping table of QoS

Configuration example:

Configure **dscp-cos** map,map 1－10 to 7:

Raisecom#config

Raisecom(config)# **mls qos map dscp-cos 1-10 to 7**

Raisecom(config)#exit

Raisecom# show mls qos maps dscp-cos

In order to check whether the configuration is correct or not, use show command:

Raisecom#show mls qos maps dscp-cos

Dscp-cos map:

d1 : d2 0 1 2 3 4 5 6 7 8 9

```
0 :     0  7  7  7  7  7  7  7  7  7
1 :     7  1  1  1  1  1  2  2  2  2
2 :     2  2  2  2  3  3  3  3  3  3
3 :     3  3  4  4  4  4  4  4  4  4
4 :     5  5  5  5  5  5  5  5  6  6
5 :     6  6  6  6  6  6  7  7  7  7
6 :     7  7  7  7
```

In order to recover DSCP-COS mapping table to default mapping relationship, use no command:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**no mls qos map dscp-cos**	Recover to default mapping relationship.
3	**exit**	Back to privilege EXEC mode
4	**show mls qos maps dscp-cos**	Show DSCP-COS mapping table of QoS

In order to check whether the configuration is correct or not, use show command:

```
Raisecom#show mls qos maps dscp-cos
Dscp-cos map:
d1 : d2   0   1   2   3   4   5   6   7   8   9
---------------------------------------
0 :     0  0  0  0  0  0  0  0  1  1
1 :     1  1  1  1  1  1  2  2  2  2
2 :     2  2  2  2  3  3  3  3  3  3
3 :     3  3  4  4  4  4  4  4  4  4
4 :     5  5  5  5  5  5  5  5  6  6
5 :     6  6  6  6  6  6  7  7  7  7
6 :     7  7  7  7
```

Set the scheduling mode for egress queue

Currently, the device only supports two types scheduling mode: Strict priority, weighted round robin. The default setting is strict priority mode.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**queue strict-priority**	Configure as strict priority
3	**queue wrr-weight**	Set the scheduling mode of the port as WRR
4	**exit**	Back to privilege EXEC mode
5	**show mls qos queuing**	Show QoS queue information

Configuration example: set the queue to WRR mode, weight to 1:2:4:8:

Raisecom#config

Raisecom(config)# queue wrr-weight

Raisecom(config)#exit

Raisecom#show mls qos queuing

The results is shown as:

Raisecom#show mls qos queuing

Queue schedule mode: Weighted round robin(WRR)

WRR queue weights:

Queue ID - Weights

1 - 1

2 - 2

3 - 4

4 - 8

CoS-Queue map:

CoS - Queue ID

0 - 1

1 - 1

2 - 1

3 - 1

4 - 1

5 - 1

6 - 1

7 - 1

QOS monitor and maintenance

Use show commands to check the demarcation QoS running information and the configuration information, which can make monitor and maintenance more conveniently. For QoS monitor and maintenance, use the following show commands:

Command, mode	Following command should be executed under ENABLE mode.
show mls qos	Show the enable and disable status of Qos
show mls qos maps [**cos-dscp** | **dscp-cos**]	Show the table configuration contents
show mls qos queueing	Show ingress/egress queuing configuration information
show mls qos port *portid*	Show the configuration policy for the port, and policer information etc.

Show QOS enable information

Raisecom#show mls qos

QoS: Enable

Show QOS map information

Raisecom#show mls qos maps

DSCP-CoS map:

```
d1 : d2  0  1  2  3  4  5  6  7  8  9
----------------------------------------
 0 :     0  0  0  0  0  0  0  0  1  1
 1 :     1  1  1  1  1  1  2  2  2  2
 2 :     2  2  2  2  3  3  3  3  3  3
 3 :     3  3  4  4  4  4  4  4  4  4
 4 :     5  5  5  5  5  5  5  5  6  6
 5 :     6  6  6  6  6  6  7  7  7  7
 6 :     7  7  7  7
```

CoS-DSCP map:

```
    CoS:    0   1   2   3   4   5   6   7
    ----------------------------------------
DSCP:    0   8   16  24  32  40  48  56
```

Show QOS queue information

Raisecom#sh mls qos queueing

Queue schedule mode: Strict priority (SP)

CoS-Queue map:

```
CoS - Queue ID
 0  -  1
 1  -  1
 2  -  1
 3  -  1
 4  -  1
 5  -  1
 6  -  1
 7  -  1
```

Show QOS port information

Raisecom#show mls qos port 1

Port Id Trust state Default CoS

---

1 not trusted 0

If user wants to check all the port information:

Raisecom#show mls qos port

Port Id Trust state Default CoS

---

1 not trusted 0

2 not trusted 0

QOS command reference

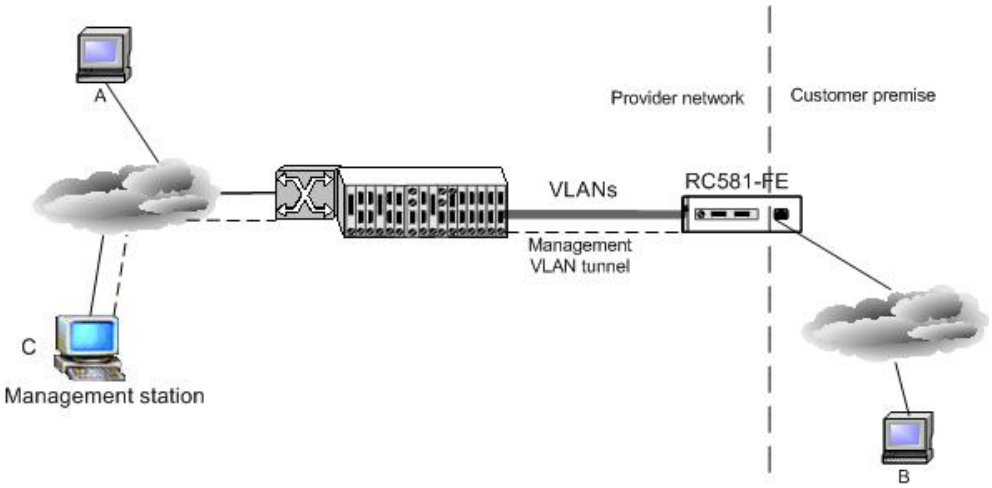
Command	Description
[no] mls qos	Enable or disable QoS
[no] mls qos trust [**cos** | **dscp**]	Configure the port TRUST status
mls qos default-cos *default-cos*	Configure the default COS value for QOS port
no mls qos default-cos	Recover the default COS value of QOS port
mls qos map cos-dscp *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Configure the mapping of cos to dscp
no mls qos map cos-dscp	Recover the map from cos to dscp
mls qos map dscp-cos *dscp-list* **to** *cos*	Configure the map from dscp to demarcation interior priority.
no mls qos map dscp-cos	Recover the map from dscp to demarcation interior priority.
queue wrr-weight	Configure demarcation scheduling mode to WRR.
queue strict-priority	Set the port scheduling mode to strict priority mode.
show mls qos	Show QoS enable/disable.
show mls qos maps [**cos-dscp**|**dscp-cos**]	Show the configuration content for different map table.
show mls qos queueing	Show the configuration information for ingress/egress queue.
show mls qos port *portid*	Show the port configuration information

Chapter 17 USER network

This chapter introduces the function of user network with the configuration method. User can make diagnosis to the customer's data channel by using this function.

User network introduction

RC581-FE can divide the customer and service provider network, support NID/UNI. RC581-FE has very flexible network diagnosis function. As NID(network interface device), it can make diagnosis to the network among the service provider devices. As UNI(user network interface), it can also make diagnosis to the network of customer data channel.



In the topology structure above, as UNI, RC581-FE is able to make diagnosis to the integrality of connection between A and B by using the ping function. It can log on A or B to execute management by using telnet function. As NID it can make diagnosis to the connection between RC581-FE and the management station C at the service provider. It can also use telnet function to log on C to execute the management.

User network command

Enable user network

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**user-network diagnostics**	Enter the user network mode
3	**exit**	Back to global configuration mode

User network permit only one user to log on at one time

The user network show command is under the user network mode, the user network configuration will be automatically cleared up after exiting the user network mode unless using the *exit save-diagconfig* command.

The configuration under user network dose not support loading.

Configure the user network IP address

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**user-network diagnostics**	Enter the user network mode

3	**ip address** *ipaddress [mask]* *<1-4094>* **[port** *{1-2}***]**	Configure the user network IP address
4	**ip default-gateway** *A.B.C.D*	Configure the user network default gateway
5	**show interface ip**	Show ip interface configuration
6	**exit save-diagconfig**	Save the user network configuration and back to the global configuration mode

Layer-3 interface of user network is based on virtual interface configuration of VLAN. User can use **ip address** command to configure the interface IP address and specify the associated VLAN ID and management port. User can also use **no ip address** to delete the layer-3 interface after creation.

User can use **ip default-gateway** command to configure the default gateway, and use **no ip default-gateway** command to delete the default gateway.

The VLAN configuration can be referred to chapter 14.

User network supports only one virtual layer-3 interface. Virtual layer-3 interface corresponds to multiple static VLAN ID and multiple management port. After creating layer-3 interface, if the static VLAN does not exist, this layer-3 interface will not work properly.

The management port is all the ports under the default situation.

The user network uses an independent protocol stack differentiated from management network. User can differentiate user network from management network according to VLAN.

After the layer-3 interface configuration, user can use ping tools to diagnose the network connection, or use telnet tools to manage the remote host system..

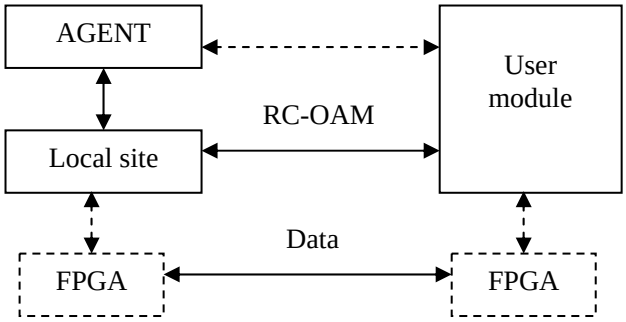
Chapter 18 RC-OAM configuration

RC-OAM protocol introduction

RC-OAM protocol is Raisecom's private OAM protocol, which is mainly applied to partial optical products such as RC581. An example is given below for the instruction.

Communication model

The communication model used by RC-OAM protocol is shown below:



Series port is applied for communication between AGENT and local site.

Basic network maintenance information is transmitted between local module and user module, which includes the optical interface's RLNK information, TLINK information, electrical port's LINK(when there is only one connection) information and the configuration information of duplex mode, rate at the customer site etc.

The communication between AGENT and customer module needs to be forwarded by the local site module. It is regulated that the local site module provides one transparent link for AGENT and customer module, the local site module only encapsulate forward the data without making any operation to the communication between AGENT and customer site module, and only encapsulate the data

The communication between local site and customer site follows RC-OAM protocol. Protocol frame is sent and received via FPGA.

Main function

RC-OAM main function includes:

- ✧ Module reset(exclude CPU);
- ✧ configuration

- ➢ fault at optical interface transferred to electrical port;
- ➢ fault at electrical port transferred to optical interface;
- ➢ optical interface fault return;
- ➢ electrical port enabling, autonegotiation, rate(10M/100M)and duplex mode;
- ➢ bandwidth at the ingress and egress for the electrical port;
  - ✧ Status information report
- ➢ Main chip number, denotes the switching chip's type;
- ➢ FPGA chip number;

- FPGA chip code edition number;
- Device host software version number: X.Y.PB.SB.YYMD. Each letter denotes one byte. X is the main version number; Y is the secondary version number; PB is the revising times of the platform BUG; SB is the revising times of software BUG; YYMD denotes year, month and day;
- Module current running status: includes the fault pass from optical to electrical, electrical to optical, whether requesting configuration information;
- The temperature current value;
- Voltage (1.2V、1.8V、2.5V and 3.3V) current value;
- Optical interface fault return configuration;
- Optical interface status, receiving fault at optical interface can lead to sending rejection at optical interface; fault at electrical port can lead to sending rejection, optical LINK status, SD signal runs normally or not;
- Electrical port confiuration value, including enable/disable configuration, auto negotiation configuration, rate configuration and duplex mode configuration;
- Electrical port status, shutting down electrical port will lead to electrical port rejection, because the fault pass is enabled, if the optical interface is LINK-DOWN, the local electrical port will shut down accordingly, electronical port LINK status, auto negotiation, actual rate, duplex mode;
- The ingress and egress bandwidth;
- Device IP address, 4 bytes, all 0 means IP address is not meaningful;
- Group attributes is one byte, denotes the name and attributes for the group. 0x01 means read only, 0x02 means read and write only, 0x00 is not meaningful;
- The length of group name is 20 bytes, the actual exceeding part is filled with 0x00;

RC-OAM configuration

Enable or disable RC-OAM function

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**oam** {**enable** | **disable**}	Enable or disable OAM function
3	**exit**	Back to privilege EXEC
4	**show oam**	Show the configuration