RAISECOM

www.raisecom.com

RC953-4FExE1T1 Configuration Guide

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:

Address: Building 2, No. 28 of the Shangdi 6th Street, Haidian District, Beijing 100085

Tel: +86-10-82883305

Fax: +86-10-82883056

World Wide Web

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

http://www.raisecom.com

Feedback

Comments and questions about how the RC953-4FExE1T1 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 RC953-4FExE1T1 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

This manual is a valuable reference for sales and marketing staff, after service staff and telecommunication network designers. For those who want to have an overview of the features, applications, structure and specifications of RC953-4FExE1T1 device, this is also a recommended document.

Relevant Manuals

Raisecom NView System User Manual

Raisecom Nview System Installation and Deployment Manual

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 Overview

1.1 Basic switch functions

- Mirror function: including the mirror that is from any port to one port, which is used for network data monitoring and analysis.
- System log: multiply log display mode is supported.
- System clock: SNTP time synchronization and manual configuration is supported.
- Task scheduling: with this function a certain command can be executed seasonally.

1.2 Layer-2 function

- MAC address table management: static MAC configuration and dynamic MAC learning are supported.
- Physical layer interface configuration: including rate and duplex mode configuration, 802.3x flowcontrol function and port enable/disable.
- Storm control: including broadcast, multicast and DLF frame control.
- Message relay and transmission: including the option of protocol messages or DLF message.
- Link aggregation: including aggregated link load balance.
- DHCP configuration: including DHCP Server, DHCP Relay and DHCP Snooping function, with the legal DHCP server user can get IP address automatically.
- ARP management: including static and dynamic ARP address table maintainnace.
- Loopback detection: aiming at the network trouble caused by Loop, it develops the robustness, fault tolerance and debugging ability of the network.
- VLAN configuration: including basic VLAN configuration, Q-in-Q and flexible Q-in-Q function.
- Shared VLAN: SVL mode is supported.
- RST configuration: IEEE 802.1w rapid spanning tree protocol is supported.
- MST configuration: IEEE 802.1Q multiply spanning tree protocol is supported.

1.3 Management function

- Basic management:
  - Management using CONSOLE is supported;
  - Remote management with TELNET is supported;
  - Auto-configuration is supported, that is to download configuration files automatically from network management configuration server and realize network management configuration.
- SNMP configuration: SNMP v1, SNMP v2 and SNMP v3 is supported.
- RMON configuration: you can use different network agent and manage-station system to monitor network data, now RMON1, 2, 3, 9 groups are supported.
- Cluster management: with Raisecom cluster management function, network administrator is able to manage several switches using the public IP address of the main switch. Three protocols are included: RNDP, RTDP and RCMP.
- Bandwidth management function configuration: rate-limit based on port or VLAN is supported.
- ACL and network security configuration: multiply access list configuration is supported, you can sort and filter the packets according to the matching list.
- QoS function: specific traffic control, it offers end to end quality of service guarantee for user's service.
- OAM configuration: IEEE802.3ah is supported
- Extended OAM configuration: management and monitor remote devices with IEEE802.3ah OAM link, the main functions include: acquiring and configuring remote device attribution, downloading or uploading remote device files, managing extending OAM link state and statistics.
- Optical module digital diagnoses: SFP fault diagnose function is supported.

1.4 Protocols that the functions are based on

- RST: IEEE 802.1w;
- MST: IEEE 802.1Q;
- OAM: IEEE 802.3ah;
- Port flowcontrol function: IEEE 802.3x.

Chapter 2 Commands Line Usage

2.1 Introduction to commands line

Commands Line is the channel for the communication between subscribers and switches. In the commands lines, subscribers is able to monitor, control and manage the switches through configuring the corresponding commands. For better convenience, subscribers can edit shortcuts to use the commands, by the same time subscribers can examine the used commands through transferring the history. The commands line mode confines the way different subscribers use commands lines, where various commands line modes are offered. Subsribers can make certain configuration only in the corresponding mode.

2.2 Commands line usage configuration

2.2.1 Commands line mode configuration

Mode	Mode description	Access	Prompt	Out
Universal subscriber mode	Subscriber is allowed to configure the basic information and the parameter shown on the switch.	Login the switch and enter the user's name and password.	Raisecom>	**Exit** Withdraw from the current mode.
Subscriber privileges mode	Subscriber is allowed to configure the basic information of the switch, like system time and the name of the switch, except the operation information.	From universal subscriber mode, type **enable** and password.	Raisecom#	**Exit** Withdraw from the current mode.
Global configuration mode	Subscriber is allowed to configure all the operation parameters.	From subscriber privilege mode, type **config**	Raisecom(config)#	**Exit** Withdraw from the current mode.
Physical layer interface configuration mode	Subscriber is allowed to configure the Ethernet physical interface of the switch.	From global configuration mode, type **interface line/client portid**.	Raisecom(config-port)#	**Exit** Withdraw from the current mode.
Physical layer interface bulk configuration mode	Subscriber is allowed to range configure the parameter of the switch's Ethernet physical interface.	From global mode, type **interface line/client portid**.	Raisecom(config-range)#	**Exit** Withdraw from the current mode.

Three-tier interface configuration mode	Subscriber is allowed to configure the switch's three-tier Ethernet interface.	From global mode, type **interface line/client ip** id.	Raisecom(config-ip)#	**Exit** Withdraw from the current mode.
VLAN configuration mode	Subscriber is allowed to configure the VLAN operation parameters.	Enter **vlan**	Raisecom(config-vlan)#	**Exit** Withdraw from the current mode.
Class Map configuration mode	Subscriber is allowed to configure the given data flow.	From global configuration mode, type **class-map** class-map-name **[match-all | match-any]** command.	Raisecom(config-cmap)#	**Exit** Withdraw from the current mode.
Policy Map configuration mode	Subscriber is allowed to classify and package the data flow defined by class-map.	From global configuration mode, type **policy-map** policy-map-name command.	Raisecom(config-pmap)#	**Exit** Withdraw from the current mode.
Traffic classification configuration mode	Subscriber is allowed to configure the action of the date flow.	From policy map exec mode, type **class-map** class-name command.	Raisecom(config-pmap-c)#	**Exit** Withdraw from the current mode.
The cluster configuration mode	Subscriber is allowed to configure the cluster.	From global configuration mode, type **cluster** command.	Raisecom(config-cluster)#	**Exit** Withdraw from the current mode.
Access control list mapping table configuration mode	Subscriber is allowed to configure the access control list mapping table.	From global configuration mode, type **access-list-map** *<0-399> {permit | deny}* command.	Raisecom(config-aclmap)#	**Exit** Withdraw from the current mode.
Subscriber network mode	Subscriber is allowed to configure three-tier network setting, show the users' network information and network tools.	Form global configuration mode, type **user-network diagnostics.**	Raisecom(config-usrnet)#	**Exit** Withdraw from the current mode.
RIP configuration mode	Subscriber is allowed to configure RIP.	Form global configuration mode, type **router rip.**	Raisecom(config-router-rip)#	**Exit** Withdraw from the current mode.
OSPF configuration mode	Subscriber is allowed to configure OSPF.	From global configuration mode, type **router ospf**.	Raisecom(config-router-ospf)#	**Exit** Withdraw from the current mode.

2.2.2 Getting 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: ISCOM> **en? english enable**
abbreviated-command-entry<*Tab*>	Makeup 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 and options for particular command with a short help information for it. Raisecom#**show ?**
command keyword ?	List the key words corresponding command For example Raisecom(config)#**ip**? IP setting ip-access-list Define IP access control list

2.2.3 Using Editing Features

up arrow:	last entered command
down arrow:	next entered command
left arrow:	move a character left
right arrow:	move a character right
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 to the right the cursor
Ctrl+w:	delete all the characters to the left of the cursor
Ctrl+u:	delete the row all
Ctrl+z:	exit from other modes to privileged mode

2.2.4 Command-line History

The switch records the latest 20 commands in the cache by default. User can use the following command to set the number of history commands that will be recorded:

Raisecom>**terminal history** *<0-20>*

Use **history** to show the history command.

2.2.5 The command-line Error

Error	Description	Getting help
Unknown command or in accurate For example Raisecom#**sh co** % “co” Unknown command.	Review the command needed.	
The command is not confirmed: For example Raisecom#**sh r** %“r” Unconfirmed command	Input the order that can not be recognized by the switch from the commands.	Add **?** for annotation and command. For example: Raisecom#**sh r** rate-limit: Rate control Rmon: Remote Network Monitoring (RMON) configuration Rndp: RNDP configuration Rtdp: RTDP configuration running-config: Running system configuration information
Command incomplete For example Raisecom#**show** % “show” Incomplete command.	The switch can not recognize the operation form the command, command that can be recognized is needed.	Add **?** for command and annotation. For example: Raisecom#**sh r** rate-limit:Rate control Rmon: Remote Network Monitoring (RMON) configuration Rndp: RNDP configuration Rtdp: RTDP configuration running-config: Running system configuration information

Chapter 3 Radius Accounting

3.1. Overview

Radius accounting function is mainly for the user that is doing Radius authentication in certification stage. When the user is logging on, a message that enables accounting function will be sent to Radius accounting server; during the time that user is landed, accounting updating message will be sent to the server according to the accounting strategy; and when the user is logging out, a message to stop accounting will be sent to the server, which contains the landing time. With these messages, the server can be clear when and who have ever landed the switch, the logging time and even the operation.

3.2. Default configuration

By default Radius accounting is disabled.

3.3. Radius accounting configuration

3.3.1. Enable/disable Radius accounting function

The configuration is to enable or disable Radius accounting function. By default the function is disabled.

Step	Command	Description
1	**aaa accounting login** *{enable|disable}*	Enable disable Radius accounting
2	**show radius-server**	Show Radius configuration

3.3.2. Configure Radius accounting server IP address and UDP port number

The configuration is to configure the IP address and UDP port number of Radius accounting server. By default the IP address is 0.0.0.0, port number is 1813.

Step	Command	Description
1	**radius accounting-server** *A.B.C.D [acct-port]*	Configure the IP address and UDP port number of Radius accounting server. A.B.C.D is the IP address of accounting server *Acct-port* is the UDP port number of accounting server, range is 1-65535. The configuration is an optical option, the current value is the default value. Use **no radius accounting-server** to restore the IP address and port number to default value.
2	**show radius-server**	Show Radius configuration

3.3.3. The strategy of Radius accounting configuration fail

When Radius accounting is enabled, user who passed Radius certification will be charged, but if the accounting fails (disconnected with the server or when shared key is different from the one on the server), there are two way, one is to allow user login, the other is to deny. By default it is to allow.

Step	Command	Description
1	**aaa accounting fail** *{online|offline}*	Configure the strategy of accounting fail
2	**show radius-server**	Show Radius configuration

3.3.4. Configure Radius accounting strategy

There are two strategies, one is to send one accounting enable message to accounting server when user is logging on, and send one accounting ending message to the server; the other way is to add accounting update messages periodically besides the two kinds of messages above, the period is changeable. By default the first way will be taken.

Step	Command	Description
1	**aaa accounting update** *<0-300>*	Configure accounting update message period *<0-300>* the period of accounting update message sent, unit is minute, if it is configure 0, the message will not be sent. Use **no aaa accounting update** to restore the accounting strategy to default value
2	**show radius-server**	Show Radius configuration

3.4. Monitoring and Maintenance

Command	Description
show radius-server	Show Radius configuration

3.5. Typical configuration example

Example 1: enable Radius accounting function, configure the IP address of accounting server to 20.20.20.20, port number is 6000, shard key is hello, the accounting fail strategy is offline, the accounting strategy is to send a accounting update message per 10 minutes.

Raisecom# **aaa accounting login** *enable*

Raisecom# **radius accounting-server** *20.20.20.20 6000*

Raisecom# **radius accounting-server key** *hello*

Raisecom# **aaa accounting fail** *offline*

Raisecom# **aaa accounting update** *10*

Chapter 4 System Function

4.1 File Management

4.1.1 Profile Management

The default configuration storage file name of the system is: **startup_config.conf**. The configuration storage file could be written into the flash file system through the command **write**, and the configuration information will be re-configured automatically the next time the system reboot. Use **erase** to delete the file. The configuration information file **startup_config.conf** could be uploaded to the server or downloaded to the system to replace the original configuration information, through FTP protocol with the command **upload** and **download**. Use **show startup-config** to show the configuration information in storage. Use **show running-config** to show the current configuration information in the system.

Command	Description
write	write the configuration file into the flash file system, and the configuration information in storage will be re-configured automatically after the system rebooting
erase	delete the file
show startup-config	the configuration information in storage
show running-config	The configuration information in the current system

4.1.2 BOOTROM file management

BOOTROM, boot of the switch, initialize the switch. User can upgrade BootROM file through FTP. BootROM file system is called **bootrom** (or **bootromfull**) in default cases. With the command **ftp file-name,** user can set these file system names.

When powered, the switch will run **BootROM** file first. When 'Press space into Bootrom menu…' is shown, user can enter **Bootrom** menu bar by pressing ENTER, and carry out the following operation:

'**?'** show all the commands available

'**h'** show all the commands available

'**v**' show the version of **Bootrom**

'**b'** quick start executive command

'**T'** download configuration file through the switch ports

'N' set the MAC address

'R' reboot the switch

4.1.3 System File Management

The documents that keep the equipment running, like host software and configuration files, are kept in the storage devices.For the convenience and efficiency of user's managing the equipment, the equipment manage the documents in the way of Document System. The function of the document system contains catalog's creating and deleting, document's copying and display, and so on. In default cases, the document system will remind user for confirmation if the command may lose any data (like deleting or recovering files).

- With the command **upload** and **download,** program files could be uploaded to the server or downloaded to the system through the TFTP protocol or FTP protocol;
- Use **dir** to look over the system FLASH files;
- Use **show version** to look over the software version;
- Use **clock** to set system time;
- Use **logout** to exit the current system.

Command	Description
dir	To look over the system files
show version	To look over the software version
clock	To set system time
logout	exit

4.1.4 FPGA files management

FPGA(field programmable gate arrays) is the most integrated in Application Specific Integrated Circuit(ASIC). To accomplish user's logic, subscriber can re-configure the logical module and I/O module in FPGA, which can also be used on CPU's simulation. User's programming data to FPGA, stored in FLASH chip, could be uploaded to FPGA when powered and initialized. Online-programming is also available, making the system reconstructed online.

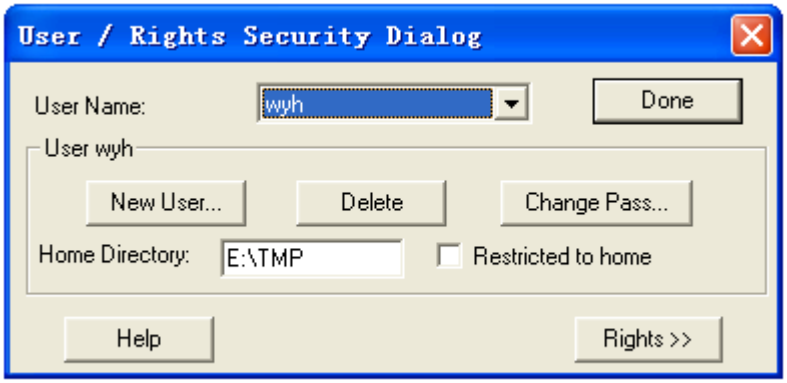
When powered, the FPGA chip will write the data in EPROM into programming ROM and get into working state after the configuration finished. When power off, FPGA will be empty and the logic inside is gone, thus FPGA could be repeated used. There is no special programmer for FPGA programming, the universal EPROM, PROM programmer can fit it. When the function of FPGA needs to be modified, only on piece of EPROM needs to be changed. So, by one FPGA different programming data brings different circuit function.

Command	Description
Upload *{system-boot|startup-configure|remote-fpga }* **ftp** *A.B.C.D username password filename*	Files are uploaded to server through FTP protocol A.B.C.D:IP destination address **username** server user name **password** user's password **filename** filename(o.0)
download *{system-boot|startup-configure|bootstrap |remote-fpga}* **ftp** *A.B.C.D username*	By FTP protocol the files are downloaded to the system and replace the files before. A.B.C.D:IP destination address

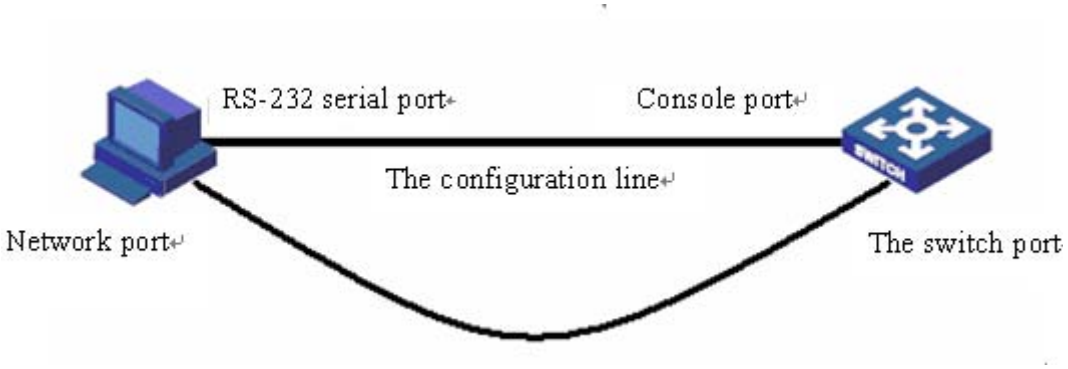
password filename	**username** server user name **password** user's password **Filename** filename(o.0)
upload *{system-boot|startup-configure|remote-fpga }* **tftp** *A.B.C.D filename*	Files are uploaded to server through FTP protocol **A.B.C.D**:IP destination address **Filename** filename
download *{system-boot|startup-configure|remote-fpga }* **tftp** *A.B.C.D filename*	Files are uploaded to server through FTP protocol **A.B.C.D**:IP destination address **Filename** filename

4.1.5 A typical configuration example

When subscriber has already have his/her own configuration files or new upgrade files, he/she can download the configuration files into the switch. To make it, subscriber should open the FTP software, like wftpd32.exe, and set user name, password and file path. As shown below, user name is wyj, password:123, the path of the configuration file is E:\TMP.



User uses serial line to connect the switch and PC, and connect the line to the switch port, as shown below. Open the terminal emulation program, such as **SecureCRT 5.1**. Take Console management as reference when using Console interface.



User can also use **Upload, download** to upload and download files from FTP. The connection line is shown as figure.

For example:

Using FTP to download system file **ROS_4.3.313.ISCOM2926.31.20080602** to the switch, user should set

the switch IP address:20.0.0.10 first, then open the FTP software **wftpd32.exe** and set user name, password, and file path. Input **download** and select **system-boot**, input the host IP address: 20.0.0.10, user name, password of the FTP software, and all the process is done.

Raisecom#**config**

Raisecom(config)#**interface ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Set successfully

Raisecom(config-ip)#**exit**

Raisecom(config)#**exit**

Raisecom#**download startup-config ftp** *20.0.0.221* **wyh** *123*

ROS_4.3.313.ISCOM2926.31.20080602

Waiting....Start

Getting from source ...Done

Writing to destination...Size 1754K / 1754K

Success!

When the files in switch need to be uploaded to the host, user can use TFTP to upload **startup-config** to the host. To do this, user should set the IP address 20.0.0.10 of the switch, then open the TFTP software **Cisco TFTP Server** to set the file path, input **upload**, host IP address 20.0.0.221, and upload the generated file name WW.

Raisecom#**config**

Raisecom(config)#**interface ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Set successfully

Raisecom(config-ip)#**exit**

Raisecom(config)#**exit**

Raisecom#**upload startup-config tftp** *20.0.0.221 ww*

Waiting....Start

Getting from source ...Done

Writing to destination...Size 1K / 1K

Success!

4.2 Switch Management

4.2.1 Console Management

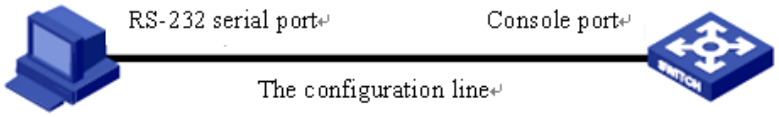
Local control port management means using a console port of a terminal or a PC that is running terminal simulation program to configure and manage the switch. This management approach is out-of-band management, and needs no network for communication. Thus the console port can configure and manage the switch even if the network is not going on well.

Local management manage the switch by connecting the terminal and console program inside the switch.

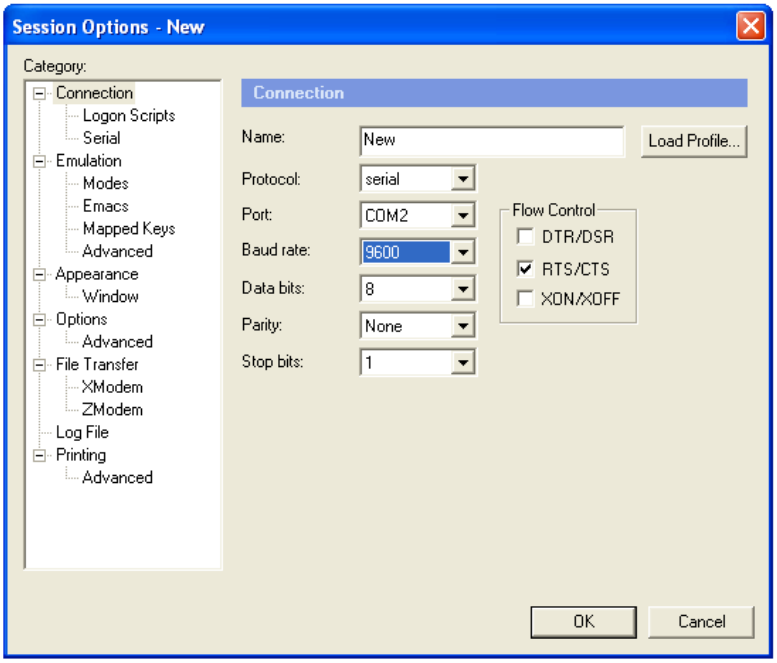
To login in the Ethernet switch through the console port, the user's terminal communication parameter configuration and the configuration of switch's console port should be consistent. The default configuration of the switch's console port is shown below

Attribution	Default value
Baud rate	9600bit/s
Flow control mode	No flow control
Check mode	No check
Stop bit	1
Data bit	8

First, connect the switch console port and the serial port of PC, and keep the PC online. As shown below,



Then, run the terminal simulation program on PC, such as **SecureCRT 5.1**, as is shown below. Select the serial port connected with the switch port, and configure the terminal communication parameter as: baud rate 9600 bit/s, 8 data bits, 1 stop bit, no validation and flow control, serial interrupted default value 100ms.



At last, download the system files to the switch and run it through console port. The calculation of the switch data can also be observed and controlled by computer.

4.2.2 Telnet management

The TELNET protocol aims at offering a communication mechanism which is generally universal, two-way

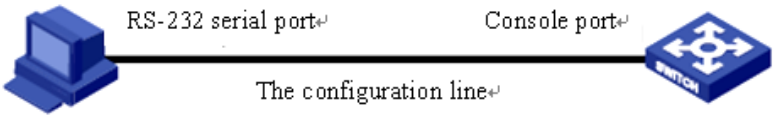
and 8 byte available. Its main objective is letting terminal interface device and the process for terminal interact. In addition, as you can see, the protocol could be used in terminal communication (connection) and process to process communication (distributed computing).

A general thought: a telnet connection is a connection which is used to transfer TCP that contains TELNET control data.

TELNET protocol base on the following 3 ideas mainly: first, virtual network terminals; second, the principle of negotiating options; third, viewing the terminal and process as a balanced approach.

User can make remote management and maintenance through Telnet. Both switch client and telnet client need corresponding configuration so that user can login in the switch by Telnet.

When user login on a switch, the picture following shows the detail:



User can start TELNET services by command:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *0*	Enter IP port mode
3	**ip address** *A.B.C.D [A.B.C.D] <1-4094>*	Configure the IP address A.B.C.D: IP address [A.B.C.D]: subnet mask <1-4094>: vlan number
4	**exit**	Exit global configuration mode and enter enable mode
5	**telnet-server {accept|close|max-session}** *port-list*	Set telnet services; port-list port list
6	**show telnet-server**	Show telnet configuration

4.2.3 SSH management

4.2.3.1 SSH default configuration

Function	Default
SSH server status	Stop
Key-pair	No

4.2.3.2 SSH configuration

Before the server start key-pair have to be created. User manage command creating and key-pair deletion

by key-pair. User use keys to create command and key-pair, before new key-pair is created, user must delete the key-pair that existed, because only one key-pair can be created on one equipment.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**key-pair generate** *KEYNAME* **rsa** *[modulus <768-2048>] [comment COMMENT]*	Create key pair KEYNAME key-pair name 768-2048 range of the module length COMMENT key-pair comment
3	**ssh server** *KEYNAME*	Start SSH server KEYNAME key-pair name
4	**exit**	Return to global configuration mode
5	**show key-pair KEYNAME**	Show key-pair information

User can use **no ssh server** to stop SSH server after the SSH server start.

The key-pair will be stored on the equipment automatically after successful creation, until user delete it or the equipment is formatted.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**key-pair destroy** *KEYNAME*	Destroy key-pair
3	**exit**	Return to global configuration mode
4	**show key-pair** *KEYNAME*	Show key-pair information

4.2.3.3 Monitoring And Maintaining

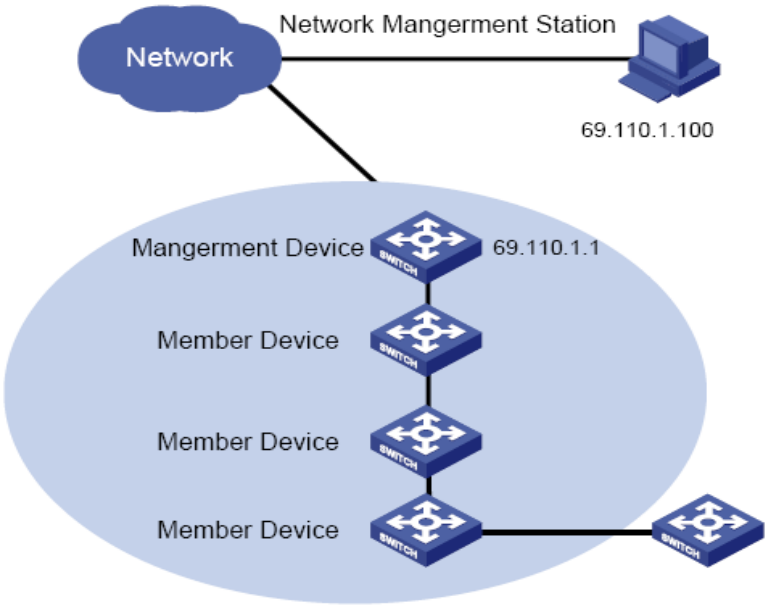
Command	Description
show key-pair *KEYNAME*	Show key-pair information
show ssh server	Show server configuration information
show ssh session	Show SSH dialog information

4.2.4 Cluster 'rcommand' Management

4.2.4.1 Cluster 'rcommand' Function Introduction

Using Raisecom cluster management function, network administrator is able to manage several switch through a registered IP address of the main switch. The main switch is command facility, while the other switches that are under administration will be member equipments. Member equipment needs not IP

address setting usually, it is managed and maintained by manage equipment's redirection. The typical using environment is shown below:



Cluster management contains three protocol: RNDP (Raisecom Neighbor Discover Protocol), RTDP (Raisecom Topology Discover Protocol) and RCMP (Raisecom Cluster Management Protocol). RNDP see to the facility neighbor discovery and information collection, RTDP see to collecting and handling all the network topology information, while RCMP see to the cluster member's joining, validation, deletion and so on. Among them, RTDP and RCMP communicate in cluster VLAN. So, appropriate configuration to VLAN2 is needed to make sure that RTDP and RCMP communicate normally, when there be facility that does not support Raisecom cluster management function between the two facilities that need cluster management.

Different roles form by the different degrees and functions of each switch in the cluster, but user can constitute a certain switch's role form configuration. The roles in cluster include supervisory unit, member unit and alternate unit.

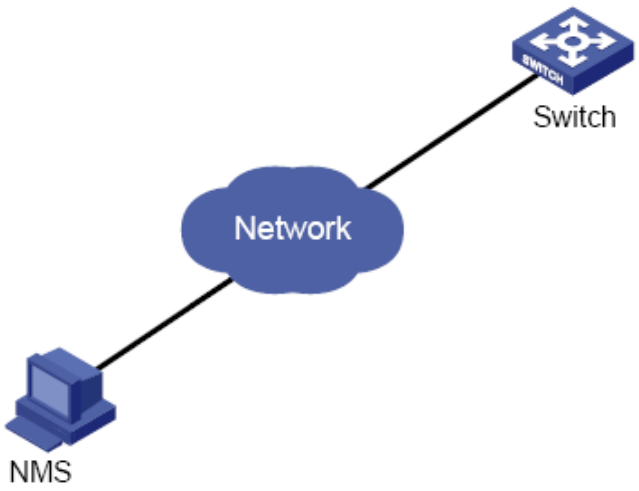
Rcommand, like telnet, can login member switch on the command-line interface of the supervisor switch. Consult cluster management function about configuration and commands of cluster management.

4.2.5 NMS Management

NMS: Network Management System. It has 5 functions: alarming, performance, configuration, safety and accounting. In SNMP, NMS is the workstation running the client program. IBM NetView and Sun NetManager are the usual NMS stations in use. When SNMP Agent receives the query message Get-Request, Get-Next-Request, Get-Bulk-Request about MIB from NMS, Agent carry out **read** or **write** to MIB according to the message style, then create **Response** message according to the operation result and sent it to NMS as response.

On the other side, once SNMP Agent receives any change on facilities like normal/hot booting or anything unusual it will create a **Trap** massage and report it to NMS actively.

User can login the switch through NMS, manage and configure the switch by the Agent process on the switch. As shown below.



4.2.6 User Logging Management

User can login, configure and manage the switch by the following way:1, local login from Console port;2, local or remote login using Telnet through Ethernet port;3, login from NMS port. User's name and password is needed when logging, by default username is **raisecom**, password **raisecom**:

Step	Command	Description
1	**user** *USERNAME* **password** {**no-encryption**|**md5**} *PASSWORD*	User login **USERNAME username**; **PASSWORD** password;
2	**user** *USERNAME* **privilege** <*1-15*>	User login privileges; **USERNAME** username; <1-15> user privileges grade;
3	**write**	Save configuration information
4	**show user**	Show user information

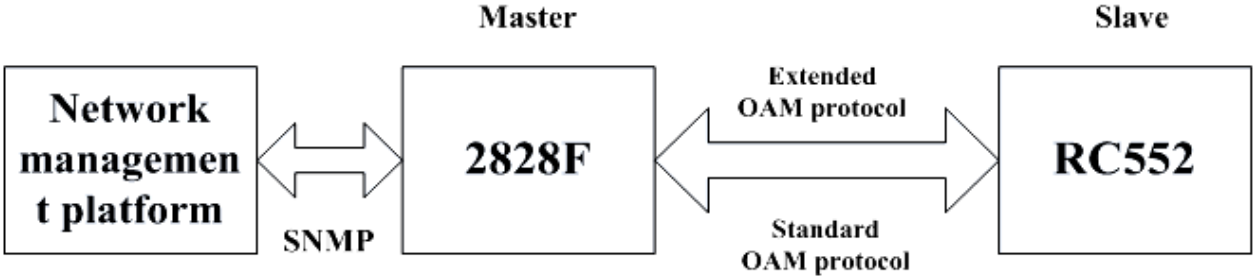
4.2.7 Expended OAM Management

Expended OAM, by IEEE802.3ah OAM link, manage and monitor remote facilities. It contains 3 parts of function:1,aquire and set remote facilities;2, download and upload remote facility files;3, manage the expended OAM line state and stat.. Specific functions are as follows:

- Remote attribution acquirement: local facility can get remote facilities' attribution, configuration and statistics.
- Configuring remote facility basic function: local facility could configure remote facility function by expending OAM, including host name, port enable/disable, port speed duplex, port bandwidth, failover and so on.
- Configuring remote facility management parameter: configure network administration parameter for remote facility that support SNMP network administration, like IP address, gateway, group parameter and VLAN management, and carry out comprehensive network management through SNMP protocol.
- Remote TRAP: when remote facilities find **LINK UP/DOWN** port, the remote port will inform local port by sending expended OAM **notification** frame, then the local port will send remote TRAP alarm to network administrator.

- Expended remote end loopback: the local end is able to manage remote fiber port inner loop function, and set the loopback data to decide if CRC needs re-computing.
- Resetting remote facilities: orders from local end is able to reset or reboot remote facilities.
- Other remote facilities' function management: as remote facilities increases, local facility can manage more remote end functions by expend OAM protocol, like SFP, Q-in-Q, virtual line diagnoses and so on.
- Downloading remote end files: remote end files could be downloaded to remote facilities directly from FTP/TFTP server, another way is downloading them from server to local end, then to the remote facilities.
- Uploading remote end files: remote end files could be upnloaded to remote facilities directly from FTP/TFTP server, another way is uploading them from server to local end, then to the remote facilities.
- Expended OAM line stat. and function management.

Expended OAM network is shown as below. Local switch MASTER:ISCOM2828F; remote end SLAVE: RC552-GE.



Notice: The expended OAM line could be established only between the local facility and remote facility, that is to say, the facility on each end must be OAM active mode and OAM passive mode respectively.

4.3 Keepalive Function

4.3.1 The Introduction To Keepalive Principle

To find out the facility out of order in time, user needs to acquire the facility information periodically to see if the facility is available and the basic facility information. Users can receive the state of **Keepalive Trap** information collection facility from NMS periodically without any operation. Keepalive module send TRAP periodically to NMS about the basic information of facilities, including facilities' name, facilities' OID, the hardware and software version, MAC address and IP address.

Keepalive module send **keepalive trap** that contains the basic information of the switch to the network administration station, so that the network administration station could find the switch in a short time.

4.3.2 Keepalive Default Configuration

Function	Default
keepalive trap switch	On
Keepalive alternation	300 seconds

4.3.3 Keepalive Configuration

By default, KEEPALIVE is open on the switch, and the switch send KEEPALIVE trap periodically. By carrying out the following command in global configuration mode, KEEPALIVE can be set OPEN, CLOSE and PAUSE. If it is CLOSE, the configuration can be loaded. And if it is PAUSE, the configuration can not be saved, the configuration is still default after reboot.

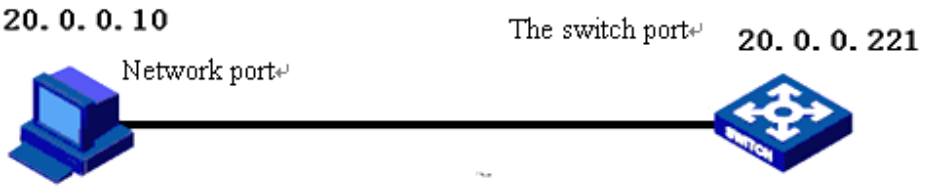
Step	Command	Description
1	**config**	Enter configuration mode
2	**interface ip** *0*	Enter IP port mode
3	**ip address** *A.B.C.D [A.B.C.D] <1-4094>*	Configure the IP address of the switch *A.B.C.D*: IP address *[A.B.C.D]*: subnet mask *<1-4094>*: vlan number
4	**exit**	Quit global configuration mode and enter privileged EXEC mode
5	**snmp-server host** *A.B.C.D* **version** *3 { noauthnopriv | authnopriv } NAME [udpport <1-65535>] [bridge] [config] [interface] [rmon] [snmp] [ospf]*	Configure SNMPv3 Trap the destination host *A.B.C.D*: IP address *NAME*: SNMPv3 team name *<1-65535>*: the UDP port number which the destination use to receive TRAP
6	**snmp-server keepalive-trap interval** *<120-28800>*	Set he interval time fo the switch sending KEEPALIVE-TRAP to SNMP network administration station *<120-28800>*: the interval range, the unit is second
7	**snmp-server keepalive-trap** {*enable|disable|pause}*	Start, close, pause sending keep alive trap
8	**exit**	Return to privileged EXEC mode
9	**show snmp config**	Show basic SNMP configuration

4.3.4 Monitoring And Maintenance

Show is used to show switch the operation and configuration for maintenance and monitoring. To do this, the following **show** command is available:

Command	Description
show snmp config	Show the basic configuration of SNMP

4.3.5 An Example Of Typical Configuration



As is shown above, set the IP address as 20.0.0.10 first, then configure the SNMPv2c Trap destination host address: add a **host_1** host address, username public, SNMP version v2c, all trap, set the interval time 500S of the switch sending **keepalive-trap** to SNMP network administration station, open **keepalive trap**, show basic SNMP information at last.

Raisecom#**config**

Raisecom(config)# **int ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**snmp-server host** *20.0.0.221* **version 2c public**

Raisecom(config)#**snmp-server keepalive-trap interval** *500*

Raisecom(config)#**snmp-server keepalive-trap** *enable*

Raisecom(config)# **show snmp config**

4.4 Task Scheduling Function

4.4.1 The Introduction To Task Scheduling Function Principle

The function is to carry out certain command periodically and maintain the switch configuration function seasonally. By configuring time list a time attribution list could be found, including start time , periodically time and end time. There are two kinds of time attribution, one begins when the switch starts, which is relative time; the other is the normal time, including year, month, day and so on, which is absolute time.

4.4.2 Task Scheduling Configuration

1. Setting task schedule:

Step	Command	Description
1	**config**	Enter global configuration mode

2	**schedule-list list-no start {up-time days time** *[every days time [stop days time]]* **|date-time** *date time [every {day|week|days time} [stop date time]]}*	Add or modify **sechedule-list** table. The command set the beginning time and end time of scheduling task, and the cycling interval. **list-no**: the range of scheduling list number<0-99>; **days time**: from the start-up time start, it is relative time; input format **days:** *<0-65535>*, **time: HH:MM:SS** such as 3 3:2:1 date time: the calculation of time is in accordance with the system data, it is absolute time; input format: **MMM-DD-YYYY HH:MM:SS**: like jan-1-2003 or 1-1-2003, the range of **YYYY** is from 1970 to 2199.
3	**command-string** *schedule-list* **list-no**	Add the commands that support **schedule-list** to the scheduling list. **command-string**: command string. **list-no**: list number range<0-99>
4	**show schedule-list**	Show **schedule-list** configuration。

4.4.3 Monitoring And Maintaining

Command	Description
show schedule-list	Show schedule-list configuration

4.4.4 Typical Configuration

First, add a **schedule-list** table, **List number:** 1, the beginning time is Feb-2-2004 0:0:0 according to system date, and perform every six days, while the terminal time is Feb-2-2005. Then, add the commands that support **schedule-list** to schedule list, and show the **schedule-list** configuration at last.

Raisecom#**config**

Raisecom(config)#**schedule-list** *1* **start date-time** *Feb-2-2004 0:0:0 every 6 0:0:0 stop Feb-2-2005 0:0:0*

Raisecom(config)#**storm-control dlf schedule-list** *1*

Raisecom(config)#**exit**

Raisecom# **show schedule-list**

4.5 Fault Location

4.5.1 Fault Location Principle

When anything abnormal happened in the system, fault location can be carried out by examining the facilities' running information, which includes the following contents:

- RAM using;
- port driver;

- process and stack state;
- port UP/DOWN statistics;
- the information needed for fault location.

4.5.2 Memory Show

Command	Description
show memory	Show the memory state

4.5.3 Port Driver Memory Pool Show

Command	Description
show buffer [port *<1-26>***]**	Show the port driver pool state; *<1-26>*: port range

4.5.4 Port UP/DOWN History

Command	Description
show diags link-flap	Show the UP/DOWN statistics

4.5.5 Fault Location Information Summarize Show

Command	Description
show tech-support	Show the fault location information summarize .

This command shows the information summarize for fault location, including:

- version (**show version**)
- running configuration information (**show running-config**)
- current CPU utilization (**show cpu-utilization**)
- memory usage (**show memory**)
- port driver pool usage (**show buffer**)
- processes (**show processes**)
- files in flash (**dir**)
- current system time (**show clock**)
- interface line/client state (**show interface line/client)**
- interface line/client statistics (**show interface line/client statistics)**
- port **UP/DOWN** statistics **(show diags link-flap)**
- SNMP statistics (**show snmp statistics)**
- spanning-tree in general (**show spanning-tree)**
- vlan statistics (**show vlan static)**
- ARP (**show arp)**
- trunk (**show trunk)**
- TCP link state

4.6 Ping Diagnose Function

4.6.1 Ping Principle

Ping is the most frequently-used command for troubleshooting, which is usually used to test if the link between the two hosts works. **Ping** is carried out by ICMP ECHO messages usually. It is made of ICMP reply and questioning messages, and if the network works well a reply messages will be received.

Ping can also be carried out through other paths, such as UDP, TCP and SNMP. In general, almost all the requests/replies can be used to acquire reply time. Usually, the ways except ICMP ECHO is used to settle the problem that some routers' no response or low response priority leads to the wrong answering time.

4.6.2 Ping Configuration

Test if the remote host is accessible.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** 0	Inter ip port mode
3	**ip address** *A.B.C.D [A.B.C.D] <1-4094>*	Configure the ip address on the switch A.B.C.D IP address [A.B.C.D] subnet mask <1-4094> vlan number
4	**exit**	Exit global configuration mode and enter privileged EXEC mode
5	**exit**	Exit privileged EXEC mode
6	**ping** *Ipaddress* **[count** *NumPktsRe***]** **[size** *SizeofIcmpeChPkt***]** **[waittime** *PktTimOut***]**	Test if the remote host is accessible *Ipaddress*: test the IP address A.B.C.D NumPktsRe: *Number of packets to receive* specify the package number before the **ping** program ends <1-65535> *SizeofIcmpeChPkt*: *Size of icmp echo packet* specify the size of the ICMP answering message<1-4096> *PktTimOut*: *Packet timeout in seconds* specify the time-out time of **ping** waiting for answer <1-100>, the unit is milliseconds

4.6.3 Typical Configuration Example

As is shown below, the host connects the switch with cable. User can confirm if the connection works through the command **ping**, while the switch is also able to transfer data to the host through **ping**.

1. Set the switch IP address as 20.0.0.10, the connection IP address as 10.168.0.221, the number of messages sent is 3, the message size is 100, waiting time 3. Because the destination IP address goes against the PC IP, the connection does not work.

Raisecom#**config**

Raisecom(config)# **int ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**exit**

Raisecom#**ping** *10.168.0.221* **count** *3* **size** *100* **waittime** *3*

Type CTRL+C to abort.

Sending 3, 108-byte ICMP Echos to 10.168.0.221 , timeout is 3 seconds:

UUU

no answer from 10.168.0.221

Ping unsuccessfully

2. connect PC, the IP address is 20.0.0.221, set the switch IP 20.0.0.10, connect success will be shown.

Raisecom#**config**

Raisecom(config)# **int ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**exit**

Raisecom#**ping** *20.0.0.10* **count** *3* **size** *100* **waittime** *3*

Type CTRL+C to abort.

Sending 3, 108-byte ICMP Echos to 20.0.0.221 , timeout is 3 seconds:

!!!

Success rate is 100 percent(3/3)

round-trip (ms) min/avg/max = 0/10/32

4.7 Tracerout Diagnose

4.7.1 Traceroute Principle

Traceroute, like **ping,** is a useful way of network management, which is use to find the route that the router

s and lines that the message actually passes.

L3 Traceroute is carried out by sending a group of incremental TTL probe packets. Probe packets work in the form of UDP or ICMP Echo. If only TTL>0, or a ICMP will be returned per hop to the destination. From this message the RRT of per hop on the way to destination.

4.7.2 Traceroute Configuration

Before L3 Traceroute is used, the IP address and default gateway of the switch need configuration first.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *0*	Enter IP configuration mode
3	**ip address** *A.B.C.D [A.B.C.D] <1-4094>*	Configure the IP address of the switch *A.B.C.D*: IP address *[A.B.C.D]*: subnet mask *<1-4094>*: vlan number
4	**exit**	Quit global configuration mode and enter privileged EXEC mode
5	**ip default-gateway** *A.B.C.D*	Configure the default gateway *A.B.C.D*: gateway number
6	**show int ip**	Show IP configuration
7	**show running**	Show default gateway configuration
8	**traceroute** *A.B.C.D* [**firstTTL** *<1-255>*] [**maxTTL** *<1-255>*] [**port** *<1-65535>*] [**waittime** *<1-60>*] [**count** *<1-10>]*	traceRoute show the route to destination *A.B.C.D*: IP address *firstTTL*: initialize TTL value *maxTTL*: maximize TTL value *<1-255>*: TTL value range *<1-65535>*: Port number range *<1-60>*: waiting time range *<1-10>*: count value

4.7.3 Typical Configuration Example

Example: set the IP address as 10.0.0.8, default gateway 10.100.0.1, trace the route to 58.63.236.42(www.sina.com.cn)

Raisecom#**config**

Raisecom(config)# **int ip** *0*

Raisecom(config-ip)#**ip address** *10.0.0.8 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**ip default-gateway** *10.100.0.1*

Raisecom(config)#**exit**

Raisecom#**Tracing** *the route to 58.63.236.42*

Type ctrl+c to abort.

1 10.0.0.1 10 ms 10 ms 10 ms

2 192.168.101.5 3 ms 3 ms 73 ms

3 192.168.101.5 10 ms 10 ms 10 ms

4 202.96.4.81 18 ms 16 ms 19 ms

5 202.106.228.177 9 ms 5 ms 12 ms

6 202.106.228.5 10 ms 8 ms 9 ms

7 202.96.12.25 7 ms 8 ms 5 ms

8 219.158.11.66 24 ms 20 ms 10 ms

9 202.97.15.57 101 ms 101 ms 126 ms

10 202.97.60.185 218 ms 222 ms 205 ms

11 202.97.40.58 119 ms 112 ms 113 ms

12 219.136.246.134 118 ms 142 ms 131 ms

13 219.136.246.6 138 ms 135 ms 110 ms

14 58.63.232.46 103 ms 115 ms 105 ms

15 58.63.236.42 199 ms 205 ms 197 ms

Trace complete.

4.8 Telnetd

4.8.1 Telnetd Principle

Telnet is the standard protocol and main way of remote login, which offers the ability of working on the local machine for remote host. The telnetd module in ROS4.0 implements the function of telnet server, letting telnet remote client login the facility so that it could be logged in and managed by telnet client.

4.8.2 Telnet Default Configuration

Function	Default value
Telnet server up-ling limit	5
telnet server link physical port	All the ports

4.8.3 Telnetd Configuration

1. Close telnet configuration

Step	Command	Description
1	**config**	Enter global configuration mode

2	**telnet-server close**	Telnet server close
	terminal-telnet *<1-5>*	<1-5> end telnet dialog number
3	**exit**	Return to privileged EXEC mode
4	**show telnet-server**	Show current telnet server configuration

2. Set the telnet server linking upper-limit

Step	Command	Description
1	**config**	Enter global configuration mode
2	**telnet-server max-session** *<0-5>*	Set the telnet server linking upper-limit <0-5> linking number
3	**telnet-server accept** *port-list* ***(****all****|{****1-MAX_PORT_STR****})***	Set the available port of the telnet server port-list: port list All: all the ports MAX_PORT_STR: port upper limit
4	**exit**	Return to privileged EXEC mode
5	**show telnet-server**	Show the current configuration of the telnet server
6	**Show information port**	Show information port

4.8.4 Typical Configuration Example

Set the linking upper limit of the telnet server as 3, open the available ports of Telnet server and show the current configuration.

Raisecom#**config**

Raisecom(config)#**telnet-server max-session** *3*

Set successfully

Raisecom(config)#**telnet-server accept port** *3*

Raisecom(config)#**exit**

Raisecom#**show telnet-server**

Max session: 3

Accept port-list: 1-26

4.9 Watchdog Function

4.9.1 Watchdog Principle

By configuring the watchdog software, the system program going into endless loop can be avoided, and the system stability will be better.

4.9.2 Configure Watchdog

Enable and Disable watchdog

Step	Command	Description
1	**watchdog** *{enable|disable}*	Enable: open watchdog Disable: close watchdog
2	**show watchdog**	Show watchdog state

4.9.3 Typical Configuration Example

Open watchdog and show the state

Raisecom#**watchdog** *enable*

Set successfully

Raisecom#**show watchdog**

Watchdog function: Enable

Chapter 5 Port Rate Limiting and Shaping

5.1 Port rate limiting and shaping principle

Line rate means rate limiting based on ports, which restricts the overall rate of the ports' receiving and sending messages. Line rate uses token bucket to control the rate. If some port of the facility is in rate limit, all the messages received or sent by the port need to be handled by token bucket. If there is enough token in token bucket, then messages can be received or sent, or it will be abandoned.

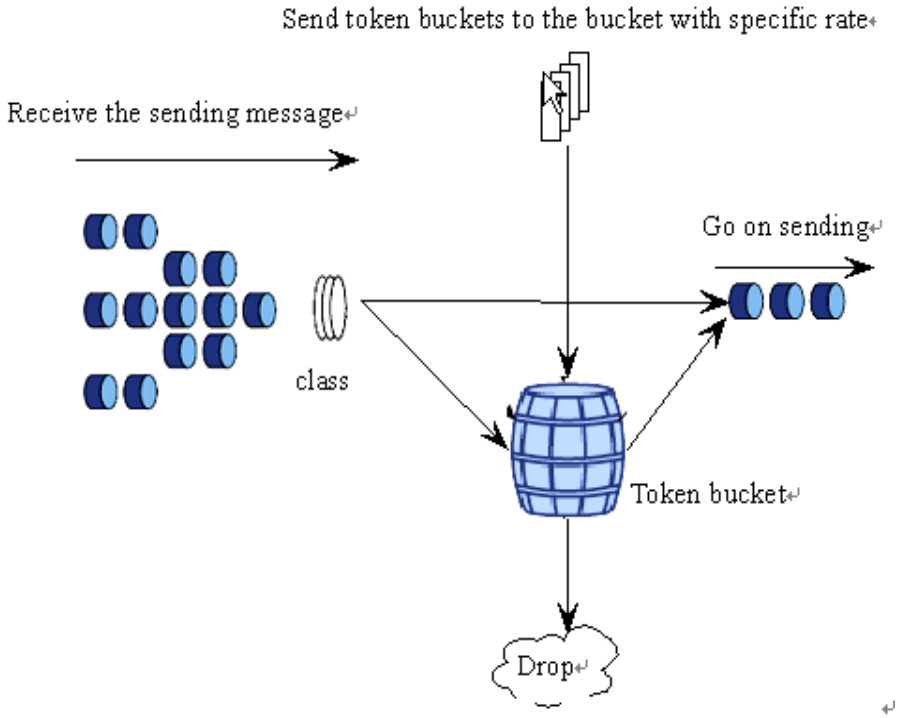


Fig 5-1 line rate process

Traffic shaping is used typically in confining the rate and limit of one stream in the output-network, so that this kind of message can be sent out steadily. Stream shaping is usually carried out by buffer and token bucket. When some groups' rate is too high, the message will be stored in buffer first, then it will be sent into the groups steadily.

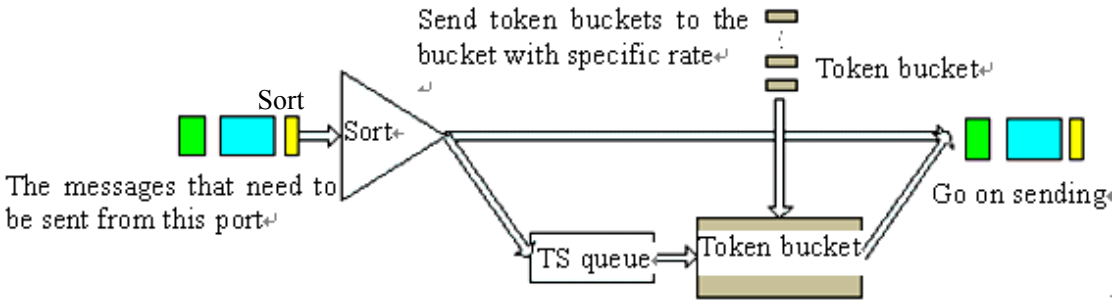


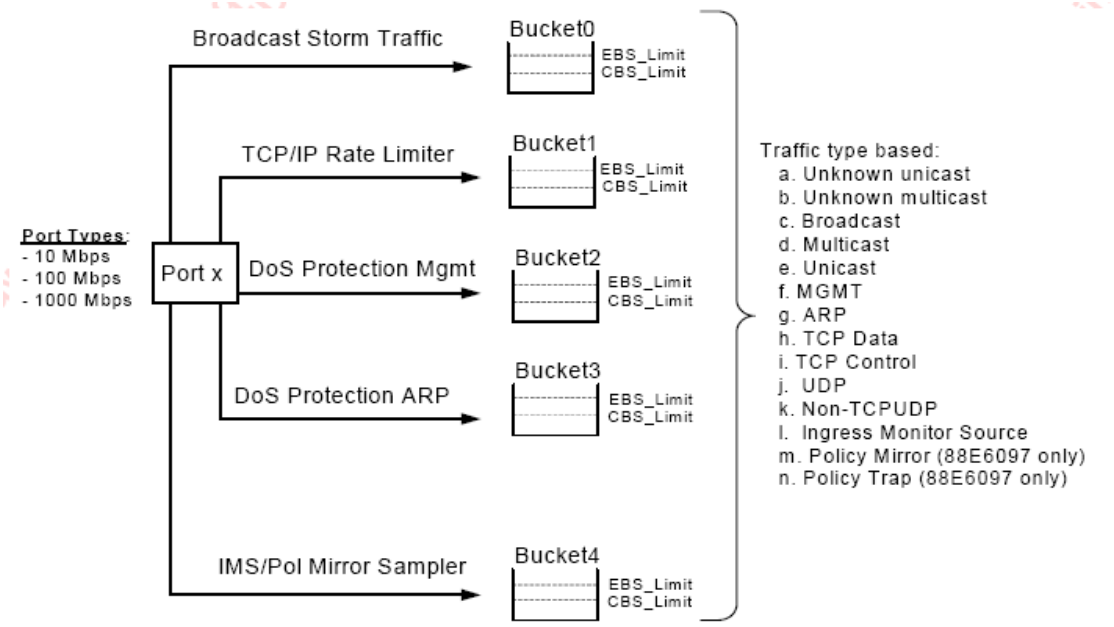
Figure 5-2 TS processing

TS can reshape given group stream or all the groups. When the groups come, it is classified first, and then continue transmission if there is no need for TS and token bucket. If TS is needed, the group will be compared with the token in token bucket. The token bucket put token in the bucket according to the rate that users set. If there is enough token for sending, the group will be sent, while the token number decreases according to the group length. When the token is the bucket is not enough for sending, the group will be stored in TS line. When there is group in the TS line, TS pick up one group and send it out periodically. Each sending will be compared with the token in the token bucket, until the token is not enough for the group in the line being sent out or all the groups in the line have been sent out.

For some purpose the bandwidth of the ports or VLAN needs to be confined. In this situation the bandwidth function needs to be configured that the port or VLAN bandwidth be confined in a range, the data that is over the bandwidth will be abandoned. By default, the ports and VLAN rate is auto negotiated, which need not to be confined.

The ingress port rate can be confined based on specified message and line priority. PIRL module uses speed confining resources to accomplish speed confining, aiming at the message type, message line privilege of the ingress port. Take MV6097 for example, this chip support 5 speed limitation resource every port, which is seized by global storm control, ports' message type and line privilege. Rate limitation is carried out by token bucket.

The model is as the following:



The speed limitation steps include: 64Kbps-1Mbps, the step is 64Kbps; 1Mbps-100Mbps, the step is 1Mbps; 100Mbps-1000Mbps, the step is 10Mbps.

Speed limitation aims at the following message type: ARP, TCP Data, TCP Ctrl, UDP, Non-TCPUDP, the line priority is 4. When the messages transmission speed exceeds the limit value, it can be abandoned or under traffic control.

5.2 Speed limitation and reshaping based on port function configuration

5.2.1. The default configuration

Function	Default value
The ingress port resource speed limitation message type, line priority calculation.	Or calculation relationship
When ingress port resource exceed the given speed limit	Drop drop
MAC no-speed limitation	Disabled
Port no-speed limitation function based on smac, dmac	Disabled

5.2.2. Port speed limitation and reshaping function

1. configure the ingress port bandwidth and burst:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rate-limit port-list** {**all** | *port-list*} **ingress** *rate* [*burst*]	Set the physical port bandwidth limit *port-list* physical port, ranging from 1 to the maximum number, use ‘,’and ‘-‘ for multi-port input: *rate* means the bandwidth, the unit is kbps, from 1 to 1048576. *burst* the burst, unit Kbps, can be set from 1 to 512. The actual value may be different from the value setting; *ingress* the ingress direction
3	**exit**	Quit global configuration mode and enter EXEC privileged mode
4	**show rate-limit port-list** [*port-list*]	Show port bandwidth limitation. *port-list* is accord with the meaning above.

What’s special, the specified message and queue priority speed limitation can be set.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rate-limit port-list** *portlist* **ingress** *<1-1000000>* **queue-priority** {*1-4*}	Configure the port number, speed limitation value and message queue priority; *Portlist* is the physical port, the range is 1 to the maximum number, use ‘,’ and ‘-‘ to carry out multi-port input; 1-1000000 is the ingress port bandwidth, the unit is kbps; 1-4 means queue priority.

3	**rate-limit port-list** *portlist* **ingress** <*1-1000000*>	Configure the speed configuration port and value; *Portlist* means the physical port, the range is 1 to max no.; use ',' and '-' to carry out multi-port input. 1-1000000: ingress port bandwidth, the unit is kbps;
4	**rate-limit port-list** *portlist* **ingress** <*1-1000000*> [**arp**] [**tcp-data**] [**tcp-ctrl**] [**udp**] [**non-udptcp**]	Configure the speed configuration port and value; *Portlist* means the physical port, the range is 1 to max no.; use ',' and '-' to carry out multi-port input. 1-1000000: ingress port bandwidth, the unit is kbps; arp: arp messages tcp-data: tcp data; message; tcp-ctr:tcp control message; udp: udp message; non-udptcp: includes IGMP, ICMP, GRE, IGRP, cisco, L2TP message;
5	**rate-limit port-list** *portlist* **ingress** <*1-1000000*> **queue-priority** {*1-4*} {**and**|**or**} [**arp**] [**tcp-data**] [**tcp-ctrl**] [**udp**] [**non-udptcp**]	Configure the speed configuration port and value; *Portlist* means the physical port, the range is 1 to max no.; use ',' and '-' to carry out multi-port input. 1-1000000: ingress port bandwidth, the unit is kbps; *or:* calculation type; and calculation type: the ingress message; arp: arp message; tcp-data: tcp-data message; tcp-ctr: tcp control message; udp: udp message; non-udptcp: includes IGMP, ICMP, GRE, IGRP, cisco, L2TP message;
6	**exit**	Return to EXEC privileged mode;
7	**show interface line/client** *port_id* **rate-limit**	Show PIRL configuration information *port_id* port ID

Notice: PIRL (Port Ingress Rate Limiting) module confines the ingress port value in the following range: mega port <64-100000>kbps, giga port <64-100000>kbps; when the mega port configuration value exceeds 100000kbps, it will be set as 100000kbps. If there is no specified speed limitation message or message queue priority, all the messages will be limited. The configuration value might be different from the actual value, which is decided by the chip.

In PIRL module, when the speed limited message transmission speed exceeds the speed limitation, use **drop** and sending pause frame to handle it.

The configuration step is show as following:

Step	Command	Description
1	**config**	Enter global configuration mode;

2	**interface line/client** *<1-MAX_PORT_NUM>*	Enter Ethernet physical port mode; MAX_PORT_NUM the maximum port number that the equipment support;
3	**[no] rate-limit flow-control**	Configure flow-control mode, by default it is drop mode ;
4	**exit**	Return to EXEC privileged mode
5	**show interface line/client** *port_id* **rate-limit**	Show PIRL configuration information; *port id*: port number

In PIRL mode, the specified MAC speed no-limitation is available only to the messages that has already entered the switch; if it fits the static MAC configuration, then there will be no such message speed limitation.

The configuration step is show as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mac-address-table static unicast** *HHHH.HHHH.HHHH* **vlan** *vlan_id* **port** *port-number* **none-rate-limit**	Configure the static MAC no-speed limitation function; *HHHH.HHHH.HHHH* static MAC address; Vlan id: VLAN ID, the range is 1~4094; *port-number* port number, the range is from 1to the maximum port number;
3	**exit**	Return to EXEC privileged mode
4	**show mac-address-table static**	Show MAC strategy configuration.

Open/close no-speed limit function based on **smac, dmac**, the configuration step is show below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface line/client***<1-MAX_PORT_NUM >*	Enter Ethernet physical port mode; *1-MAX_PORT_NUM* the port range that the equipment supports
3	**[no] rate-limit** {**smac**|**dmac**} **none-rate-limit**	Configure the no-speed limit function based on **smac,damc**;
4	**exit**	Return to global configuration mode
5	**show interface line/client** *port_id* **rate-limit**	Show PIRL configuration information; *Port id* port ID

2. Configure the ingress port bandwidth and burst:

Step	Command	Description
1	**config**	Enter global configuration mode

2		Configure the rate limiting.
	rate-limit port-list {**all** | *port-list*} **egress** *rate* [*burst*]	*port-list* physical port number, range is 1-26, use "," and "-" for multiple ports' rate limiting. *rate* stands for the maximum bandwidth allowed to be transmitted, unit is kbps, range is 1-1048576. (The actual value may be a little bit different from the configured value because it can only be the exponential of 2). *burst*: the configured bandwidth. Unit is KBps, the available value is 1-512. *The real value can be different with the configured value.* *egress:* the out traffic
3	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
4	**show rate-limit port-list** [*port-list*]	Show the rate limiting of the port *port-list* physical port number, range is 1-26,use "," and "-" for multiple ports configuration.

To delete port speed limitation, use global configuration command **norate-limit port-list {all|***port-list***} {both | ingress | egress}**

5.2.3. Monitoring and maintaining

Use **show** to look over the switch's configuration and states of port speed limitation and PIRL function for the convenience of monitoring and maintaining. The relative command is show below:

Command	Description
show interface line/client *port_id* **rate-limit**	Show PIRL configuration
show mac-address-table static	Show MAC strategy configuration
show rate-limit port-list [*port-list*]	Show the port bandwidth limitation *port-list* strands for physical port number, range is 1-26, use ',' and '-' for multi-port ingress

5.2.4. Typical configuration example

- Aim

Configure the uplink bandwidth of the sw1's port 1 as 1000kbps, burst 64kbps, port 2 fits message **arp** and speed limit at message priority level 1-2, the speed limit value is 1000Kbps, open port 2 traffic control mode, so that the switch could manage the network traffic.

- Network structure:

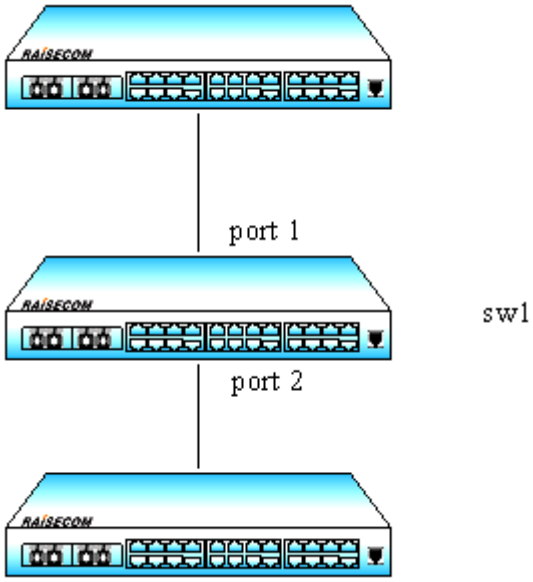


Figure 5-4 network structure

- Configuration step:

Step 1:

Raisecom#**config**

Raisecom(config)# **rate-limit port-list** *1* **ingress** *1000 64*

Set successfully

Actual ingress rate of FE port: 1000

Actual ingress burst of FE port: 64

*Raisecom(config)#**exit***

Raisecom# show rate-limit port-list 1

I-Rate: Ingress Rate

I-Burst: Ingress Burst

E-Rate: Egress Rate

E-Burst: Egress Burst

Port I-Rate(Kbps) I-Burst(KBps) E-Rate(Kbps) E-Burst(KBps)

---

1 1000 64 0 0

Step 2:

Raisecom(config)# **rate-limit port-list** *2* **ingress** *100* **queue-priority** *1-2* **and arp**

Set successfully

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)# **rate-limit flow-control**

Set successfully

Raisecom#**show interface line/client** *2* **rate-limit**

port: 2

flow-control: Enable

smac-none-limit-rate: Disable

dmac-none-limit-rate: Disable

session CIR(kbps) BA(kBps) rate-limit-operation queue-priority traffic-type

---

1 100 128 and 1 2 arp

5.3 Speed limitation and reshaping function based on VLAN configuration

5.3.1 The default configuration

By default, there is no bandwidth limit based on VLAN.

5.3.2 Speed limitation and reshaping function based on VLAN configuration

1. Configure speed limitation based on VLAN:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rate-limit vlan** *<1-4094> rate burst*	Set the traffic limitation based on VLAN. *<1-4094>*:VLANID; *Rate* strands for the bandwidth limitation based on VLAN, the unit is kbps, range is 1-1048576. The actual value may be different from the configured one. *burst* configured burst, the unit is Kbps,
3	**exit**	Exit from global configuration and enter EXEC privileged mode
4	**show rate-limit vlan**	Show the port speed limitation

2. configure the bandwidth and burst based on QinQ VLAN

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rate-limit double-tagging-vlan outer** {*<1-4094>*|**any**} **inner** {*<1-4094>*|**any**} *rate burst*	Configure the bandwidth limit based on QinQ VLAN; **outer** *{<1-4094>|any}* outer layer VLAN, *any* strands for any outer layer VLAN; **inner** *{<1-4094>|any}* lining VLAN, *any* strands for

		any outer layer VLAN; *rate* strands for the configured bandwidth value, the unit is kbps, range is 1-1048576,the actual value may be different from the configured value. *burst* the configured burst, the unit is kbps, the value can be set from 1 to 512. The actual value may be different from the configured value.
3	**exit**	Exit from global configuration mode and enter EXEC privileged mode.
4	**show rate-limit vlan**	Show the port bandwidth limitation.

Notice: The outer layer VLAN can not be un-assigned at the same time.

5.3.3 Monitoring and maintaining

Using **show,** the switch's VLAN speed limit configuration and state can be shown for the convenience of monitoring and maintaining. The related command is shown below:

Command	Description
show rate-limit vlan	Show the port bandwidth limitation.

5.3.4 Typical configuration example

- Aim

Set the switch's VLAN 5 bandwidth as 2048kbps, the burst is 128kbps;

Set the outer layer VLAN as 6, lining VLAN as 10, the bandwidth 1024kbps, the burst 64kbps, to accomplish VLAN management.

- Configuration step:

Step 1:

Raisecom#**config**

Raisecom(config)# **rate-limit vlan** *5 2048 128*

Set successfully

Actual rate: 2048

Actual burs: 128

Step 2:

Raisecom(config)# **rate-limit double-tagging-vlan outer** *6* **inner** *10 1024 64*

Set successfully

Actual rate: 1024

Actual burs: 64

Raisecom(config)#**exit**

Raisecom# **show rate-limit vlan**

CVLAN: Customer VLAN(inner VLAN)

SPVLAN:Service provider VLAN(outer VLAN)

Type	*CVLAN*	*SPVLAN*	*Rate(Kbps)*	*Burst(KBps)*
single	*5*	*--*	*2048*	*128*
double	*10*	*6*	*1024*	*64*

Chapter 6 MAC Address Transmission Table

6.1 MAC transmission table management introduction

6.1.1. MAC address transmission table

The Ethernet switch's main function is to transmit message in data link layer, that is to transmit messages to the corresponding port according to the destination MAC address. MAC address transmission table is a two-ply table that contains MAC address and transmission port matchup, which is the base of the Ethernet switch transmitting two-ply messages.

MAC address transmission table contains the following information:

- The destination MAC address;
- The VLAN ID belongs to the port;
- The transmission egress port number of the local equipment;

When the Ethernet switch is transmitting messages, according to the MAC address table information, the following way is available:

- Unicast: when there is table item that fits the message destination MAC address in the MAC address transmission table, the switch will transmit it directly from the transmission egress port of the table item;
- Broadcast: when the messages that the switch received from the destination address are all F, or when there is no table item that is accord with the message destination MAC address in the MAC address transmission table, the switch will use broadcast and transmit the message to all the ports except the receive ports.

6.1.2. MAC address learning

The table item in MAC address table can be upgraded and maintained through the following two ways:

- Manual configuration
- MAC address learning

Usually, most MAC address is created and maintained by the MAC address function. The Ethernet switch learning MAC address process is shown below:

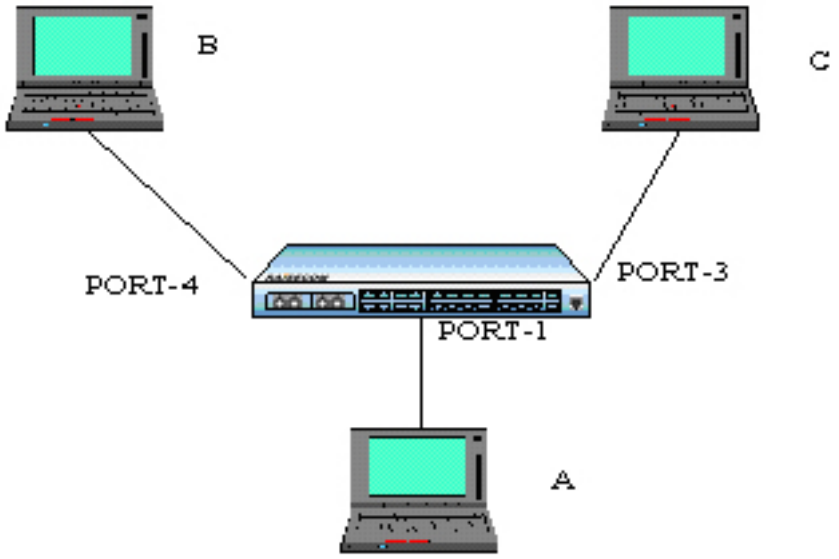


Fig 1 Mac address learning

When User A need to communicate with User B in the same VLAN1, the message need to be sent to the switch's port 1, while the switch record the message's source MAC address, or User A's address 'MAC-A', to its own MAC address transmission table.

When the learning process is done, the switch will transmit the message. Because there is no MAC address and port table item, the switch will transmit the message to all the port except port 1 to confirm that User B could receive the message;

Because the switch use broadcast to transmit the message, both User B and User C will receive the message, while User C is not the destination equipment, so he will not process it. Normally, User B will respond User A by sending messages. When the response message is sent to port 4, the switch will use the same MAC address learning way and save User B's address and port corresponding relationship in the MAC address transmission table.

By this time there will be two table item in the switch's transmission table. When transmitting response message, because there has already been the table item that the destination is 'MAC-A' in the MAC address transmission table, the switch will no longer use broadcast, but send the message directly to User A through port 1 to accomplish the message interaction.

The way above is independent MAC address learning, or IVL, while there is another way for learning MAC address, that is share-VLAN MAC address learning, or SVL. By default, the switch use IVL mode, and SVL mode needs to be set in some cases.

6.1.3. MAC address table management

1. MAC address transmission table aging mechanism:

The switch MAC address transmission table has limitation in capacity, so it use aging mechanism to refresh the MAC address transmission table to make full use of the address transmission table resource. That is, the system open the aging timer when it is creating one table item dynamically, and if there is no more messages received from the MAC address of the table item in the aging time, the switch will delete the MAC address table item.

Notice:

- When 'destination MAC address refresh' function is enabled, if the switch transmits a message which the destination is one MAC address in the aging time, the MAC table item will be refreshed, and restart aging;
- MAC address aging mechanism is valid only to dynamic MAC address table item.

2. MAC address table sorts and features:

- Static MAC address table item: or 'permanent address', it is added or deleted by user, without aging. For a network in which the equipments change rarely, manually adding static address table item can reduce the network broadcast traffic.
- Dynamic MAC address table item: it stands for the MAC address table item that ages according to the aging time that user set. The switch could add dynamic MAC address table item through MAC address learning mechanism or user handwork.

6.2 MAC address transmission table management configuration

6.2.1 The default MAC address transmission table configuration

Function	Default value
MAC address aging time	300s
MAC address learning feature	Enable
Static MAC address privilege	-1（N/A in command lines）
Static MAC address MAC strategy	Transmit normally
Static MAC address no-speed-limit	enable

6.2.2 Static MAC address configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mac-address-table static unicast** *HHHH.HHHH.HHHH* **vlan** *vlan id* **port** *port-number*	Set the static MAC address. *HHHH.HHHH.HH*HH is the static MAC address which will be set; format is hex, dotted notation for every four characters. Vlan_id range is 1-4094. *port_number* is the physical port number.
3	**mac-address-table static multicast** *HHHH.HHHH.HHHH* **vlan** *vlan_id* **port** *port-list*	Set the static MAC address. *HHHH.HHHH.HHHH is the static MAC address which will be set; format is hex,* dotted notation for every four characters. Vlan_id range is 1-4094. *port_number* is the physical port number, range is 1-26, use ',' or '-' to input the port list.
4	**exit**	Exit global configuration mode and enter privileged EXEC mode

5	**show mac-address-table static** [**port** *port-number* | **vlan** *vlan_id*]	Show (port or VLAN) static address. *port_number* is physical port, range is 1-26. *vlan_id:* range is 1-4094.

Note: The switch MAC address, multicasting address, FFFF.FFFF.FFFF and 0000.0000.0000 can not be configured as the static MAC address.

6.2.3 MAC address aging time configuration

The dynamic source MAC address that the switch has learned will age when it is not in use. The aging time can be changed, and the MAC address aging can be disabled. By default, the aging time is 300s.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mac-address-table aging-time** {*0* | *time*}	Set the aging time of MAC address table. 0 stands for MAC address will not be aged *time* is the target MAC address aging time, unit is second, range is 3-765, and default value is 300.
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show mac aging-time**	Show MAC address aging time

To Restore the default value, use the command **no: no mac-address-table aging-time**.

6.2.4 MAC address learning enable/disable

Sometimes disable/enable a certain physical port learning MAC address is needed, which can be achieved by configuring the switch of MAC address learning ability. By default, every physical port can be allowed to learn MAC address.

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**mac-address-table learning** {**enable**|**disable**} **port-list** {**all**|{1-26}}	Enable or disable the MAC address learning function of physical port. **enable** enable MAC address learning function. **disable** disable MAC address learning function. *MAX_PORT_NUM* the maximum port number that the equipment support
3	**exit**	Exit from global configuration mode to privileged EXEC mode.
4	**show interface line/client** [*port-number*]	Show port status. *port_number physical port*,range is 1-26.

6.2.5 Clear MAC address table

Clear layer-2 MAC address table entries of the switch, includes static and dynamic MAC address. The command can be used in global configuration mode.

Step	Command	Description
1	**clear mac-address-table** {*all*|*dynamic*|*static*}	**all:** delete all the 2 MAC addresses in the MAC address table **dynamic:** delete dynamic MAC addresses in the MAC address table **static:** delete static MAC addresses in the MAC address table

6.2.6 Configure static MAC address privilege

The static MAC address privilege value range is 0~7, the default value is -1, and the command line shows N/A when it is -1.

The configuration step is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mac-address-table static unicast** *HHHH.HHHH.HHHH* **vlan** *vlan_id* **port** *port-number* **[priority** <*0-7*>**]**	Set static MAC address *HHHH.HHHH.HHHH* is the static MAC address which will be set; format is hex, dotted notation for every four characters. *vlan_id* VLAN ID, range is 1~4094. *port_number* physical port number configure the privilege value, range is 0~7
3	**exit**	Quit global configuration mode and enter privileged EXEC mode.
4	**show mac-address-table static** [**port** *port-number* | **vlan** *vlan_id*]	Show (port or VLAN) static address *port_number* physical port number *vlan_id* VLAN ID, range is 1~4094.

To restore static MAC address default privilege (-1), use **no: no mac-address-table static unicast** HHHH.HHHH.HHHH **vlan** vlan id **priority.**

6.2.7 enable/disable static MAC strategy

Static MAC address MAC strategy includes normal transmission (default), mirror and drop, all of which are based on port. This command enable global switches.

The step is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode

		Set static MAC configuration
2	**mac-address-table static unicast** *HHHH.HHHH.HHHH* **vlan** *vlan_id* **port** *port-number* **[mac-policy]**	*HHHH.HHHH.HHHH* static MAC address which is to be set, format is hex, dotted notation for every four characters.
		vlan_id VLAN ID, range is 1~4094.
		port_number physical port number
		mac-policy enable MAC strategy.
3	**exit**	Quit global configuration mode and enter privileged EXEC mode.
		Show (port or VLAN) static address
4	**show mac-address-table static** [**port** *port-number* | **vlan** *vlan_id*]	*port_number* physical port number
		vlan_id VLAN ID, range is 1~4094.

To close static MAC address MAC strategy default configuration, use **no: no mac-addresss-table static unicast** HHHH.HHHH.HHHH **vlan** vlan id **mac-policy.**

6.2.8 Enable/disable static MAC address non-rate-limit

Static MAC address can be set non-rat-limit. To the given MAC address, with non-speed-limit configuration, the messages into the MAC address have no speed limit.

Step	Command	Description
1	**config**	Enter global configuration mode
		Set static MAC configuration
2	**mac-address-table static unicast** *HHHH.HHHH.HHHH* **vlan** *vlan_id* **port** *port-number* **[non-rate-limit]**	*HHHH.HHHH.HHHH* static MAC address which is to be set, format is hex, dotted notation for every four characters.
		vlan_id VLAN ID, range is 1~4094.
		port_number physical port number
		non-rate-limit non-rate-limit feature
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
		Show (port or VLAN) static address
4	**show mac-address-table static** [**port** *port-number* | **vlan** *vlan_id*]	*port_number* physical port number
		vlan_id VLAN ID, range is 1~4094.

To close static MAC address non-rate-limit, use **no: no mac-address-table static unicast** HHHH.HHHH.HHHH.HHHH **vlan** vlan_id **non-rate-limit**

6.2.9 Monitoring and maintaining

Use **show** to look over MAC address transmission table configuration:

Command	Description

show mac aging-time	Show MAC address aging time
show mac-address-table l2-address port *port-number*	Show the switch port MAC address *Port_number* physical port, range is 1~26
show mac-address-table l2-address vlan *vlan_id*	Show the switch port MAC address *vlan_id* VLAN ID, range is 1~4094
show mac-address-table l2-address count port *port-number*	Show the switch port MAC address number **Count** stands for the MAC address number related to the statistics *port_number* physical port number, range is 1~26.
show mac-address-table l2-address count vlan *vlan_id*	Show the switch VLAN MAC address **Count** stands for the MAC address number related to the statistics *vlan_id* VLAN ID, range is 1~4094
show mac-address-table static	Show the switch static MAC address configuration information
show mac-policy portlist *portlist*	Show the MAC strategy of each port

Especially, the command for searching the information of a certain MAC address in the switch.

Command	Description
search mac-address *HHHH.HHHH.HHHH*	Search for MAC address *HHHH.HHHH.HHHH* static MAC address which is to be set, format is hex, dotted notation for every four characters.

6.2.10 Typical configuration example

- Destination:

Enable all the ports' MAC address learning function of the switch;

Configure a static unicast MAC address 1234.1234.1234 in port 2, VLAN 10;

Set the aging time 100s, observe the switch MAC address learning and aging situation.

- Network figure

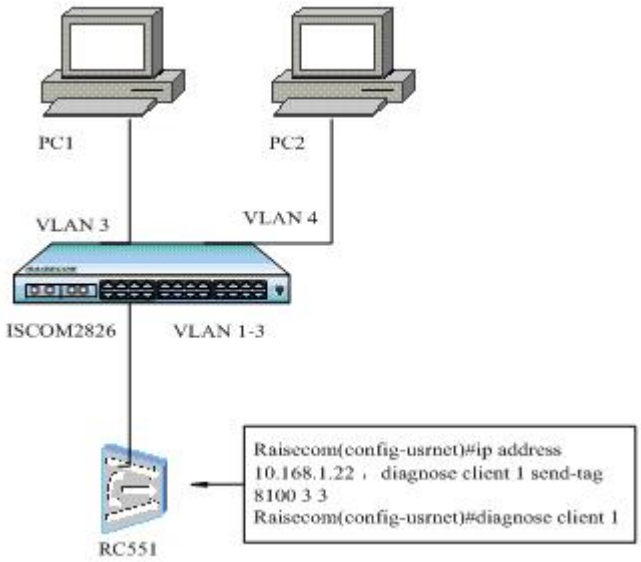


Fig 6-2 network

- Configuration step

Step 1:

Enable all the ports' MAC address learning function

Raisecom(config)#**mac-address-table learning** *enable* **port-list** *all*

Step 2:

Set static unicast MAC address 1234.1234.1234.1234 in port 2, VLAN 10

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)#**switchport access vlan** *10*

Raisecom(config)#**mac-address-table static unicast** *1234.1234.1234* **vlan** *10* **port** *2*

Step 3:

Set the aging time as 100s

Raisecom(config)#**mac-address-table aging-time** *100*

We can notice that the switch can learn 2 dynamic MAC address through port 2, which age 100s later, then restart learning, while static MAC address will no age.

6.3 MAC address number limit

With MAC address learning function, the Ethernet switch can get the MAC address within the same network segment. To the message that is sent to the MAC addresses, the Ethernet switch use hardware for transmission through looking for MAC address transmission table to raise the transmission efficiency. If the MAC address transmission table is much too large, the time of looking for the corresponding transmission table item may be prolonged, and the switch transmission function will drop. By configuring the maximum MAC address number that the Ethernet port can learn, the administrator is able to control the MAC address transmission table item number that the Ethernet switch maintains. When the MAC address number that the

port has learned rises to the maximum value that user set, the port will no longer learn MAC address.

6.3.1 Configure the default MAC address number limit

By default, the MAC address learning number has no upper limit.

6.3.2 Configure the MAC address number

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface { port | line | client}** *<1-MAX_PORT_NUM >*	Enter Ethernet physical port mode
3	**mac-address-table threshold <** *PORT_MAC_MIN_THRESHOLD_STR - PORT_MAC_MAX_THRESHOLD_STR***>**	Configure the MAC address learning upper limit *PORT_MAC_MIN_THRESHOLD_STR* value upper limit *PORT_MAC_MAX_THRESHOLD_STR* value lower limit
4	**exit**	Quit global configuration mode and enter privileged EXEC mode
5	**show interface mac-address-table threshold**	Show interface mac address table threshold value

6.3.3 Monitoring and maintaining

Command	Description
show interface mac-address-table threshold	Show interface MAC address table threshold value
Show mac-addres l2	Show interface MAC address number that has been learned

6.3.4 Typical configuration example

- Destination

Configure the MAC address learning threshold of the switch port as 1, and the switch won't learn the dynamic MAC address that extend the threshold value.

- Network

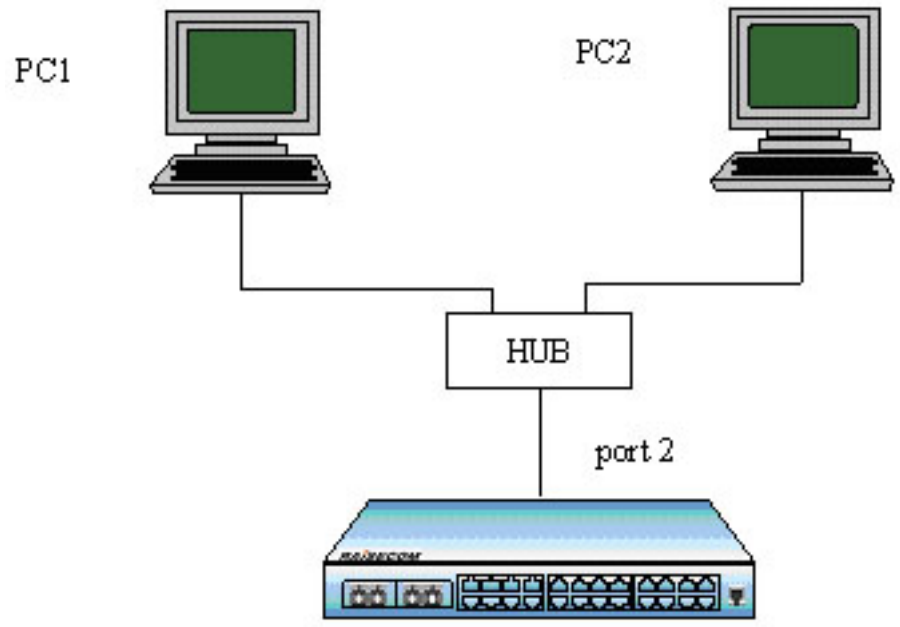


Fig 6-3 Network

- Configuration step

Step 1:

The upper limit of port 2 learning MAC address is 100

Raisecom(config-port)#**mac-address-table threshold** *1*

Step 2:

Show interface MAC address learning number:

Raisecom# **show mac-address-table** *l2*-**address count port** *1*

Port 2 shows only 1 dynamic MAC is learned.

Step 3:

Cancel the MAC learning confirmation of port 2

Raisecom(config-port)#**no mac-address-table threshold**

Show interface MAC address learning number:

Raisecom# **show mac-address-table** *l2*-**address count port** *1*

Port 2 shows there are 2 dynamic MAC that has been learned.

6.4 Shared VLAN learning function

6.4.1 The default SVL configuration

Function	Default value
SVL feature	Disabled

Interface SVL default VLAN list	Empty
SVL default VLAN	VLAN 1

6.4.2 SVL configuration

The step is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**svl** {*enable* | *disable*}	Enable/disable SVL mode
3	**interface line/client** *<1-MAX_PORT_NUM>*	Enter port configuration mode *1-MAX_PORT_NUM* the port number that the equipment supports
4	**switchport svl vlanlist** {*1-4094*}	Optical Set the shared VLAN list of the port
5	**exit**	Enter global configuration mode
6	**svl default vlan** <*1-4094*>	Set SVL default VLAN *1-4094*:VLAN ID
7	**exit**	Quit global configuration mode and enter privileged EXEC mode
8	**show svl**	Show SVL state
9	**show switchport [**<*1-MAX_PORT_NUM*>**] svl vlanlist**	Show interface shared VLAN list *1-MAX_PORT_NUM* the port number that the equipment supports
10	**show svl default vlan**	Show SVL default VLAN

Notice: When some port is not configured the SVL VLAN list, the MAC will be shared to SVL default VLAN.

6.4.3 Monitoring and maintaining

Command	Description
Show svl	Show SVL state
show switchport [<*1-MAX_PORT_NUM*>**] svl vlanlist**	Show interface shared VLAN list *1-MAX_PORT_NUM* the port number that the equipment supports
Show svl default vlan	Show SVL default VLAN

6.4.4 Typical configuration example

- Destination

Enable the switch SVL function, and share the MAC address learned in port 1 between VLAN 1-4;

- Configuration step

Step 1:

Enable SVL mode

Raisecom # **config**

Raisecom (config)# **svl** *enable*

Raisecom (config)# **exit**

Raisecom # **show svl**

SVL: Enable

Step 2:

Set port 1 shared VLAN 1-4

Raisecom#**config**

Raisecom(config)#**interface line/client** *1*

Raisecom(config-port)# **switchport svl vlanlist** *1-4*

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

Raisecom(config)#**exit**

Raisecom# **show switchport** *1* **svl vlanlist**

Port SVL VLAN list

---

1 1-4

Chapter 7 Interface Configuration Guide

7.1 Physical ports features

For a switch, whatever the equipment is, physical interface is necessary for connection. And physical ports have many features, any message that is entering or leaving the switch needs physical ports to transmit, so the function of physical port is relatively more difficult, which is also very important; to some of the function manual configuration is available, like port rate, duplex mode, negotiation mode, crossover cable automatic recognization and system maximum transmission unit, all of which are the features of the physical ports. To the certain use, the corresponding setting is needed for the physical port to receive or transmit messages.

7.2 The default configuration for physical ports

By default, the physical port commands is shown below:

Command	Default value
Rate configuration	The rate of electronic port and 100M optical port is auto negotiated, 100M iptical port rate is 100M by default
Duplex mode configuration	The rate of electronic port and 100M optical port is auto negotiated, 100M optical port in duplex is full duplex
Rate control configuration	Physical port rate control function is off
Crossover Ethernet cable auto-recognization and straight Ethernet cable function	Normal mode
Port maximum transmission unit	1522 byte
Interface on/off configuration	on

7.3 Rate and duplex mode configuration

Gigabit port is always working in 1000Mbps and full duplex mode. When auto negotiation function is enabled, the duplex mode (speed) will be set according to the result auto negotiation. In default situation, auto negotiation is enabled for all the electronic ports and 1000M optical port, only the default value of 100M optical port is 100M/FD.

Rate and duplex mode configuration step is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode.

2	**interface line/client** *port-number*	Enter Ethernet physical interface configuration mode. *port_number* is the physical interface, range is 1-26. *port-list r*ange is 1-26, use "," and "-"for multiple interfaces configuration.
3	**speed** *{auto|10|100|1000}* **duplex** *{full|half}*	Set the speed and duplex mode of the port. *auto*: represents that both the speed and duplex are set according to the result of auto negotiation. *10*: represents that the speed is set to 10Mbps. *100*: represents that the speed is set to 100Mbps. *1000*: represents that the speed is set to 1000Mbps. *full*: set the duplex mode to full duplex. *half*: set the duplex mode to half duplex.
4	**exit**	Exit from Ethernet physical interface configuration mode to global configuration mode.
5	**exit**	Exit from global configuration mode to privileged EXEC mode
6	**show interface line/client** *port-number*	Show the status for the port. *port_number* physical port, range is 1-26.

Note:

- Using the Ethernet interface configuration mode **speed auto**, the rate and duplex mode will be restored to auto negotiation by default.
- Different ports fit different rate and duplex mode. 100M electronic ports can not be set to 1000M, 100M optical port can be set to 100M/FD only, 1000M optical port can be only configured 1000M/FD/auto, while extended card port can not be configured rate and duplex mode when the extended card does not exist.

Example 1: set the speed of port 15 to 10Mbps, duplex mode is full duplex.

Raisecom#**config**

ISCOM2826(config)#**interface line/client** *15*

ISCOM2826(config-port)#**speed** *10*

ISCOM2826(config-port)# **duplex** *full*

ISCOM2826(config-port)#**exit**

ISCOM2826(config)#**exit**

Raisecom#**show interface line/client** *15*

R: Receive Direction

S: Send Direction

Port Admin Operate Speed/Duplex Flowcontrol(R/S) Mac-learning

---

15 enable down 10/full off/off enable

Example 2: set the rate of 100M optical port to 10Mbps, duplex mode is half-duplex.

Raisecom#**config**

Raisecom(config)#**interface line/client** *1*

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

Port 1 only supports 100M/FD!/ port1 support only100M/FD!

Raisecom(config-port)# **duplex** *half*

Port 1 only supports 100M/FD!/ port1 support only 100M/FD!

Example 3: set 1000M optical port P2 to 100Mbps, duplex mode is half-duplex

Raisecom#**config**

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)#**speed** *100*

Port 2 only supports 1000M/FD or auto-negotiation!/ port 2 support only 100M/FD or auto negotiation.

Raisecom(config-port)# **duplex** *half*

Port 2 only supports 1000M/FD or auto-negotiation!/ port 2 support only 100M/FD or auto negotiation.

Example 4: set 100M electronic port P3 to 1000Mbps

Raisecom#**config**

Raisecom(config)#**interface line/client** *3*

Raisecom(config-port)#**speed** *1000*

Port 3 does not support 1000M!/port 3 do not support 1000M!

Example 5: set extended card P25 to 1000Mbps

Raisecom#**config**

Raisecom(config)#**interface line/client** *25*

Raisecom(config-port)#**speed** *1000*

Port 25 is unavailable!/ port 25 does not exist.

7.4 Configure IEEE 802.3X flow control function

The flow control function of Raisecom series switches is set on both RX and TX direction, that is to say, you can set the interface's ability to receive and send pause frame to on/off separately. By default, flow control function is disabled on both directions. For extended card port, if there is no corresponding extended card inserted, the flow control commands fail.

Step	Command	Description
1	**config**	Enter global configuration mode

2	**interface line/client** *port-number*	Enter Ethernet physical interface configuration mode. *port_number* physical ports, range is 1-26. *port-list*, range is 1-26,use "," and "-" for multiple ports.
3	**flowcontrol** *{receive|send}{on|off}*	Enable/disable the flow control function on RX and TX direction. Send represents the traffic control function at TX direction. *receive:* represents the traffic control function at RX direction. *on:* enabe the flow control function of the port. *off:* disable the flow control function of the port.
4	**exit**	Exit from the physical interface configuration mode and enter global configuration mode.
5	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
6	**show interface line/client** *port-number*	Show the traffic control of the port. *port_number* physical port number, range is 1-26.

Example 1: Set the flow control for port 10.

Raisecom#**config**

ISCOM2826(config)# **interface line/client** *10*

ISCOM2826(config-port)#**flowcontrol receive** *on*

ISCOM2826(config-port)#**exit**

ISCOM2826(config)#**exit**

Raisecom#**show interface line/client** *10*

R: RX Direction

S: tx Direction

Port Admin Operate Speed/Duplex Flowcontrol(R/S) Mac-learning

---

10 enable down auto on/off enable

Example 2: set the extended card P25 flow control function on.

Raisecom#**config**

Raisecom(config)#**interface line/client** *25*

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

Port 25 is unavailable! /port 25 does not exist!

For some equipment, the flow control situation of the ports' receiving direction and sending direction is configured respectively. By default all the ports' flow control is off.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface line/client** *port-number*	Enter physical port mode. *port_number* physical port number, range is 1-26 *port-list* port list, range is 1-26, use ‘,’ and ‘-‘ for multiple setting.
3	**flowcontrol** *{receive|send}{on|off}*	Configure physical port flow control function on/off **send** strands for the flow control function of the sending direction; **receive** strands for flow control function of the receiving direction; **on** enable interface flow control function; **off** disable interface flow control function
4	**exit**	Quit physical port configuration mode and enter global configuration mode
5	**exit**	Quit global configuration mode and enter privileged EXEC mode
6	**show interface line/client** *port-number*	Show interface flow control state; *port_number* physical port number.

For example: set port 10 flow control function on receiving direction to on.

Raisecom#**config**

Raisecom(config)# **interface line/client** *10*

Raisecom(config-port)#**flowcontrol receive** *on*

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

Raisecom(config)#**exit**

Raisecom#**show interface line/client** *10*

R: Receive Direction

S: Send Direction

Port Admin Operate Speed/Duplex Flowcontrol(R/S) Mac-learning

---

10 enable down auto on/off enable

For some equipments, the flow control situation of the ports’ receiving direction and sending direction is configured respectively, but the result take effect at the same time, that is to say, changing the flow control setting of any direction will effect the flow control configuration of both side, on or off at the same time. By default all the ports’ flow control is off.

Step	Command	Description
1	**config**	Enter global configuration mode

2	**interface line/client** *port-number*	Enter physical port mode ; *port_number* physical interface number; *port-list* port list, use ‘,’ and ‘-‘ for multiple setting.
3	**flowcontrol** *{receive|send} {on|off}*	Configure physical port flow control function on/off Send strands for the flow control function of the sending direction; Receive strands for flow control function of the receiving direction; on enable flow control function Off disable port flow control function
4	**exit**	Quit physical port configuration mode and enter global configuration mode;
5	**exit**	Quit global configuration mode and enter privileged EXEC mode;
6	**show interface line/client** *port-number*	Show the port flow control state *port_number* physical port number.

For example: enable port 10 flow control function

Raisecom#**config**

Raisecom(config)# **interface line/client** *10*

Raisecom(config-port)#**flowcontrol receive on**

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

Raisecom(config)#**exit**

Raisecom#**show interface line/client** *10*

R: Receive Direction

S: Send Direction

Port Admin Operate Speed/Duplex Flowcontrol(R/S) Mac-learning

---

10 enable down auto on/on enable

7.5 Auto-MDIX function configuration

The function of Auto-MDIX is to auto-recognize crossover Ethernet cable and straight Ethernet cable. The configuration step is show below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface line/client** *port-number*	Enter physical port mode ; *port_number* physical interface number; *port-list* port list, use ‘,’ and ‘-‘ for multiple setting.

3	**mdi** *(auto |normal |across)*	Configure port MDI mode; auto linear ordering auto reserve mode normal normal mode across cross mode
4	**exit**	Quit physical port configuration mode and enter global configuration mode
5	**exit**	Quit global configuration mode and enter privileged EXEC mode
6	**show mdi** [*<1-MAX_PORT_STR>*]	Show port MDI state *<1-MAX_PORT_STR>*: physical port

For example: set port 8 Auto-MDIX function to auto mode.

Raisecom#**config**

Raisecom(config)# **interface line/client** *8*

Raisecom(config-port)#**mdi auto**

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

Raisecom(config)#**exit**

Raisecom#**show mdi** *8*

Port 8 MDI mode :auto Current status :across

7.6 Maximum transmission unit configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**system mtu** *<1500-8000>* **no system mtu**	Set maximum transmission unit; <1500-8000> system maximum transmission unit range; Delete maximum transmission unit configuration
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show system mtu**	Show system maximum transmission unit configuration

For example: set system maximum transmission unit to 5000.

Raisecom#**config**

Raisecom(config)# **systemc mtu** *5000*

Raisecom(config)#**exit**

Raisecom#**show system mtu**

System MTU size: 5000 bytes

7.7 Add description for interfaces

Description of the Physical port and IP port can be added.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface line/client** *port-number*	Enter physical layer port configuration mode or volume configuration mode *port_number* physical port number, range is 1-26
3	**[no]description** *WORD*	Add physical port or IP interface decription *WORD*——specify class-map decription. 255 character the most, can not be departed by space.
4	**exit**	Quit physical layer port configuration mode and enter global configuration mode.
5	**exit**	Quit global configuration mode and enter privileged EXEC mode.
6	**show interface line/client** [<*1-MAXPORT*>] **detail**	Show port information <1-MAXPORT> port number.

Example 1: add decription for physical port 20.

Raisecom#**config**

Raisecom(config)# **interface line/client** *20*

Raisecom(config-port)# **description** *this-is-a-class-map*

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

Raisecom(config)#**exit**

Raisecom#**show interface line/client** *20* **detail**

7.8 Open and close physical layer port

Sometimes, for a certain intention, to close physical ports is needed, and configuring the ports' on/off is necessary. By default all the ports are on. To extended card port, physical port on/off commands are invalid when the card is not inserted.

Step	Command	Description
1	**config**	Enter global configuration
2	**interface line/client** *port-number*	Enter physical layer port configuration mode or volume configuration mode. *port_number* physical port number. *port-list* port list, use ',' and '-' to make multi-port input.
3	*{shutdown | no shutdown}*	Close or open physical port. shutdown stands for closing physical port. no shutdown stands for opening physical port.

4	**exit**	Quit physical layer interface configuration mode and enter global configuration mode
5	**exit**	Quit global configuration mode and enter privileged EXEC mode.
6	**show interface line/client** *port-number*	Show port state *port_number* physical port number.

Example 1: close port 20.

Raisecom#**config**

Raisecom(config)# **interface line/client** *20*

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

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

Raisecom(config)#**exit**

Raisecom#**show interface line/client** *20*

R: Receive Direction

S: Send Direction

Port Admin Operate Speed/Duplex Flowcontrol(R/S) Mac-learning

---

20 enable down auto off/off enable

Example 2: close extended card port P25 (without extended card inserted)

Raisecom#**config**

Raisecom(config)#**interface line/client** 25

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

Port 25 is unavailable!

7.9 Monitoring and maintaining

Use **show** to show port state.

Command	Description
show interface line/client *port-number*	Show port state *port_number* physical port number.
show interface line/client [<*1-MAXPORT*>] **detail**	Show port information. <*1-MAXPORT*> port number.

For example: show port 8 state.

Raisecom#**show interface line/client** *8*

R: Receive Direction

S: Send Direction

Port	*Admin*	*Operate*	*Speed/Duplex*	*Flowcontrol(R/S)*	*Mac-learning*
8	*enable*	*down*	*auto*	*off/off*	*enable*

Chapter 8 Layer-2 Protocol Transparent Transmission

8.1 Layer-two protocol transparent transmission principle

QinQ offers a relatively simple layer-two VPN tunnel, by packaging outer layer VLAN Tag of user's private network message, so that the message is able to go through the operator's backbone network with layer-two Tag. Based on this, with layer-two protocol transparent transmission function, the layer-two protocol of the user's network can go through the operator's network, so that the same user network of the different places can run layer-two protocol in uniform.

Usually layer-two protocol transparent transmission is carried out by the operator's network edge switch. Transparent transmission function starts on the port that connect the operator's network edge switch and user network. The port exchange mode is access mode or dot1 q-tunnel mode, while the user switch port that is connected with it is trunk mode or hybrid mode. User network's layer-two protocol message, coming from the transparent transmission port, enters operator's network after being packaged by operator edge switch (message input interface). Then decapsulation will be done by the edge switch and the message will be transmitted to user network.

Transparent transmission function includes message packaging and decapsulation, the basic principle is shown below:

- Message encapsulation: in the message input side, the equipment will change the destination MAC address of layer-two protocol message from user network into special broadcast MAC address (default value 010E.05E00.0003). In operator network, the modified message will be transmitted in the user's VLAN as data message.
- Message decapsulation: in the message output side, the equipment will recognize the message that the destination MAC address is special broadcast MAC address (default value is 010E.5E00.0003), and revert the destination MAC address to the source destination MAC address of layer-two protocol message, then send the message to the given user network.

Layer-two protocol transparent transmission function can run with QinQ function or work respectively. But in actual, after the protocol message MAC address being modified, it still need to be covered with outer Tag to go through the operator network.

8.2 Layer-two protocol transparent transmission configuration

Layer-two transparent transmission configuration includes: transparent transmission protocol enable/diabale, transparent transmission message destination MAC address, COS value, the specified VLAN, the specified output port, message lost limit and port off limit. Configuring specified VLAN can make the transparent transmission message be transmitted by the specified VLAN, not the input VLAN; configuring the specified output port, can make the transparent transmission message being transmitted by only the given output port.

8.2.1 Layer-two protocol transparent transmission default configuration

Function	Default value

Enable/disable protocol transparent transmission	Disable
Message destination MAC address	010E.5E00.0003
Message COS	5
Specified VLAN	No specified VLAN
Specified output port	No specified output port
Message package lost limit	No limit
Message port disabled limit	No limit

8.2.2 Layer-two protocol transparent transmission configuration

By the following step, transparent transmission message destination MAC address, message COS value, the specified output port and VLAN can be configured, and enable/disable layer-two protocol transparent transmission function is available.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**relay destination-address** *HHHH.HHHH.HHHH*	Configure transparent transmission message destination MAC address, transparent transmission message destination MAC address must be broadcast address, and can not take 0x0180C2 or 010E.5E00.0003 as front
3 (optical)	**relay cos** <*0-7*>	Set transparent transmission COS value, range is 0-7
4	**interface line/client** *portid*	Enter Ethernet physical port mode
5	**relay port** *portid*	Set transparent transmission specified output port, range is 1-MAX port number.
6	**relay vlan** <*1-4094*>	Set transparent transmission message specified VLAN, range is 1-4094.
7	**relay** *{stp|dot1x|lacp|gmrp|gvrp|all}*	Enable/disable port layer-two transparent transmission function, all stands for all layer-two protocols that support transparent transmission.
8	**exit**	Return to global configuration mode
9	**exit**	Return to privileged EXECmode
10	**show relay**	Show transparent transmission function configuration and state
11	**write**	Save current system configuration

No relay destination-address reverts transparent transmission message destination MAC address to default value, that is 010E.5E00.0003. **no relay cos** clears transparent transmission message specified VLAN, that is the not specified VLAN. **no relay**{stp|dot1x|lacp|gmrp|gvrp|all} closes layer-two protocol transparent transmission function.

Notice:

- Transparent transmission message input equipment and output equipment need to configure the same transparent transmission message destination MAC address, that is to say, to cooperate with other manufacturers, it is needed to keep the equipment transparent transmission message

destination MAC address to stay the same. Transparent transmission message destination MAC address must be broadcast address, and can not begin with 0x0180c2 or 0x010E5E, but can be set to 010E.5E00.0003.

- Transparent transmission message COS value range is 0-7. Usually, transparent transmission protocol message PRI should be higher than ordinary data message.
- Transparent transmission specified output port can be any port of the equipment (except source port). User needs to make sure port VLAN attribution correct by configuration, or the message transparent transmission will fail.
- Transparent transmission specified VLAN value range is 1-4094. If this VLAN has not been created, transparent transmission message real-time transmission fails. So, when configuring specified VLAN, it is necessary to create and enable the VLAN on the equipment.
- To start layer-two protocol transparent transmission, it is needed to disable the corresponding protocols. To enable STP transparent transmission, closing STP protocol is needed.
- On the same equipment, when both the protocol message input port and output port transparent transmission function is enabled, the destination MAC address of protocol message will not be modified.

8.2.3 Layer-two protocol transparent transmission speed limit configuration

To configure transparent transmission message lost threshold and port off threshold, follow the steps below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface line/client** *portid*	Enter Ethernet physical port mode
3	**relay drop-threshold {***stp* | *dot1x* | *lacp* | *gmrp* | *gvrp***}** *<1-4096>*	Set transparent transmission message lost threshold, value range is 1-4096 PDUs/sec.
4	**relay shutdown-threshold {***stp* | *dot1x* | *lacp* | *gmrp* | *gvrp***}** *<1-4096>*	Set transparent transmission message close threshold, value range is 1-4096 PDUs/sec.
5	**exit**	Return to global configuration mode
6	**exit**	Return to privileged EXEC mode
7	**show relay**	Show transparent transmission configuration and state
8	**write**	Save the current configuration of the system

No relay drop-threshold {*stp*|*dot1x*|*lacp*|*gmrp*|*gvrp}*: revert transparent transmission protocol packet lost default configuration. **no relay shutdown-threshold** *{stp*|*dot1x*|*lacp*|*gmrp*|*gvrp}:* revert transparent transmission protocol port close threshold to default configuration, use **no relay shutdown** to enable the port.

Notice:

- Transparent transmission message packet lost threshold and port close threshold value range is 1-40%, usually, packet lost threshold should be less than port close threshold.
- After port transparent transmission function is enabled, if message receiving rate exceeds port close threshold, or if the port receives the message of specified destination MAC address, the port will be closed. When the port is closed because of transparent transmission function, use **no relay shutdown** to enable the port.

8.2.4 Layer-two protocol transparent transmission message statistics clear

Follow the step below to clear transparent transmission message statistics

Step	Command	Description
1	**config**	Enter global configuration mode
2	**clear relay statistics [port-list** *port-list*]	Clear transparent transmission message stat. information
3	**exit**	Return to privileged EXEC mode
4	**show relay statistics**	Show transparent transmission stat. information.

8.2.5 Monitoring and maintaining

Command	Description
show relay [**port-list** *port-list*]	Show transparent transmission configuration and state
show relay statistics [**port-list** *port-list*]	Show transparent transmission message stat. information

8.2.6 Typical configuration example

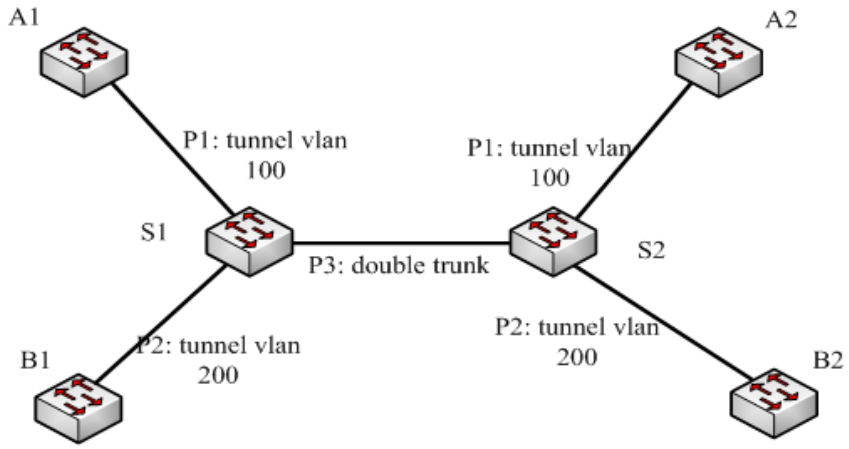


Fig 8-1 transparent transmission basic function configuration

S1,S2 configuration is the same. S1 configuration is shown below:

1) Create VLAN

Raisecom(config)#**create vlan** *100* **active**

Raisecom(config)#**create vlan** *200* **active**

2) Set port 1 exchange mode to dot1q-tunnel mode, ACCESS VLAN to 100, enable STP protocol transparent transmission and set STP message transparent transmission threshold to 1500.

Raisecom(config)# **interface line/client** *1*

Raisecom(config-port)#**switchport mode** d*ot1q-tunnel*

Raisecom(config-port)#**switchport access** vlan *100*

Raisecom (config-port)#**relay** *stp*

Raisecom(config-port)#**relay drop-threshold** *stp 1500*

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

3) Set port 2 exchange mode to dot 1q-tunnel mode, ACCESS VLAN to 200, enable STP protocol transparent transmission and set STP message transparent transmission threshold to 1000.

Raisecom(config)# **interface line/client** *2*

Raisecom(config-port)#**switchport mode** *dot1q-tunnel*

Raisecom(config-port)#**switchport access vlan** *200*

Raisecom (config-port)#**relay** *stp*

Raisecom(config-port)#**relay drop-threshold** *stp 1000*

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

4) Set port 3 exchange mode to trunk double-tagging mode.

Raisecom(config)# **interface line/client** *3*

Raisecom(config-port)# **switchport mode** *trunk double-tagging*

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

Chapter 9 Layer-3 Interface Configuration Guide

This chapter gives an introduction to how to configure and maintain the switch layer-three port, which includes:

- There-layer port introduction
- Layer-three port configuration
- Monitoring and maintaining
- Typical configuration example
- Layer-three port configuration debugging

9.1 Layer-three port introduction

ISCOM switch layer-three port is based on VLAN virtual port configuration, which is for network facility management. To the VLAN that needs router function, a related virtual layer-three port can be set for it. Layer-three port shows as IP address, and every layer-three port has a IP address and relate at least one VLAN.

9.2 Layer-three port configuration

At present, to ISCOM two-layer switch, 15 virtual layer-three ports can be configured, range is 0-14; to ISCOM layer-three switch, 63 virtual layer-three ports can be configured, range is 0-62.

The process of creating layer-three port and configuring IP address is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**Interface ip** <*0-ifNum*>	Enter Ethernet layer-three port configuration mode
3	**ip address ip-address** *[ip-mask] vlanlist*	Set layer-three port IP address and related static VLAN ID

9.3 Monitoring and maintaining

In privileged EXEC mode, use **show interface ip** to show layer-three port configuration state. By looking over the information shown, user can validate the configuration effect.

Command	Description
show interface ip <*0-ifNum*>	Show layer-three information

9.4 Typical configuration example

Set ISCOM switch IP port 1 address to 20.0.1.4, subnet mask to 255.255.255.0, and relate VLAN 1.

Raisecom #**config**

Raisecom (config)#**interface ip 1**

Raisecom (config-ip)#**ip address** *20.0.1.4 255.255.255.0 1*

9.5 Layer-three interface configuration debugging

Fault appearance: ISCOM switch can not connect the host by **ping**.

Debugging step:

Step 1: check out if the switch configuration is correct, use **show arp** to show if there is host ARP table unit in the ARP table.

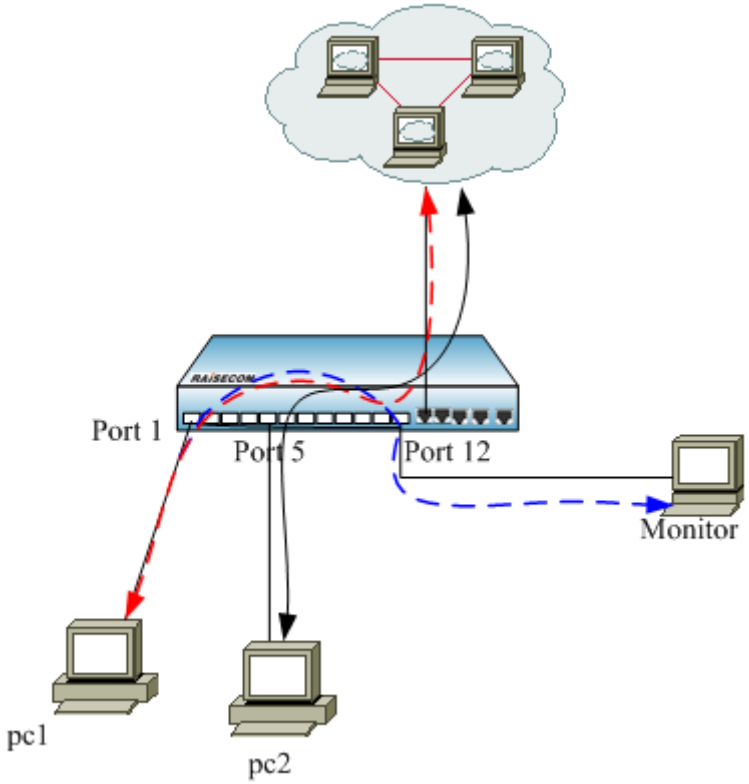
Step 2: check out which VLAN the port that connect the switch and the host belongs to, if the VLAN belongs to the IP interface that is configured, if the IP address and the host belong to the same network segment.

Step 3: if the configuration is correct, open ARP debugging on-off on the switch, and check out if the switch has sent and receive ARP message correctly. If there is only message sent out, while no message received, then there may be problem in Ethernet physical layer.

Chapter 10 Mirroring

10.1 Local Port Mirror Function Principle

Mirror function is to copy some messages the appointed destination port from the appointed source port, while the normal message transmission works well. With this function, exchange equipment user can monitor the message delivering and receiving of a certain port, and analyze the network situation or defaults.



Mirror Function

Consult 1-1 as the principle.

PC1 and PC2 connect internet through port 1 and port 5 of the exchange equipment. When we need to monitor the data from PC1, we need to appoint the port 1 of the facility on connection as the mirror source port, and enable the mirror function of the receiving port message, then appoint monitoring port 12 as the destination port. When the data message from PC1 enters the exchange equipment, it will transfer the message and copy the message to the mirroring destination port (port 12). The monitoring equipment connected with the mirror destination port can receive the messages that is mirrored and make analysis.

10.2 Local Port Mirror Function Configuration

10.2.1 The Default Configuration

Function	Default value
Port mirroring	Disable
Mirror source port	Example
Mirror destination port	Port 1

10.2.2 Local Port Mirroring Function configuration

The traffic of source port will be copied to monitor port, so that network administrators can analyze the network.. Port 1 is monitor port by default, the source port and the monitor can not be same port.

When the mirror function go into effect, the message from I/O mirror ports will be copied to the monitoring port. The mirroring rules are set when the mirror ports are configured: both, ingress and/or egress. Also, the port can not be set as mirror port when it has already been set as monitoring port.

Only after the mirror function is enabled can the other configurations go into effect.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mirror** { **enable** | **disable** }	Enable/disable the mirror function
3	**mirror monitor-port** *port_number*	Set the monitor port. *port_number* is physical port number, range is 1-26.
4	**mirror source-port-list**{ **both** *port-list* | **ingress** *port-list*| **egress** *port-list* | **ingress** *port-list* **egress** *port-list*}	Set source port list, and appoint the corresponding ingress/egress *port-list* is the physical port list, use ‘,’ and ‘- to carry out multi-port input.
5	**exit**	Quit global configuration mode and enter privileged EXEC mode.
6	**show mirror**	Show mirror configuration

Notice:

- The mirroring messages also need to comply the VLAN configuration transmission rules of the port.
- There can be more than one mirroring port, but only one monitoring port is allowed. Mirror function is disabled by default.

With configuration command **no mirror source-port-list**, the mirroring port that has been configured can be deleted.

With configuration command **no mirror all**, all the mirroring configuration can be deleted.

10.2.3 Monitoring And Maintaining

The command to show the port mirroring function

Command	Description
show mirror	Show the port mirroring function

10.2.4 Typical Configuration Example

Set port 26 as the monitoring port, **ingress** port 5-8, **egress** port 7-12

Raisecom #**config**

Raisecom (config)#**mirror enable**

Raisecom (config)#**mirror monitor-port** *26*

Raisecom (config)#**mirror source-port-list ingres**s *5-8* **egress** *7-12*

Raisecom (config)**#exit**

Raisecom #**show mirror**

Mirror: Enable

Monitor port: 26

----------the ingress mirror rule----------

Mirrored ports: 5-8

----------the egress mirror rule----------

Mirrored ports: 7-12

10.3 Mirroring Data Control Function

10.3.1 Mirroring Data Control Default Configuration

Function	Default value
Mirror destination port halting the not-mirroring data	Disable
Mirror source port ingress message split-flow number	1
Mirror source port ingress message filter source MAC address	0000.0000.0000
Mirror source port ingress filter destination MAC address	0000.0000.0000
Mirror source port egress message split-flow number	1
Mirror source port egress message filter source MAC address	0000.0000.0000
Mirror source port egress message filter destination MAC address	0000.0000.0000

10.3.2 Mirror Data Control Configuration

With the following commands, the mirror data can be within transmission control:

Step	Command	Description
1	**config**	Enter global mode

2(optical)	**mirror block-non-mirror** [*enable*|*disable*]	Configure the mirror destination port to enable/disable the filter function for the not-mirror messages
3(optical)	**mirror** [*ingress*|*egress*] **divider** *<1-1023>*	Configure after how many messages a packet is sent to the mirror pot from the source mirror ports' mirror data
4(optical)	**mirror** *[ingress | egress] filter {source | destination} HHHH.HHHH.HHHH*	For the source mirror port, configure to which MAC address the mirror function is closed
5	**exit**	Quit global configuration mode and enter privileged EXEC mode
6	**show mirror**	Show mirror configuration

Notice: These commands are all configured in global configuration mode, and once the configuration is carried out it will affect all the source ports and destination ports.

The source and destination filter can configure only one MAC address.

10.3.3 Monitoring And Maintaining

Show the commands of mirror function

Command	Description
show mirror	Show mirror configuration

10.3.4 Typical Configuration Example

To figure 1-1, if there is too many data messages for port 1 to receive, and reducing the packets number for the monitoring facility is needed, it is supposed to do the following configuration:

Raisecom #**config**

Raisecom (config)#**mirror** *enable*

Raisecom (config)#**mirror monitor-port** *12*

Raisecom (config)#**mirror source-port-list ingres**s *1*

Raisecom (config)# **mirror ingress divider** *200*

Raisecom (config)**#exit**

Raisecom #**show mirror**

Mirror: enable

Monitor port: 12

Non-mirror port: Not block

----------the ingress mirror rule----------

Mirrored ports: 1

Filter rule: All

Divider: 200

MAC address: 0000.0000.0000

----------the egress mirror rule----------

Mirrored ports: --

Filter rule: All

Divider: 1

MAC address: 0000.0000.0000

10.4 VLAN Stream Mirror Function

Function	Default
VLAN mirror port list	Empty
VLAN mirror VLANlist	Empty

10.4.1 Configure VLAN Stream Mirror Function

VLAN included in the VLAN stream mirror VLAN list, can be mirrored to the monitoring port if the entrance to the switch exists in the VLAN stream mirror port list.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mirror source-vlan portlist** *portlist*	Configure VLAN stream mirror port list *portlist*: port list. can make multi-port input through the connector ‘,’ and ‘-’.
3	**mirror source-vlan vlanlist** *vlanlist*	Configure VLAN stream mirror VLAN list *vlan list*: VLAN list, can make multi-VLAN ID input through the connector ‘,’ and ‘-’.
4	**exit**	Quit global configuration mode and enter privileged EXEC mode
5	**show mirror**	Show mirror configuration

Use **no** to clear up VLAN stream mirror port list, or **no mirror source-vlan portlist.**

Use **no** to clear up VLAN stream mirror VLAN list, or **no mirror source-vlan vlanlist.**

Notice:

- Use the same command to enable VLAN stream mirror function and enable local port mirror function.
- The same monitoring port is used for VLAN stream mirror function and local port stream mirroring function.
- The local port mirror command **no mirror all** is compatible, but when it is executed, VLAN stream mirror function is no longer valid.
- VLAN that has not been created can be added to VLAN stream mirror VLAN list, but will not be valid until it has been created and active.

10.4.2 Monitoring And Maintaining

Show the command of VLAN stream mirror function:

Command	Description
show mirror	Show mirror configuration

10.4.3 Typical Configuration Example

- Aim

Configure the monitoring port as 5, mirror the messages from VLAN 10, port 2 to the monitoring port.

- Configuration step

Step 1: enable mirror function, and configure monitoring port 5

Raisecom (config)#**mirror** *enable*

Raisecom (config)#**mirror monitor-port** *5*

Step 2: configure VLAN stream mirror VLAN list

Raisecom (config)#**mirror source-vlan** *vlanlist 10*

Step 3: configure VLAN stream mirror port list

Raisecom (config)#**mirror source-vlan** *portlist 2*

Show the result:

Raisecom#**show mirror**

Mirror: Enable

Monitor port: 5

----------the ingress mirror rule----------

Mirrored ports: --

VlanMirrored ports: 10

VlanMirrored Vlans: 2

----------the egress mirror rule----------

Mirrored ports: --

Chapter 11 DHCP Client Configuration

This chapter is mainly about how to configure and maintain DHCP Client on the switch, including:

- ✧ DHCP Client overview
- ✧ DHCP Client configuration
- ✧ Monitoring and maintenance
- ✧ Typical configuration example
- ✧ DHCP Client trouble shooting

11.1 DHCP client overview

DHCP (Dynamic Host Configuration Protocol) is a protocol to offer client device the configuration information. Based on BOOTP, it adds some function like assigning available network address automatically, network address reuse and other extension configuration. The two protocols can do some interoperation with some mechanism. DHCP offers configuration parameters to the network host, which can be divided into two basic parts: one is offering specific configuration information nto network host, the other part is assigning network address to the host. DHCP is based on client/server mode, where the designated host offers network address and configuration information to the needed host. The designated host is called server.

Usually, DHCP server is used to accomplish IP address assignation in the following situations:

1) Large network scale, it is much too verbose for manual configuration, and cluster management is difficult.
2) In the network the host number is larger than supported IP address number, the system can not offer a static IP address for each host, and the user number access to the network is also limited (for example, Internet service provider is of the situation), lot of users must use DHCP service to get IP address.
3) Only a few hosts need static IP addresses, most hosts do not need that.

There are usually one host and multiple clients (like PC and portable devices) in a typical DHCP application.

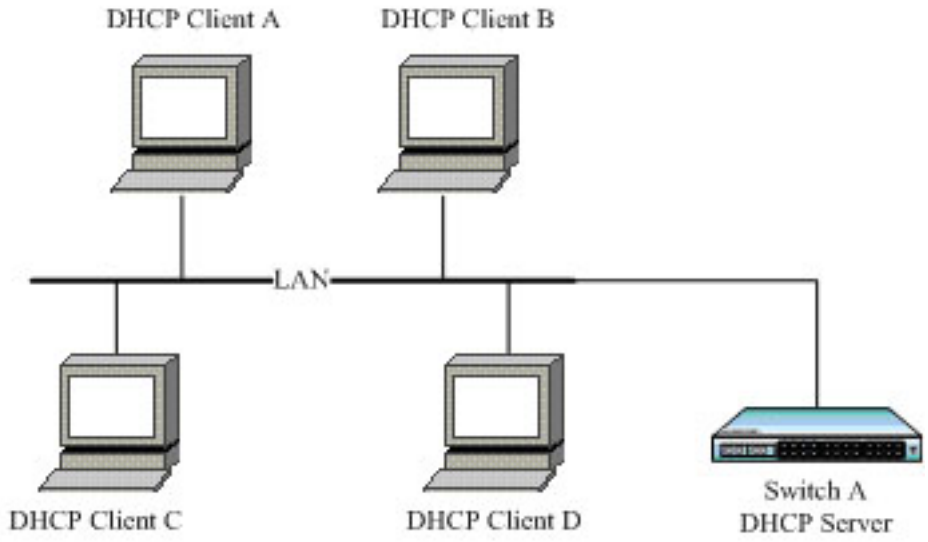


Fig 11-1 Typical DHCP Client application

11.2 Configure DHCP Client

The part is about how to configure DHCP Client on the switch, including:

- ✧ Default DHCP Client configuration
- ✧ DHCP Client configuration guide
- ✧ Configure IP port 0 getting IP address by DHCP
- ✧ DHCP Client renew
- ✧ DHCP Client releasing IP address
- ✧ Configure hostname/class-id/client-id

Attention: To ISCOM serious devices, the commands related to DHCP Client is under IP port; when it comes to RC551 devices, they are in global configuration mode.

11.2.1 Default DHCP Client configuration

Function	Default
hostname	raisecomFTTH
class-id	raisecomFTTH-ROS_VERSION
client-id	raisecomFTTH-SYSMAC- IF0
The IP port acquiring IP address by DHCP	N/A
DHCP Client renew	N/A
DHCP Client release IP address	N/A

11.2.2 DHCP Client configuration guide

- Make sure that DHCP Server or DHCP Relay is not enabled on the switch;
- To a switch, only IP port 0 supports DHCP Client function;
- When DHCP Client is enabled, DHCP Server or DHCP Relay can not be enabled on the switch
- Before using the command, you should make sure that the designated VLAN has been created manually, and the port that IP port lays in has joined the VLAN, while DHCP server has been configured. Or IP address will not be acquired successfully by DHCP.
- If IP port 0 has been configured acquiring IP address from DHCP, then it not allowed to configure IP address manually under the port.
- If IP port 0 has acquired IP address form DHCP, run **ip address dhcp** *{1-4094}* **[server-ip ip-address]**, and if the acquired address is different from the designated VLAN or DHCP Server IP address , then the port will release the acquired IP address and start a new application.
- To port 0, the IP address acquired from DHCP and the manually configured one can cover each other.
- If IP port 0 has acquired IP address by DHCP, then it will start IP address renewal automatically.
- If the client goes through multiple Relay to acquire IP address from DHCP server, make sure that each device is connected and configured correctly. The number of DHCP Relay between the client and server should not exceed 16 in RFC1542, and it is usually recommended not to pass 4.

11.2.3 Configure IP port 0 applying IP address by DHCP

In IP port 0 (only IP port 0), enable DHCP Client, and the device will acquire IP address and requested parameters in the designated VLAN. The parameters includes: gateway address (option 3), TFTP server name (option66), TFTP server address (option 150), configured filename (option 67).

If DHCP server does not support option 150, then you can configure TFTP server address in option 66, which is also supported by DHCP Client.

If one IP address has been configured to IP port 0, then no matter if default gateway configuration successes or not, DHCP Client is thought to have acquired IP address successfully from the server.

The configuration steps are shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *0*	Enter IP port 0 configuration mode
3	**ip address dhcp** *1*	Configure IP port 0 acquiring IP address by DHCP
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp client**	Show DHCP Client configuration and the acquired information (run the command when the application ends)

Attention:

- If DHCP Server or DHCP Relay has been enabled on the switch, DHCP Client can not longer be enabled.
- If DHCP Client has been enabled on the switch, then DHCP server or DHCP Relay can not be enabled.

11.2.4 DHCP Client renewal

In IP port 0, if IP address has been acquired through DHCP, then you can use the command to renew.

When renewing, the result will be shown in the command lines automatically. If renew successes will be typed out by SYSLOG.

The steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *0*	Enter IP port 0 configuration mode
3	**ip dhcp client renew**	DHCP Client renew
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp client**	Show DHCP Client configuration and the acquired information (execute the command when renewal ends)

Attention: The command is available only when IP port 0 has acquired IP address through DHCP.

11.2.5 DHCP Client release IP address

In IP port 0, the steps to release the IP address and other information (like gateway address, TFTP server host name, TFTP server IP address and configured filename) are shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip 0**	Enter IP port 0 configuration mode
3	**no ip address dhcp**	DHCP Client release IP address
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp client**	Show DHCP Client configuration information and the acquired information

Attention: Only when DHCP Client has been enabled in IP port 0 can the command takes effect.

11.2.6 Configure hostname/class-id/client-id

In IP port 0, configure hostname, class-id and client-id for DHCP Client, which will be used when DHCP Client is sending out messages. Take configuring hostname for example, it is similar when configuring class-id and client-id.

The steps are shown below:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**interface ip 0**	Enter IP port 0 configuration mode
3	**ip dhcp client hostname** *myhost*	Configure hostname to myhost
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show ip dhcp client**	Show DHCP Client configuration and acquired information

Attention: No matter if DHCP Client has been enabled, hostname, class-id or client-id can be configured. When IP port 0 applies IP address by DHCP Client, current hostname, class-id or client-id is used; when DHCP Client renews, hostname, class-id or client-id should be the same with the one when it is applying IP address.

11.3 Monitoring and maintenance

Use different **show** to show DHCP Client running state and configuration. All the listed **show** commands are shown below:

Command	Description
show ip dhcp client	Show DHCP Client configuration and the acquired information

Use **show ip dhcp client** to show the configuration and acquired information of DHCP Client. The configuration includes: hostname, class-id and client-id. The acquired information includes: the acquired IP address, subnet mask, default gateway, lease length, lease starting and ending time, server address, TFTP server hostname, TFTP server IP address and the configuration filename.

Raisecom#**show ip dhcp client**

Echo 1: IP port 0 has acquired IP address through DHCP:

Hostname: *raisecomFTTH*

Class-ID: *raisecomFTTH-3.5.856*

Client-ID: *raisecomFTTH-000e5e48e596-IF0*

Assigned IP Addr: *10.0.0.5*

Subnet mask: *255.0.0.0*

Default Gateway: *10.0.0.1*

Client lease Starts: *Jan-01-2007 08:00:41*

Client lease Ends: *Jan-11-2007 11:00:41*

Client lease duration: *874800(sec)*

DHCP Server: *10.100.0.1*

Tftp server name: TftpServer

Tftp server IP Addr: 10.168.0.205

Startup_config filename: 2109.conf

Echo 2: IP port 0 is acquiring IP address through DHCP:

Hostname: Raisecom

Class-ID: Raisecom-3.5.856

Client-ID: Raisecom-000e5e48e596-IF0

DHCP Client is requesting for a lease.

Echo 4: applying IP address fails, no available lease information:

Hostname: Raisecom

Class-ID: Raisecom-3.5.856

Client-ID: Raisecom-000e5e48e596-IF0

No lease information is available.

P.S.:

The blue words, if DHCP Server do not support the option, then replace it with – when showing DHCP Client.

11.4 Typical configuration example

The example is simple but classical on the process of configuring DHCP Client.

1. Configuration instruction:

   The two DHCP clients connect DHCP server by port 2 and 3 respectively.

   1) Configure direct ip pool on DHCP Server, and enable DHCP Server globally.

   2) Configure the two DHCP client acquiring IP address and other configuration information by DHCP.

2. Topology

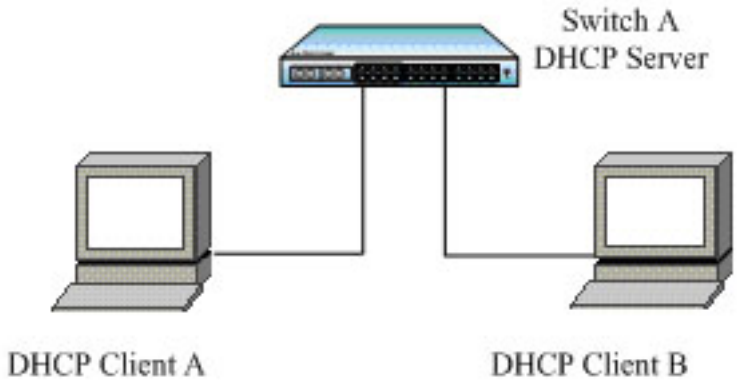


Fig 11-2 Typical configuration example

3. The configuration steps:

Only the configuration steps of Client A are listed here, the steps of the other one is the same and will not be listed.

- Configure IP port 0 acquiring IP address by DHCP:

Raisecom(config)# **interface ip** *0*

Raisecom(ip-config)**#ip address dhcp** *1*

4. Show

On DHCP Client, use **show ip dhcp client** to show the client IP address applied from DHCP and other configuration information.

Raisecom(config)# **show ip dhcp client**

Hostname: raisecomFTTH

Class-ID: raisecomFTTH-3.6.1025

Client-ID: raisecomFTTH-000e5e8a0798-IF0

Assigned IP Addr: 10.0.0.5

Subnet mask: 255.0.0.0

Default Gateway: 10.0.0.1

Client lease Starts: Jan-01-2007 08:00:41

Client lease Ends: Jan-11-2007 11:00:41

Client lease duration: 874800(sec)

DHCP Server: 10.100.0.1

Tftp server name: --

Tftp server IP Addr: 10.168.0.205

Startup_config filename: 2109.conf

11.5 DHCP Client trouble shooting

1. Make sure that DHCP server is able to support option 1, option 3, option 66, option 67, option 150. If some option is not supported, DHCP can not get information of this kind, but for still can get IP address.
2. If the device as DHCP Client starts DHCP Snooping as well, make sure the port it uses to connect DHCP server is the trusted port. Or DHCP Client can not get IP address.

Chapter 12 RMON

12.1 RMON principle interview

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

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

- Statistics: Collects Ethernet, Fast Ethernet, and Gigabit Ethernet statistics on an interface.
- History: Collects a history group of statistics on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces for a specified polling interval.
- Alarm: Monitors a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified value (rising threshold), and resets the alarm at another value (falling threshold). Alarms can be used with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.
- Event: Determines the action to take when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.

12.2 RMON configuration

12.2.1 Default RMON configuration

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

12.2.2 RMON static group configuration

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

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rmon statistics** {**ip** *l3_interface* | **port** *port_list*} [**owner** *STRING*]	**ip** *l3_interface* set the statistics function of layer 3 interface, range is 0-14;

		port *port_list* set the statistics function for the physical port, range is 1-26; **owner** *STRING* set the owner name of current statistics group, default value is "monitorEtherStats".
3	**exit**	Exit from global configuration mode to enter privileged EXEC mode.
4	**show rmon statistics**	Show statistics group information.

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

Notice:

- Before RMON function is configured, SNMP Agent correct configuration must be made sure.
- When the statistic function of some port is disabled, it means not that data statistic is stopped, but that user can no longer acquire the port's statistic data.

12.2.3 RMON history statistic and configuration

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

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rmon history** {**ip***l3_interface* | **port** *port_list*} [**shortinterval** *short-time*] [**longinterval** *long-time*] [**buckets** *queuesize*] [**owner** *STRING*]	**ip** *l3_interface* Set the RMON history function of layer 3 interface, range is 0-14; **port** *port_list* set the RMON history function of physical port, range is 1-26; **shortinterval** *short-time:* the short time interval of history data collection of the port, range is 1-3600, default value is 2 seconds. **longinterval** *long-time* the long time interval of history data collection of the port, range is 1-3600, default value is 300 seconds (5 minutes); **buckets** *queuesize:* circular queue size for history data, range is 10-1000, default is 10. **owner** *STRING:* set the owner name of RMON history group, default name is "monitorHistory".
3	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
4	**show rmon history**	Show history statistics information

12.2.4 RMON alarm group configuration

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

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

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

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

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

12.2.5 RMON event group configuration

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

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

12.2.6 Monitoring and maintenance

Command	Description
show rmon	Show all the RMON four group information

show rmon alarms	Show alarm information, including alarm number, name, threshold, sampling period and sampling value.
show rmon events	Show alarm information, including alarm number, name, threshold, sampling period and sampling value.
show rmon statistics	Show port information which has enabled statistics group.

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

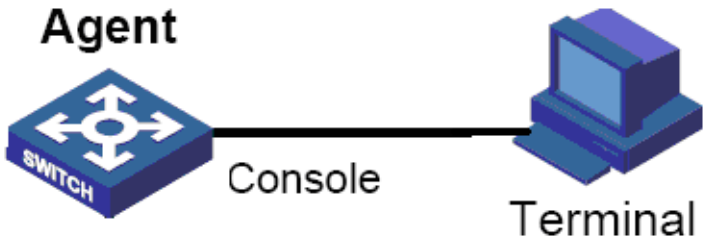
Step	Command	Description
1	**config**	Enter global configuration mode
2	**clear rmon**	Restore to the default state
3	**exit**	Quit global configuration mode and enter privileged EXEC mode.

12.2.7 Typical configuration example

1. Network requirement:

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

2. Network figure



3. Configuration steps:

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

Raisecom#**config**

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

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

Raisecom(config)#**exit**

Raisecom#**show rmon alarm**

Alarm 10 is active, owned by system

Monitors 1.3.6.1.2.1.2.2.1.20.1 every 20 seconds

Taking delta samples, last value was 0

Rising threshold is 15, assigned to event 1

Falling threshold is 0, assigned to event 0

On startup enable rising and falling alarm

Raisecom#show rmon event

Event 1 is active, owned by system

Event generated at 0:0:0

Send TRAP when event is fired.

Chapter 13 ARP

This chapter is mainly about how to configure and maintain ARP on the switch, including:

- ARP interview
- ARP configuration
- Monitoring and maintenance
- Typical configuration example

13.1 ARP principle interview

When the switch software system is transmitting IP message, it is needed to look for its physical address according to the requirement so that the message can be sent to destination host. The mapping relationship of IP address and MAC address is kept in ARP address mapping table.

ARP address mapping table includes 2 types of MAC addresses:

- Dynamic learned MAC address: Dynamic MAC addresses learned through ARP protocol and will be aged if not used.
- Static MAC address: added manually to the table and do not age.

If host A sends IP packets to host B, host A uses the IP address of host B and searches corresponding MAC address in its own ARP table. If there is the MAC address of host B, host A will send the IP packet directly; if there is not the MAC address of host B , host A will send ARP request, get the MAC address of host B and add the address to the ARP table.

In most of the cases, when host A sends IP packets to host B, it is pretty possible that host B will sent packets to host A again, so host B will also need to send ARP request to host A. In order to reduce the traffic in the network, host A write its own MAC address in the ARP request. When host B receives the ARP request, it will record the MAC address of host A to its mapping table. Then it is more convenient for host B to communicate host A.

In some special situation, administrator also can configure ARP address mapping table manually.

13.2 ARP configuration

This part is about how to configure and maintain ARP on the switch, including:

- Default ARP configuration
- Adding stable ARP address table item
- Deleting ARP address mapping table item
- Configuring ARP dynamic address mapping table item overtime
- Configuring ARP dynamic learning mode
- Clearing ARP address mapping table

13.2.1 Default ARP configuration

Function	Default
Stable ARP address table item	No
APR dynamic address mapping table item overtime	1200s
ARP dynamic learning mode	learn-reply-only

13.2.2 Adding dynamic ARP address table item

Usually, ARP mapping table is maintained by dynamic ARP protocol, ARP will search the resolution from IP address to MAC address according to the protocol, needing not the participation of administrator. Only when it is needed to add stable ARP table item will the ARP manual configuration commands be used to ARP mapping table.

Stable ARP address table item has the features below:

- Stable ARP address table item has to be added and deleted manually
- Stable ARP address will not grow old

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**arp** *ip-address mac-address*	Add a stable table item to ARP address mapping table
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show arp**	Show all the table units in ARP address mapping table

Notice: The IP address that is stable added to ARP table item must belongs to the IP network segment that the switch's three-layer port belongs to.

Use global configuration command **no arp** *ip-address* to delete stable ARP table item.

13.2.3 Configure the overtime of ARP dynamic address table item

User can configure the existing time of ARP dynamic item, ARP dynamic table that exceeds the time will be deleted.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**arp aging-time** *sec*	Configure the existing time of ARP dynamic table item, ARP dynamic table item that exceeds the time will be deleted
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show arp**	Show all the table items of ARP address mapping table

Notice: If the exceeding time is set to 0, ARP dynamic table item will no longer grow old.

Use global configuration command **no arp aging-time** to restore the default configuration of ARP dynamic

address mapping table item exceeding time.

13.2.4 Configure ARP dynamic learning mode

It is mentioned above that, to reduce the network communication capacity, when host A is sending its ARP request group, it will write the mapping from its own IP address to the physical address into ARP request group. When host B receives the ARP request group from host A, host B will write the address mapping of host A into its own mapping table. This makes the process of host B sending data to host A more convenient. Configure ARP dynamic learning mode to realize the process mentioned above for learn-all.

The intention of configuring ARP dynamic learning mode is to prevent ARP attack from happening. When configured **learn-all** mode, the host will learn both ARP request message and response message; when configured **learn-reply-only** mode, it will learn ARP response message only, and responds ARP response messages only for request message, without learning ARP.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**arp mode** *{learn-all| learn-reply-only}*	Configure ARP dynamic learning mode
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show arp**	Show all the table items in ARP address mapping table

13.2.5 Clearing ARP address mapping table

In some situations, network administrator may need to clear all the ARP table items. Use command **clear arp** to realize it.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**clear arp**	Clear all the table items in ARP address mapping table
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show arp**	Show all the table items in ARP address mapping table

13.3 Monitoring and maintenance

Use command **show arp** to show the commands of all the table items in the ARP address mapping table, including: the IP address of each table item, MAC address and table item type.

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

13.4 Typical configuration example

1) Network request:

- Configure the aging time of the switch dynamic ARP table item to 600s.
- To prevent ARP attack in some situations, configure the switch's dynamic ARP learning mode to **learn-reply-only.**
- Under the premise that IP port address is configured, add a stable ARP table item.

2) Configuration steps:

Raisecom(config)# **arp aging-time** *600*

Raisecom(config)# **arp mode learn-reply-only**

Raisecom(config)# **arp** *10.0.0.1 0050.8d4b.fd1e*

Chapter 14 SNMP

14.1 SNMP principle

14.1.1 SNMP overview

Now, the network management protocol that is the most extensively used in computer network is SNMP (Simple Network Management Protocol), which is also one of the standard protocol for Internet management.

On structure, SNMP is made up of agent and Network Management Station (NMS), or agent/management station mode. Among them, NMS is the workstation that runs the client program, the management workstations that is usually used now are IBM NetView and Sun NetManager; Agent means the server software that is running on the network equipment like the switch, management information base （MIB） is maintained in Agent.

When SNMP Agent receives the request message Get-Request, Get-Next-Request, Get-Bulk-Request that about MIB variable from NMS, Agent will take read/write operation to the MIB variable that NMS requested according to the message type, then create Response message according to the result, and send it to NMS as response.

On the other side, when SNMP Agent receives the message about some equipment's state like cold/warm booting or anomalous event, it will create a Trap message and send it to NMS actively and report these important incidents.

Raisecom serious SNMP Agent supports SNMPv1, SNMPv2c and SNMPv3

14.1.2 SNMP V1/V2 interview

SNPMv1 is a simple request/response protocol. The network management system sends out a request, the manager returns a response. The action is realized by one of the four protocol operations. The four operations are GET, GETNEXT, SET and TRAP. Through GET operation, NMS get one or more object (instance) values. If the agent can not offer all the request (instance) values from the request list, it will not offer any value. NMS use GETNEXT operation to get the next object instance value from the request list or the object list. NMS use SET operation to send commands to SNMP proxy and request re-configuration to the object value. SNMP proxy use TRAP operation to inform NMS the specific event irregularly.

Different from SNMPv1's simplex centralized management, SNMPv2 supports distributed/layered network management structure, in SNMPv2 management model some systems have both manager and proxy function; as proxy, it can receive the commands from senior management system, interview the local information stored, and offer the information summary of other proxy in the management domain that it charges, then send Trap information to senior manager.

14.1.3 SNMPv3 interview

SNMPv3 uses user-based security model. Whatever it is NMS sending query message to SNMP Agent, or

SNMP Agent sending Trap message to NMS, the communication between NMS and SNMP Agent must be in the name of a certain user. Both SNMP NMS and proxy side maintains a local SNMP user table, user table record username, user related engine ID, if identification is needed and the identification key, encryption information, so that it could make correct resolution to the message content and suitable response. SNMP user's configuration is to create key through the password information in the command lines, and add a user in local SNMP user table of the switch.

14.2 SNMPv1/v2/v3 management configuration

14.2.1 Default SNMP configuration

Function	Default
trap switch	Enabled
The mapping relationship between SNMP user and visiting group	The existed ones by default: initialnone, initial group *Index GroupName UserName SecModel* *0 initialnone raisecomnone usm* *1 initial raisecommd5nopriv usm* *2 initial raisecomshanopriv usm*
SNMP interview group	The existed ones by default: initialnone, initial group Index: 0 Group: initial Security Model: usm Security Level: authnopriv Context Prefix: -- Context Match: exact Read View: internet Write View: internet Notify View: internet Index: 1 Group: initialnone Security Model: usm Security Level: noauthnopriv Context Prefix: -- Context Match: exact Read View: system Write View: -- Notify View: interne

SNMP user	The existed ones by default: raisecomnone, raisecommd5nopriv, raisecomshanopriv user Index: 0 User Name: raisecomnone Security Name: raisecomnone EngineID: 800022b603000e5e00c8d9 Authentication: NoAuth Privacy: NoPriv Index: 1 User Name: raisecommd5nopriv Security Name: raisecommd5nopriv EngineID: 800022b603000e5e00c8d9 Authentication: MD5 Privacy: NoPriv Index: 2 User Name: raisecomshanopriv Security Name: raisecomshanopriv EngineID: 800022b603000e5e00c8d9 Authentication: SHA Privacy: NoPriv
SNMP group	The existed ones by default: public, private group *Index Community Name View Name Permission* *1 public internet ro* *2 private internet rw*
The network administrator's contact information and logo	Contact information: support@Raisecom.com Device location: world china raisecom
SNMP object host address	None
SNMP figure	The existed ones by default: system,internet figure *Index: 0* *View Name: system* *OID Tree: 1.3.6.1.2.1.1* *Mask: --* *Type: included* *Index: 1* *View Name: internet* *OID Tree: 1.3.6* *Mask: --* *Type: included*

14.2.2 SNMPv1/v2 configuration

To protect itself and keep MIB from invalid visit, SNMP Agent brings in the idea of group. The management station in a group must use the group's name in all the Get/Set operations, or the request will not be taken.

The group name uses different character stream to sign different SNMP groups. Different groups may have read-only or read-write visit right. The group that has read-only right can only query the equipment information, while the group with read-write right can not only query the equipment information but also configure it.

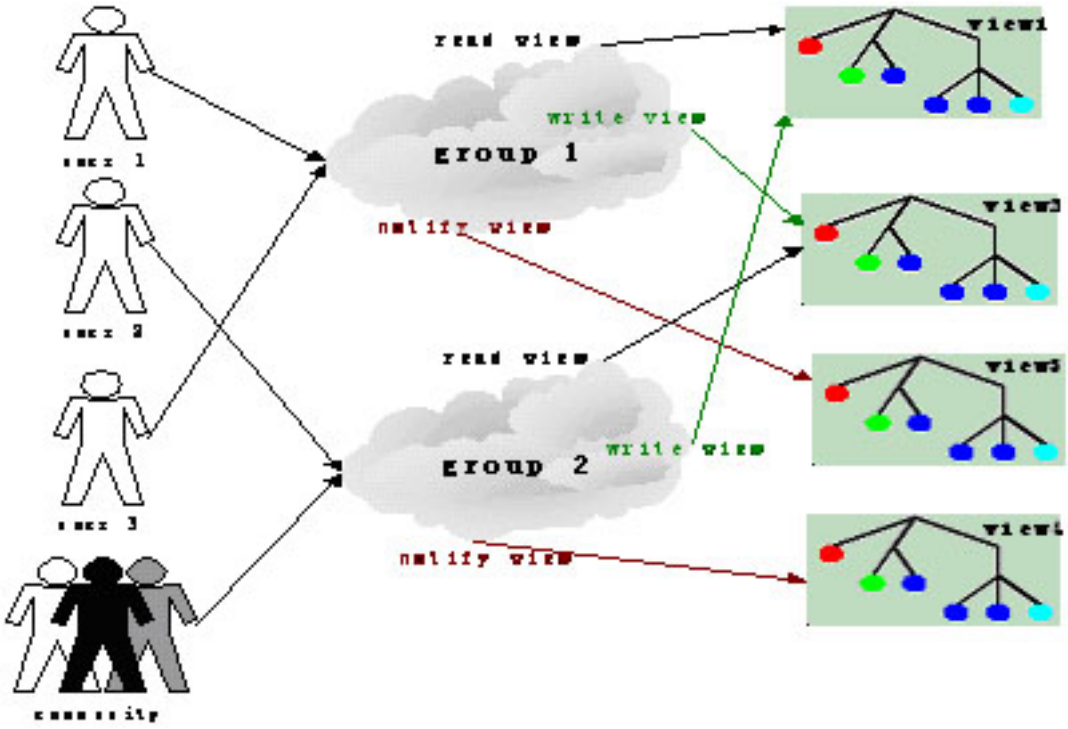
When SNMPv1 and SNMPv2 takes group name authentication project, the SNMP message whose group name is not accorded will be dropped. The whole configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
(optical)	**snmp-server view** *view-name oid-tree* [*mask*] {**included | excluded**}	Define the figure and the contained MIB tree range; *view-name:* figure name, the length can not exceed 32 character; *oid-tree:* 0ID tree, 0ID number which the depth can not exceed 128; *mask:* 0ID tree mask, the depth can not exceed 128, format is 0ID, each option of 0ID can be only 0 or 1;
2	**snmp-server community** *community-name* [**view** *view-name*] *{ro|rw}*	Configure the community name and the relevant attributes. *view-name:* the view name ro: read-only rw: read-and-write
3	**exit**	Return to privileged EXEC mode
4	**show snmp community**	Show group information

Notice: Both SNOMPv1 and SNMPv2 takes group name authentication project, the SNMP message that is not accord with the group name that has been identified will be dropped.

14.2.3 SNMPv3 configuration

SNMPv3 takes USM (user-based security model) which is based on user's security safety model. USM brings the principle of interview group: one user or several users accord with a interview group, each interview group set the corresponding write, read, notify view, the user in interview group has the right in the figure. The interview group in which user send requests likeGet and Set must have the corresponding right, or the request will not be taken.



From the figure above, we can see that the normal interview to the switch for NMS, needs not only configuring the user but also making sure which group the user belongs to, the figure right that the interview group has and each figure. Complete configuration (including user's configuration) process is as follow:

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 privilege of the MIB *view-name* specify the configured name of view *oid-tree* specify OID tree *mask* the mask of OID sub-tree, each bit corresponds to a note of the sub-tree **included** means that the scale of the view includes all the MIB variables under OID tree **excluded** means that the scale of the view includes all the MIB variables out of OID tree
4	**snmp-server group** *groupname* **user** *username* { **v1sm** | **v2csm** | **usm**}	Configure the group which the user belongs to

5	**snmp-server access** *groupname* **[read** *readview***] [write** *writeview***] [notify** *notifyview***] [context** *contextname* **[**{**exact**	**prefix**}**]]** { **v1sm**	**v2csm**	**usm**} { **noauthnopriv**	**authnopriv** }	Define the access privilege of the group *Groupname* is the name of access group; *readview* is the read view, default is internet; *writeview* is the write view, default is empty; *notifyview* is informational view, default is empty; *contextname* is the name of context or its prefix; **exact|prefix** stands for the match type of the context name: **exact** means the input should be fully matched with the name of context, **prefix** means that only the first several letters should match with the name of context; **v1sm|v2csm|usm** are the security model, stands for SNMPv1 security model,SNMPv2 is the security model based on community and SNMPv3 is the security model based on the user respectively; **noauthnopriv|authnopriv** is the security level, stands for no authentication and no encryption, or authentication without encryption respectively.
6	**exit**	Exit to privileged configuration mode
7	**show snmp group** **show snmp access** **show snmp view** **show snmp user**	Show SNMP configuration information

14.2.4 SNMP v1/v2 TRAP configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *0*	Enter IP port mode
3	**ip address** *A.B.C.D[A.B.C.D] vlanID*	Configure the switch IP address *A. B. C. D* IP address *[A. B. C. D]* subnet mask *vlanID* vlan number
4	**exit**	Quit global configuration mode and enter privileged EXEC mode
5	**snmp-server host** *A.B.C.D* **version** {**1**|**2c**} NAME [**udpport** <*1-65535*>] [**bridge**] [**config**] [**interface**] [**rmon**] [**snmp**] [**ospf**]	Configure SNMPv1/v2 Trap object host A.B.C.D NMS IP address NAME SNMPv1/v2c group name <*1-65535*> receiving port number that object host receives Trap, by default it is 162;
6	**exit**	Return to privileged EXEC mode

7	**show snmp host**	Show configuration state

14.2.5 SNMPv3 Trap configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip** *0*	Enter IP port mode
3	**ip address** *A.B.C.D [A.B.C.D] vlanID*	Configure the switch IP address *A.B.C.D*: IP address *[A.B.C.D]*: subnet mask *vlanID*: vlan number
4	**exit**	Quit global configuration mode and enter privileged EXEC mode
5	**snmp-server host** *A.B.C.D* **version** 3 { **noauthnopriv** | **authnopriv** } NAME [**udpport** *<1-65535>*] [**bridge**] [**config**] [**interface**] [**rmon**] [**snmp**] [**ospf**]	Configure SNMPv3 Trap object host *A.B.C.D*: HOST IP address *NAME*: SNMPv3 username *<1-65535>:* receiving port number that object host receives Trap, by default it is 162;
6	**exit**	Return to privileged EXEC mode
7	**show snmp host**	Show configuration state

14.2.6 Other SNMP configuration

1. Configure the network administrator label and contact access

The network administrator label and contact access sysContact is a variable of system group, its effect is to configure the network administrator label and contact access for management switch.

Step	Command	Description
1	**config**	Enter global configuration
2	**snmp-server contact** *sysContact*	Configure network administrator label and contact access
3	**exit**	Return to privileged EXEC mode
4	**show snmp config**	Show configuration situation

2. Enable/disable system sending trap message

Trap is used mainly for providing some switch important events to NMS. For example, when receiving a request with a fault group name and being allowed to send SNMP Trap, the switch will send a Trap message of failed authentication.

Step	Command	Description

1	**config**	Enter global configuration mode
2	**snmp-server enable traps**	Allow the switch to send trap
3	**exit**	Return to privileged EXEC mode
4	**show snmp config**	Show the configuration

Use command **no snmp-server enable traps** to stop the switch from sending trap.

3. Configure the switch position

The switch position information sysLocation is a variable of MIB system group, which is used to describe the physical position of the switch.

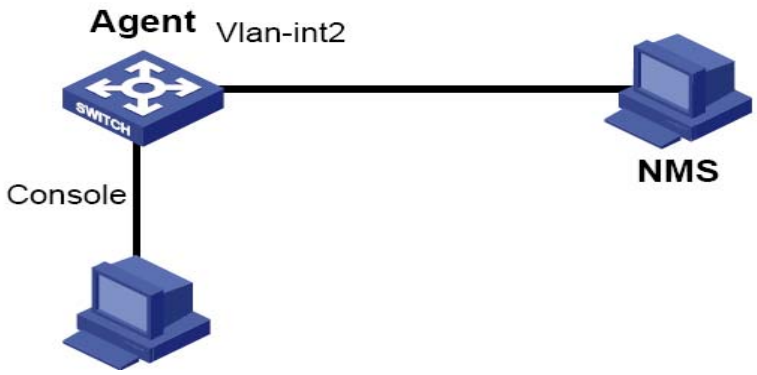
Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server location** *sysLocation*	Configure the switch position *sysLocation:* specify the switch physical position, the type is character stream
3	**exit**	Return to privileged EXEC mode
4	**show snmp config**	Show the configuration

14.2.7 Monitoring and maintenance

Step	Command	Description
1	**show snmp community**	Show SNMP community information
2	**show snmp host**	Show IP address of trap target host computer.
3	**show snmp config**	Show the SNMP engine ID, network administrator contact method, the position of the switch and whether TRAP is enabled.
4	**show snmp view**	Show view information
5	**show snmp access**	Show all the names of access group and the attributes of access group.
6	**show snmp group**	Show all the mapping relationship from user to access group.
7	**show snmp user**	Show the user information, authentication and encryption information.
8	**show snmp statistics**	Show SNMP statistics information

14.2.8 Typical configuration example

The interview control configuration example of V3:



First, set the local switch IP address to 20.0.0.10, user *guestuser1*, uses md5 identification algorithm, with the identification password raisecom, to interview the figure of MIB2, including all the MIB variable under 1.3.6.1.x.1, create guestgroup interview group, the safe mode safe model is usm, the safe grade is identified but not encrypted, the readable figure name is MIB2, thus the process of *guestuser1* mapping to interview group with the safe grade usm can be accomplished, and the result will be shown:

Raisecom#**config**

Raisecom(config)# **interface ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**snmp-server view** *mib2 1.3.6.1.2.1 1.1.1.1.0.1* **included**

Set successfully

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

Set successfully

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

Set successfully

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

Set successfully

Raisecom(config)#**exit**

Raisecom# **show snmp access**

Index: 0

Group: initial

Security Model: usm

Security Level: authnopriv

Context Prefix: --

Context Match: exact

Read View: internet

Write View: internet

Notify View: internet

Index: 1

Group: guestgroup

Security Model: usm

Security Level: authnopriv

Context Prefix: --

Context Match: exact

Read View: mib2

Write View: --

Notify View: internet

Index: 2

Group: initialnone

Security Model: usm

Security Level: noauthnopriv

Context Prefix: --

Context Match: exact

Read View: system

Write View: --

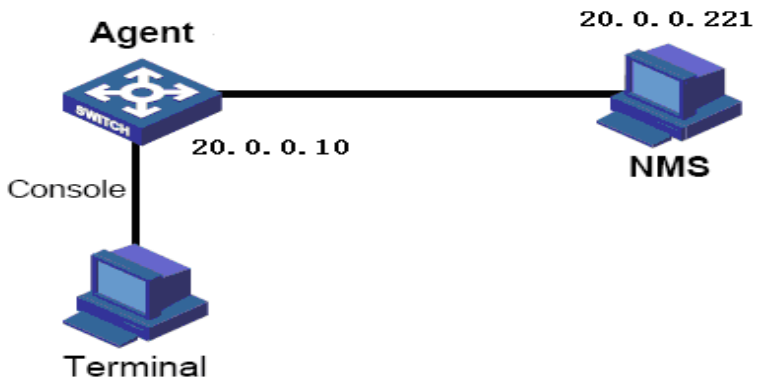
Notify View: internet

Raisecom# **show snmp group**

Index	*GroupName*	*UserName*	*SecModel*
0	*guestgroup*	*guestuser1*	*usm*
1	*initialnone*	*raisecomnone*	*usm*
2	*initial*	*raisecommd5nopriv*	*usm*
3	*initial*	*raisecomshanopriv*	*usm*

V3 Trap configuration example:

Trap is the information Agent sending to NMS actively, used to report some urgent events. As is shown below, set the switch IP address to 20.0.0.10, NMS host IP address to 20.0.0.221, username to raisecom, SNMP version v3, identified but not encrypted, all Trap



Raisecom#**config**

Raisecom(config)# **int ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**snmp-server host** *20.0.0.221* **version** *3* authnopriv *raisecom*

Raisecom#**show snmp host**

Index: 0

IP address: 20.0.0.221

Port: 162

User Name: raisecom

SNMP Version: v3

Security Level: authnopriv

TagList: bridge config interface rmon snmp ospf

Chapter 15 Switch Port Backup

This chapter is mainly about how to configure switch port backup, which is used for a pair of ports to backup each other.

The following contents are included:

- ✧ Switch port backup overview
- ✧ Configure switch port backup
- ✧ Monitoring and maintenance
- ✧ Typical configuration example

15.1 Overview

This part includes:

- ✧ Switch port backup
- ✧ Switch port backup based on VLAN

15.1.1 Switch port backup

Switch port backup is another solution to STP (Spanning Tree Protocol), user can keep basic link redundancy when STP is disabled. If the switch has enabled STP, there is no need to enable port backup, because STP has offered similar function.

Switch port backup group includes a pair of port, one is the main port, the other one is backup port. If one is in Up state, the other one is in Standby state. Only one port can be in Up state at any time, and when there is link fault on the port, the one in Standby state will change to Up.

As is shown in the figure below, switch port A and B connects with switch B and C respectively. If switch A port 1 and port 2 are the members of switch port backup group, then only one port is UP, the other one will be Standby. If port 1 is the main port, then port 1 will transmit messages with switch B, port 2(backup port) and switch C can not transmit messages. If there is link fault between port 1 and switch B, then messages will be transmitted between port 2(backup port) and switch C. Then, after a short time (restore delay) when the link connected with port restores, port 1 will be Up, and port 2 will turn to Standby.

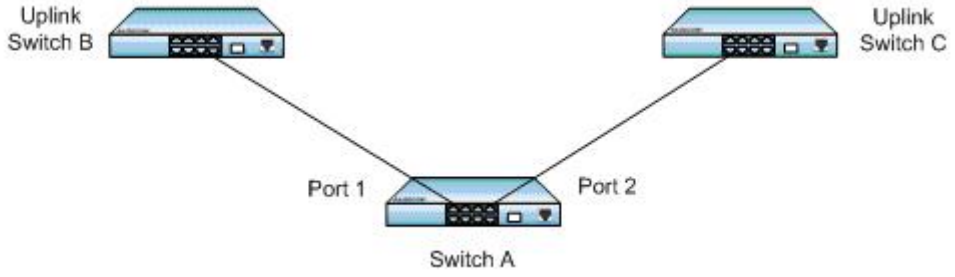


Fig. 15-1 switch port backup configuration

A Trap will be sent when main port and backup port switches.

The members of switch port backup group include physical ports and link aggregation ports, not layer-3 interfaces.

15.1.2 Switch port backup based on VLAN

Switch port backup based on VLAN realizes the communication between two ports in different VLAN.

As is shown in the figure above, if switch A is configured the main port on VLAN 1-100, switch B to backup port; on VLAN 101-200 port 2 is the main port, port 1 is the backup port. Then port 1 transmits flows on VLAN 1-100, while port 2 transmits flows on VLAN 101-200. In this way, switch port backup based on VLAN can be used on load balancing. At the same time, this application lays not on the configuration of uplink switches.

15.2 Configure switch port backup

This part includes:

- ✧ Default configuration
- ✧ Configuration guide
- ✧ Configure switch port backup

15.2.1 Default configuration

Function	Default
Switch port backup group	None
Restore time	15s
Restore mode	Port link mode (port-up)

15.2.2 Configuration guide

- ➢ On the same VLAN, one port /link aggregation group can not be the member of two switch port backup groups;
- ➢ In one switch port backup group, one port can not be either main port and backup port;
- ➢ The main port and backup port of backup group can be physical port or link aggregation group. The members of switch port backup group can be two physical ports or two link aggregation groups, or one physical port added with one link aggregation group;
- ➢ If one link aggregation group is configured to the member of switch port backup group, then it is needed to configure the least member port of the link aggregation group to the member of switch port backup group.
- ➢ The port that has enabled STP can not be configured siwtchport backup, while when configured switch port backup STP can not be enabled.

15.2.3 Configure switch port backup

15.2.3.1 Configure switch port backup group

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** *port_num*	Enter port configuration mode
3	**switch port backup port** *portNum* **[vlanlist** *vlanlist***]**	Configure *portNum* to backup port on *vlanlist*, *port_num* is main port
4	**show switch port backup**	Show switch port backup configuration

For example:

Raisecom#**config terminal**

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

CONFIG-I:Configured from console ...

Raisecom(config)# **interface port** *3*

Raisecom(config-port)# **switch port backup port** *5* **vlanlist** *1-100*

Raisecom(config-port)# **show switch port backup**

Restore delay: 15s

Restore mode: port-up

Active Port(State) Backup Port(State) Vlanlist

----

3 (Up) 5(Standby) 1-100

15.2.3.2 Configure restore delay

Step	Command	Description
1	**config**	Enter global configuration group
2	**switch port backup restore-delay** *<0-180>*	Configure restore delay
3	**show switch port backup**	Show switch port backup information

For example:

Raisecom#**config terminal**

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

CONFIG-I:Configured from console ...

Raisecom(config)# **switch port backup restore-delay** *35*

Raisecom(config)# **show switch port backup**

Restore delay: 35s

Restore mode: port-up

Active Port(State) Backup Port(State) Vlanlist

Attention: To the backup group that is in restore state, it is useless to configure restore relay.

For example:

- When main port and backup port is in LINK_UP state, configure restore delay to 35s, when the main port turns to LINK_DOWN state and then LI NK_UP and keeps still for 35s, then the main port turn to Up state
- When main port and backup port is in LINK_UP state, and when the main port turn to LINK_DOWN state and turn to LINK_UP again, then configure the restore delay time to 35s in the latest configured restore delay time, then the configured value is invalid in this restore process to the port backup group.

15.2.3.3 Configure restore mode

Step	Command	Description
1	**config**	Enter global configuration mode
2	**switch port backup restore-mode {port-up | neighbor-discover}**	Configure restore mode. **Port-up:** port link mode, when port is Up the link is thought to be normal
3	**show switch port backup**	Show switch port backup information

For example:

Raisecom#**config terminal**

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

CONFIG-I:Configured from console ...

Raisecom(config)# **switchport backup restore-mode neighbor-discover**

Raisecom(config)# **show switchport backup**

Restore delay: 15s

Restore mode: neighbor-discover

Active Port(State) Backup Port(State) Vlanlist

Attention: It is invalid to configure restore mode to the switch port backup group that is in restore state.

For example:

When the main port and backup port are both in LINK_UP state, the configuration mode will be neighbor-discover, and when the main port turns to LINK_DOWN state, and uses RNDP (Raisecom Neighbor Discover Protocol) to discover neighbor and keeps restore delay, the main port will turn to Up.

When both the main port and the backup port is in LINK_UP state, and when the main port turns to LINK_DOWN and LINK_UP, then configure restore mode to neighbor-discover in the restore delay time, the configured value is invalid to the restore process of the switch port backup group.

15.3 Monitoring and maintenance

Command	Description
show switchport backup	Show switch port backup information

Use **show switchport backup** to show the related state information of switch port backup, including restore delay, restore mode, switch port backup group information. Switch port backup information includes main port, backup port, main port state(Up/Down/Standby), backup port state(Up/Down/Standby), VLAN list, as is shown below:

Raisecom#**show switchport backup**

Restore delay: 15s

Restore mode: port-up

Active Port(State) Backup Port(State) Vlanlist

---

3 (Up) 5(Standby) 1-100

6 (Down) 7(Up) 1-100

15.4 Typical configuration example

- ✧ Network requirement
- ✧ Network structure
- ✧ Configuration steps

15.4.1. Network requirement

As is shown in the figure below, Switch A needs to support switch port back function, while Switch B, C and D need not.

To realize the stable connection between remote PC and the server, you need to configure :

Configure switch port backup group, and designate VLAN list.

15.4.2. Network structure

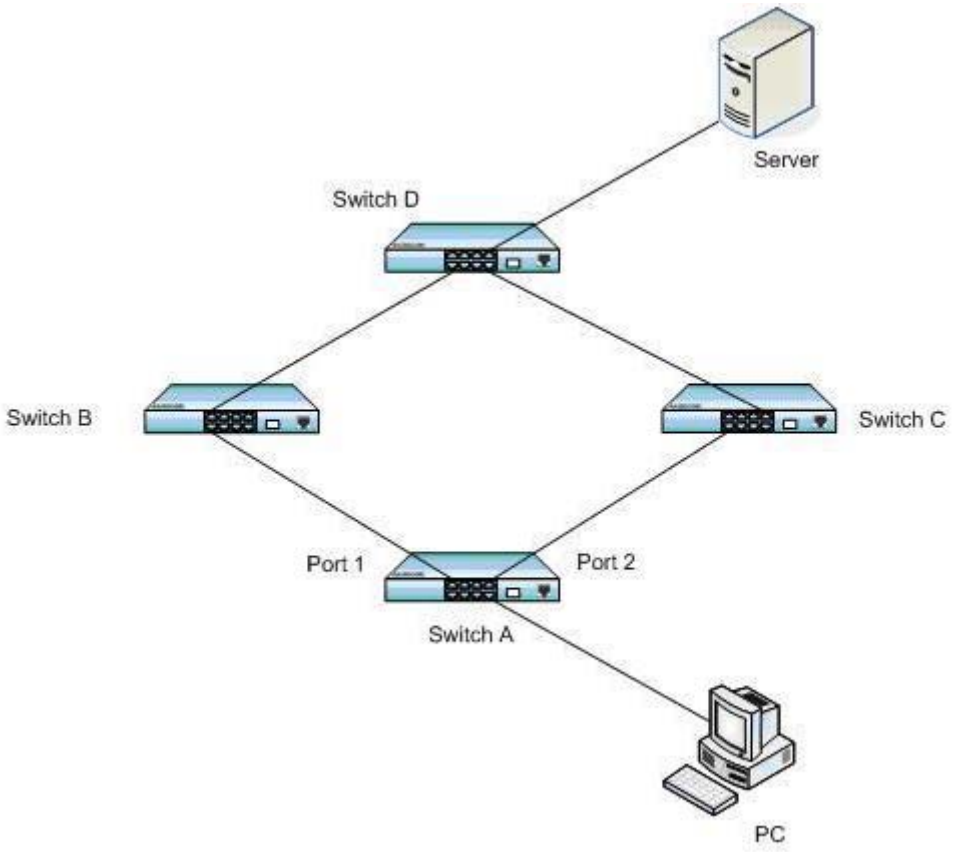


Fig 15-2

15.4.3. The configuration steps

Enter port 1 configuration mode, and configure the main port to port 1, backup port to port 2 on VLAN 1-100:

Raisecom#**config terminal**

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

CONFIG-I:Configured from console ...

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

Raisecom(config-port)# **switchport backup port** *2* **vlanlist** *1-100*

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

Raisecom(config)#

Enter port 2 configuration mode, on VLAN 101-200, configure the main port to port 2, backup port to port 1:

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

Raisecom(config-port)# **switchport backup port** *1* **vlanlist** *101-200*

When both Port 1 and Port 2 is LINK_UP, port 1 will transmit flows on VLAN 1-100, while port 2 on will transmit flows on VLAN 101-200:

Raisecom(config-port)# **show switchport backup**

Restore delay: 15s

Restore mode: port-up

Active Port(State) Backup Port(State) Vlanlist

---

1 (Up) 2(Standby) 1-100

2 (Standby) 1(Up) 101-200

When port 1 turns to LINK_DOWN, port 2 will engage in transmitting the flows on VLAN 1-200:

Raisecom(config-port)# **show switchport backup**

Restore delay: 15s

Restore mode: port-up

Active Port(State) Backup Port(State) Vlanlist

---

1 (Down) 2(Up) 1-100

2 (Up) 1(Down) 101-200

When port 1 restore to normal LINK_UP and stays 15s(restore delay), then port 1 will transmit flows on VLAN 1-100, port 2 will transmit flows on VLAN 101-200.

Raisecom(config-port)# **show switchport backup**

Restore delay: 15s

Restore mode: port-up

Active Port(State) Backup Port(State) Vlanlist

---

1 (Up) 2(Standby) 1-100

2 (Standby) 1(Up) 101-200

Chapter 16 System Log

16.1 System log function introduction n

16.1.1 System log function overview

The switch system information and some debugging output will be sent out for log handling, which will decide the destination that the log information will be sent according to the system log configuration: log files, console, TELNET, log host.

16.1.2 System log format

The format of system log is:

timestamp module-level- Message content

For example: FEB-22-2005 14:27:33 CONFIG-7-CONFIG: USER “raisecom” Run “logging on”.

16.2 Configure system log function

16.2.1 Default system log configuration

Function	Default value
Set the log information to export to the console	Console the direction of the log host is enabled; Output scale is informational.
Set the log information to export to file	Enable the output of the log on file direction
Configure log host	The configuration information without log host
Configure the log exporting to monitor	Monitor the direction of log host is disabled
Enable/disable system log	Enable
Log rate configuration	The sending rate without the limit of logs
Configure the time stand of the log information	Use standard time

16.2.2 Configure system log source

16.2.2.1 Enable/disable system log

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging on**	Enable system log
3	**exit**	Return to privileged EXEC mode

4	**show logging**	Show the configuration

For example:

Raisecom#**config**

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

CONFIG-I:Configured from console ...

Raisecom(config)#**logging on**

set successfully!

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*

16.2.2.2 Configure the time stand of the log information

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging time-stamp** *{standard|relative-start|null}*	Time stamp setting *standard:* standardtime mmm-dd-yyyy hh-mm-ss, for example “FEB-22-2005 14:27:33” *relative-start:* switch running time hh-mm-ss, for example “29:40:6” means the switch has been running for 29 hours 40 minutes 6 second *null:* no time stamp in log information
3	**exit**	Back to privileged EXEC mode
4	**show logging**	View the configuration

For example:

Raisecom#**config**

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

16.2.2.3 Configure the log rate

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging rate** *<1-1000>*	Configure the log number sent every second
3	**exit**	Return to privileged EXEC mode

16.2.3 Configure system log output

16.2.3.1 Log information output to console

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging console** *{<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings}* **no logging console**	Configure and enable log information output to console and the parameter information, use command **no** to close the log output direction <0-7>log scale alerts immediate action is needed (scale 1) critical critical state (scale 2) Debugging debug the information (scale 7) emergencies system not available (scale 0) errors errors (scale 3) Informational inform the event (scale 6) notifications normal event in the critical condition (scale 5) Warnings warning condition (scale 4)
3	**exit**	Return to privileged EXEC mode
4	**show logging**	Show the configuration

16.2.3.2 Configure the log 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|war nings}* **no logging host** *A.B.C.D*	Configure and enable log information output to console and the parameter information, use command **no** to close the log output direction. Local0-local7 the name of log host equipment <0-7>log scale alerts immediate action is needed (scale 1) critical critical state (scale 2) Debugging debug the information (scale 7) emergencies system not available (scale 0) errors errors (scale 3) Informational inform the event (scale 6) notifications normal event in the critical condition (scale 5) Warnings warning condition (scale 4)
3	**exit**	Return to privileged EXEC mode
4	**show logging**	Show the configuration

16.2.3.3 Configure the log information to the file

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging file** **no logging file**	Configure and start recording the log information into flash files, use command **no** to close the log output direction
3	**exit**	Return to privileged EXEC mode
4	**show logging**	Show the configuration

16.2.3.4 Configure the log output to monitor

Step	Command	Description
1	**config**	Enter global configuration mode

		Configure and enable log information output to console and the parameter information, use command **no** to close the log output direction <*0-7*>:log scale *alerts*: immediate action is needed (scale 1) *critical*: critical state (scale 2) *debugging*: debug the information (scale 7) *emergencies*: system not available (scale 0) *errors*: errors (scale 3) *informational*: inform the event (scale 6) *notifications*: normal event in the critical condition (scale 5) *warnings*: warning condition (scale 4)
2	**logging monitor** *{<0-7>|alerts|critical| debugging|emergencies|errors | informational|notifications| warnings}* **no logging monitor**	
3	**exit**	Return to privileged EXEC mode
4	**show logging**	Show the configuration

16.2.4 Monitoring and Maintenance

Use command **show** to monitor and maintain log function

Command	Description
show logging	Show the configuration
show logging file	Show the log file content

For example:

Use **show logging** to look over the current log configuration state:

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

Use **show logging file** to look over the log file content:

Raisecom# **show logging file**

0:15:44 CONFIG-7-REBOOT-A:Reboot system by raisecom

0:15:43 CONFIG-7-CONFIG:USER "raisecom" Run "erase"

0:15:43 CONFIG-7-ERASE-A:Erase system configuration file by raisecom

0:15:31 CONFIG-6-LINK_U:port 24 Link UP

0:11:6 CONFIG-6-LINK_U:port 17 Link UP

0:11:4 CONFIG-6-LINK_D:port 17 Link Down

0:10:40 CONFIG-6-LINK_D:port 24 Link Down

0:10:39 CONFIG-6-LINK_U:port 17 Link UP

0:10:37 CONFIG-6-LINK_D:port 17 Link Down

0:10:33 CONFIG-6-LINK_U:port 17 Link UP

0:10:30 CONFIG-6-LINK_D:port 17 Link Down

0:10:29 CONFIG-6-LINK_U:port 17 Link UP

0:7:4 CONFIG-6-LINK_U:port 24 Link UP

0:3:6 CONFIG-7-LOGIN-A:user: raisecom Login

16.2.5 Typical configuration example

Topology structure:

Fig 16-1 Topology structure

As is shown in fig 1, configure the switch IP address to 20.0.0.6, then start logging function, configure logging host, configure the IP address to 20.0.0.168.

The switch configuration is as follows:

Raisecom**#config**

Raisecom(config)# **interface ip** *0*

Raisecom(config-ip)# **ip address** *20.0.0.6 255.0.0.0 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**logging on**

Raisecom(config)#**logging time-stamp date-time**

Raisecom(config)#**logging rate** *2*

Raisecom(config)#**logging host** *20.0.0.168 local0 warings*

Raisecom(config)#**exit**

Raisecom#**show logging**

Syslog logging:Enable, 0 messages dropped, messages rate-limited 2 per second

Console logging:Enable, level=informational, 16 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

---

20. 0. 0.168 warnings local0 11 0

PC show logging file:

07-01-200811:31:28 Local0.Debug 20.0.0.6 JAN 01 10:22:15 ISCOM3026: CONFIG-7-CONFIG:USER "raisecom" Run "logging on"

07-01-200811:27:41 Local0.Debug 20.0.0.6 JAN 01 10:18:30 ISCOM3026: CONFIG-7-CONFIG:USER "raisecom" Run "ip address 20.0.0.6 255.0.0.0 1"

07-01-200811:27:35 Local0.Debug 20.0.0.10 JAN 01 10:18:24 ISCOM3026: CONFIG-7-CONFIG:USER "raisecom" Run "ip address 20.0.0.6 255.0.0.1 1"

07-01-200811:12:43 Local0.Debug 20.0.0.10 JAN 01 10:03:41 ISCOM3026: CONFIG-7-CONFIG:USER "raisecom" Run "logging host 20.0.0.168 local0 7"

07-01-200811:12:37 Local0.Debug 20.0.0.10 JAN 01 10:03:35 ISCOM3026: CONFIG-7-CONFIG:USER "raisecom" Run "logging on"

Chapter 17 System Clock

17.1 System clock management overview

Raisecom offers two ways for configuring system time: first, use SNTP protocol to make the switch system time accord with SNMP host time, configure the SNMP protocol time for synchronization to Greenwich time, and turn it to local time according to the system time zone configuration; second, configure the system time manually to local time.

17.2 System clock configuration function

17.2.1 Default system clock configuration

Function	Default
Default time	2000-01-01 08:00:00
Default time zone excursion	+08:00
Default summer time function	Disable

17.2.2 Configure system clock function

Step	Command	Description
1	**clock set** *<1-24> <0-60> <0-60> <2000-2199> <1-12> <1-31>*	Configure system time, in turn they are: hour, minute, second, year, month, day
2	**show clock**	Show the configuration

17.2.3 Configure time zone management function

Step	Command	Description
1	**show clock**	Show the configuration
2	**clock set** *<1-24> <0-60> <0-60> <2000-2199> <1-12> <1-31>*	Configure system time, in turn they are: hour, minute, second, year, month, day
3	**clock timezone** *{+|-} <0-11> <0-59>*	Configure system time zone: +: eastern hemisphere -: western hemisphere *<0-11>* : time zone excursion, hour *<0-59>*: time zone excursion, hour By default it is Beijing time, that is eastern hemisphere 8h whole.

17.2.4 Configure summer time function

When summer time configuration is enabled, the time that is accord with SNMP will be transformed into local summer time. The steps are as follows:

Step	Command	Description
1	**clock summer-time enable**	Enable the summer time function. This function can also be shutdown if you do not need it
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>*	Configure system time in turn: hour, minute, second, year, month, day *<1-4>:* the starting week, **last** stands for the last week *Sun:* Sunday *Mon:* Monday *Tue:* Tuesday *Wed:* Wednesday *Thu:* Thursday *Fri:* Friday *Sat:* Saturday *<1-12>* | *MONTH:* month, MONTH stands for the month that you inputs *<0-23>:* hour *<0-59>:* minute *<1-4>* | *last:* ending week *Last:* the last week *Sun:* Sunday *Mon:* Monday *Tue:* Tuesday *Wed:* Wednesday *Thu:* Thursday *Fri:* Friday *Sat:* Saturday *<1-12>* | *MONTH:* month, MONTH stands for the month that you inputs *<0-23>:* hour *<0-59>:* minute *<1-4>*| *last:* ending week
3	**show clock summer-time recurring**	Show summer time configuration

Notice: When configuring the system time manually, if the system uses summer time, then each year April second Sunday morning 2 O' clock to 3 O' clock is not existed. For example, the summer time is set to from the second Sunday 2:00 am of April to the second Sunday 2:00 am of September each year; when the

clock in this time domain is changed one hour faster, or 60 minutes' excursion, then the time between the second Sunday morning 2 and 3am is not existed. The result of manual configuration to the time in this time segment will be failure.

17.2.5 Monitoring and maintenance

Use the following commands to show clock information:

Command	Description
show clock	Show clock information

Use the following commands to show clock information and summer time state:

Command	Description
show clock summer-time-recurring	Show clock summer time

17.2.6 Typical configuration example

Configure the switch time zone and summer time:

Raisecom#**clock timezone** – *10 30*

set successfully!

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

set successfully!

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

Current system time: Mar-28-2005 11:15:22

Timezone offset: -10:30:00

Summer time recurring: Disable

Raisecom#**clock summer-time** *enable*

set successfully!

Raisecom#**clock summer-time recurring** *2* **sun** *3 2 0 2* **sun** *9 2 0 60*

set successfully!

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

Current system time: Mar-28-2005 12:15:53

Timezone offset: -10:30:00

Summer time recurring: Enable

Summer time start: week 02 Sunday Mar 02:00

Summer time end: week 02 Sunday Sep 02:00

Summer time Offset: 60 min

17.3 Configure SNTP function

17.3.1 Default SNTP protocol configuration

Function	Default value
SNMP server address	Not existed

17.3.2 Configure SNTP protocol function

When SNTP server address is configured, the equipment will try to get clock information from SNTP server every 10 seconds, and the maximum exceeding time of SNTP getting clock information is 10 seconds.

Step	Command	Description
1	config	Enter global configuration mode
2	**sntp server** A.B.C.D	Configure SNTP server address
3	**exit**	Return to privileged EXEC mode
4	**show sntp**	Show the configuration

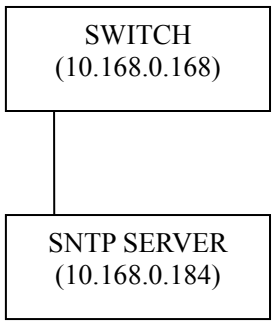
17.3.3 Monitoring and maintenance

Use the following commands to show the switch time management running state and configuration.

Command	Description
show clock	Show clock information

17.3.4 Typical configuration example

For example: the topology structure is shown below:



- Destination:

The switch will get system time from SNTP server

- The configuration steps:

Step 1: show the current default system clock

Raisecom(config)#**show clock**

Current system time: Jan-01-2000 08:00:37

Timezone offset: +08:00:00

Step 2: configure SNTP server address

Raisecom(config)#**sntp server** *10.168.0.184*

set successfully!

JUN-15-2008 20:23:55 CONFIG-6-Get SNTP time , Date is Jun-15-2008 Time is 20:23:55

Raisecom(config)#**exit**

Step 3: show SNTP configuration

Raisecom#**show sntp**

SNTP server address:10.168.0.184

SNTP Server	*Stratum*	*Version*	*Synchronize Time*
10.168.0.184	*15*	*1*	*2008-6-15 20:23:55*

Step 4: show current system clock

Raisecom#**show clock**

Current system time: Jun-15-2008 20:24:33

Timezone offset: +08:00:00

Chapter 18 Sending/receiving Packet Statistic Module Configuration

18.1 Sending/receiving packet statistic module overview

Applicable equipment:

ISCOM2000/2100/2800/2900/3000 serious;

RE5XX serious.

The sending/receiving packet statistic module offers the equipment bottom sending/receiving packet statistic information. It offers tools for equipment fault diagnoses, and supports bottom sending/receiving message control.

The classes that the configuration supports include: destination MAC, Ethernet type, ARP type, IP protocol, ICMP type, UDP port and TCP port.

Destination MAC includes the types below:

- **Broadcast** broadcast message
- **Multicast** not-BPDU multicast message
- **Bpdu** unicast not-local message
- **Dlf** unicast local message

Ethernet include the following types:

- **stp** STP protocol message（0x0042）
- **garp** GARP protocol message（0x0043）
- **gmrp** GMRP protocol message（0x2042）
- **gvrp** GVRP protocol message（0x2142）
- **igmpsnoop** igmpsnoop protocol message（0x0242）
- **lacp** slow protocol frame protocol message（0x8809）
- **eapol** EAPOL protocol message（0x888e）
- **loop** loopback inspection protocol message（0x0898）
- **rcmp** RCMP protocol control message（0x0899）
- **rcmpdata** RCMP protocol control message（0x0897）
- **rndp** RNDP protocol message（0x1a77）
- **rtdp** RTDP protocol message（0x1a78）
- **arp** ARP protocol message（0x0806）
- **ip** IP protocol message（0x0800）
- **others** other Ethernet type message

ARP type includes

- **reply** ARP reply message
- **request** ARP request message
- **others** other ARP messages

IP protocol type includes:

- **icmp** ICMP protocol message（1）
- **igmp** IGMP protocol message（2）
- **tcp** TCP protocol message（6）
- **udp** UDP protocol message（17）

- **others** other IP messages

ICMP type includes:

- **echo** ICMP echo message
- **reply** ICMP echo reply message
- **others** Other ICMP messages

UDP port type includes:

- **dhcp** DHCP protocol message（67、68）
- **snmp** SNMP protocol message（162）
- **tftp** TFTP protocol message（69）
- **sntp** SNTP protocol message（123）
- **rip** RIP protocol message（520）
- **others** other UDP messages

TCP port type includes:

- **ftp** FTP protocol message（20、21）
- **telnet** TELNET protocol message（23）
- **others** other TCP messages

Message length type

- **18-64** message length>=18 <=64
- **65-128** message length>=65 <=128
- **129-256** message length>=129 <=256
- **257-512** message length>=257 <=512
- **513-1522** message length>=513 <=1522
- **Others** other message length

ARP source/destination address types includes

- **SWx** port x
- **Others** other ARP messages

IP source/destination address types include:

- SWx port x
- Others other IP messages

18.2 Sending/receiving packets configuration list

The sending/receiving packets statistic configuration includes:

- ✧ Enable/disable a certain syslog type sending/receiving message;
- ✧ Drop/restore a certain type sending/receiving message;
- ✧ Enable/disable syslog alarm information when the message number exceeds the threshold value in 30s;
- ✧ Enable/disable dropping message when the message number exceeds the threshold value in 30s;
- ✧ Monitoring and maintenance

18.3 Enable/disable a certain syslog sending/receiving message

The steps to enable/disable a certain syslog sending/receiving message are as follows:

Step	Command	Description
1	**Debug driver**	Debug driver module
2	**config**	Enter global configuration mode
3	**Logging console debug**	Console logging scale to debug
4	**driver {receive-packet|send-packet} [dmac-classify** *{broadcast|muticast|bpdu|dlf|unicast}* **|ethertype-classify** *{stp|garp|gmrp|gvrp|igmpsnoop|lacp|eapol|loopdetect|rcmp|rcmpdata|rndp|rtdp|arp|ip|others}* **|arp-classify** *{reply|request|others}* **|ip-classify** *{icmp|igmp|udp|tcp|others}* **|icmp-classify** *{echo|reply|others}* **|udp-classify** *{dhcp|snmp|tftp|sntp|rip|others}* **|tcp-classify** *{ftp|telnet|others}***] debug {enable|disable} [port-list** *port-list***]**	enable/disable a certain logging type sending/receiving messages; Enable Disable
5	**exit**	Return to global configuration mode
6	**Show cpu-statistics**	Show the equipment sending/receiving message statistaic

By default, do not make logging to any message.

18.4 Drop/restore a certain type of sending/receiving message

The steps to drop/restore a certain type of sending/receiving message are as follows:

Step	Command	Description
1	**config**	Enter global configuration
2	**driver {receive-packet|send-packet} [dmac-classify** *{broadcast|muticast|bpdu|dlf|unicast}* **|ethertype-classify** *{stp|garp|gmrp|gvrp|igmpsnoop|lacp|eapol|loopdetect|rcmp|rcmpdata|rndp|rtdp|arp|ip|others}* **|arp-classify** *{reply|request|others}* **|ip-classify** *{icmp|igmp|udp|tcp|others}* **|icmp-classify** *{echo|reply|others}* **|udp-classify** *{dhcp|snmp|tftp|sntp|rip|others}* **|tcp-classify** *{ftp|telnet|others}***] discard {enable|disable} [port-list** *port-list***]**	Drop/restore a certain type of sending/receiving message Enable drop Disable restore
3	**exit**	Return to global configuration mode
4	**Show cpu-statistics**	Show the equipment sending/receiving message statistic

By default the following types of messages will be dropped: the DLF messages of MAC type, the other ARP messages of ARP type and ARP or destination address type and the other ICMP type messages of ICMP type.

18.5 Enable/disable the syslog alarm information when the message number exceeds the threshold number in 30s

The steps to enable/disable the syslog alarm information when the message number exceeds the threshold number in 30s are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**driver {receive-packet|send-packet} [dmac-classify** *{broadcast|muticast| bpdu|dlf|unicast}* **|ethertype-classify** *{stp|garp|gmrp |gvrp|igmpsnoop|lacp|eapol |loopdetect|rcmp|rcmpdata |rndp|rtdp|arp|ip|others}* **|arp-classify** *{reply|request|others}* **|ip-classify** *{icmp|igmp|udp|tcp|others}* **|icmp-classify** *{echo|reply|others}* **|udp-classify** *{dhcp|snmp|tftp|sntp|rip|others}* **|tcp-classify** *{ftp|telnet|others}***] threshold** *<1-10000>* **[port-list** *port-list***]**	Configure the sending/receiving threshold value of a certain type in 30s
3	**driver {receive-packet|send-packet} [dmac-classify** *{broadcast|muticast| bpdu|dlf|unicast}* **|ethertype-classify** *{stp|garp|gmrp|gvrp|igmpsnoop|lacp|eapol |loopdetect|rcmp|rcmpdata |rndp|rtdp| arp|ip|others}* **|arp-classify** *{reply|request| others}* **|ip-classify** *{icmp|igmp|udp|tcp| others}* **|icmp-classify** *{echo|reply|others}* **|udp-classify** *{dhcp|snmp|tftp|sntp|rip| others}* **|tcp-classify** *{ftp|telnet|others}***] warning {enable|disable} [port-list** *port-list***]**	Enable/disable the syslog alarm information when the message number exceeds the threshold value in 30s
3	**exit**	Return to global configuration mode
4	**Show cpu-statistics**	Show the equipment sending/receiving message statistic

By default there is no alarm.

18.6 Enable/disable dropping the message when the message number exceeds the threshold value in 30s

The steps to enable/disable dropping the message when the message number exceeds the threshold value in 30s are as follows:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**driver {receive-packet|send-packet} [dmac-classify** *{broadcast|muticast |bpdu|dlf|unicast}* **|ethertype-classify** *{stp|garp|gmrp|gvrp|igmpsnoop|lacp|eapol |loopdetect|rcmp|rcmpdata |rndp|rtdp|arp|ip |others}* **|arp-classify** *{reply|request|others}* **|ip-classify** *{icmp|igmp|udp|tcp|others}* **|icmp-classify** *{echo|reply|others}* **|udp-classify** *{dhcp|snmp|tftp|sntp|rip|others}* **|tcp-classify** *{ftp|telnet|others}***] threshold** *<1-10000>* **[port-list** *port-list***]**	Configure a certain type 30s sending/receiving message threshold
2	**driver {receive-packet|send-packet} [dmac-classify** *{broadcast|muticast| bpdu|dlf|unicast}* **|ethertype-classify** *{stp|garp|gmrp|gvrp|igmpsnoop|lacp|eapol |loopdetect|rcmp|rcmpdata |rndp|rtdp|arp|ip |others}* **| arp-classify** *{reply|request|others}* **|ip-classify** *{icmp|igmp|udp|tcp|others}* **|icmp-classify** *{echo|reply|others}* **|udp-classify** *{dhcp|snmp|tftp|sntp|rip|others}* **|tcp-classify** *{ftp|telnet|others}***] Limit {enable|disable} [port-list** *port-list***]**	Enable/disable dropping the message when the message number exceeds the threshold number in 30s Enable Disable
3	**exit**	Return to global configuration mode
4	**Show cpu-statistics**	Shown the equipment sending/receiving message statistic

By default do not drop any message.

18.7 Monitoring and maintenance

Use **show** to show CUP sending/receiving packet statistic information, use **clear** to clear CPU sending/receiving packet statistic information to realize CPU sending/receiving packet monitoring and maintenance:

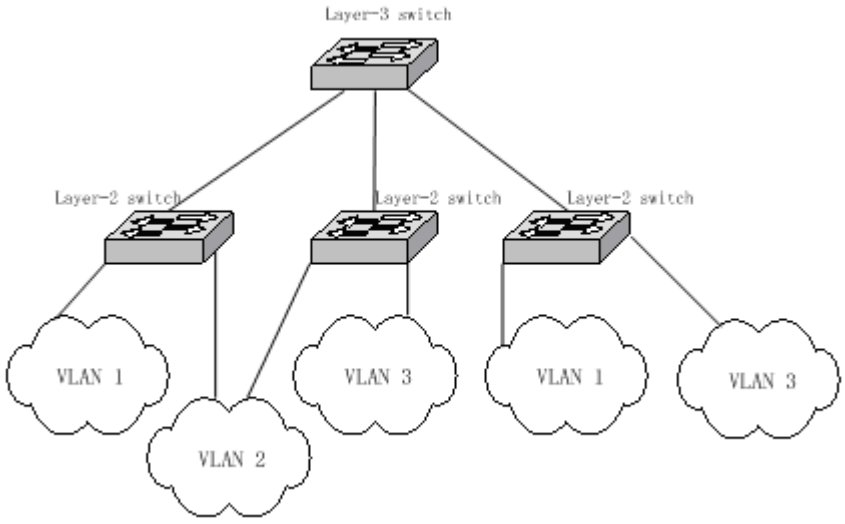
Step	Description
Show cpu-statistics	Show the equipment sending/receiving message statistic
Clear cpu-statistics	Clear the equipment sending/receiving message statistic

Chapter 19 VLAN

19.1 VLAN Principle

19.1.1 IEEE802.1Q VLAN

VLAN stands for virtual LAN (virtual Local Area Networks). In terms of functions, VLAN has the same characteristics with LAN. However, VLAN members are not restricted by physical locations. For instance, the users connected to the same switch can belong to different VLANs. The broadcast domain and multicast domain are both in reference to VLAN member, multicast, broadcast and unicast will not flood to other VLANs. Different VLANs can communicate with each other only via Layer-3 switch or router. The features above offer much convenience for network management, user can allocate VLANs based on functions in the network so as to promote the network bandwidth utility and security. A typical VLAN network topology is shown below:



VLAN, a protocol to handle the Ethernet problems from broadcasting and safety, is added VLAN port based on Ethernet frame, divides users into smaller working group using VLAN ID and limits the two-layer visit between users within different working groups. Each working group is a virtual LAN.

In 1999 IEEE issues the 802.1Q protocol standard draft for VLAN realization project. As the criterion of VLAN, it encapsulates VLAN ID in the frame header, so that the VLAN information can be kept when a frame is crossing different equipments. The switches of different producers can be under unified management and cross switches if only they support 802.1Q VLAN.

19.1.2 VLAN Mapping interview

VLAN Mapping can modify VLAN Tag in the message, and supports the following two mapping relationships:

1: 1VLAN Mapping: change the VLAN ID in VLAN Tag taken by a message into another VLAN ID.

2: 2VLAN Mapping: add out-layer VLAN Tag to the message with one layer VLAN Tag, so that the message can take two layer VLAN Tag.

19.1.3 Q-IN-Q interview

In the framework of IP data network, the switch is used as access equipment, when LAN is used as the access process, to divide users for user's data safety becomes a serious problem.

Now many producers demands end to end safety recognition, hoping each user can allocated a VLAN, but the problem is that there are only 4096 standard VLAN resources. However, using the innovative Q-in-Q technology, the limit of 4096 VLAN can be broken through in metro Ethernet assembly, which not only extends the ability of creating two-layer network using VLAN, but also realizing metro network two-layer VPN, that is suitable for metro network and WAN services.

Q-in-Q technology is a simple and flexible two-layer VPN technology. Using outer-layer VLAN Tag to encapsulate outer-layer VLAN Tag for user's private network message in carrier's access end, it can let the message carry two-layer VLAN Tag to cross carrier's backbone network (public network). Inner layer VLAN Tag is user private network VLAN Tag, outer layer VLAN Tag is the one that carrier allocates to user. In public network, messages transmit only according to the outer layer VLAN Tag, and the source MAC address table item of the messages is learned and copied to the MAC address table of the VLAN that outer layer Tag is in, while user's private network VLAN Tag will be taken as the messages' data part for transmission.

The basic working principle and method of Q-in-Q: when the data is transmitting in private network it has a private network mark, defined as CVLAN Tag; when entering the backbone network of facilitator, public network VLAN Tag will be added to it, defined as SPVLAN Tag (or Outer tag); when reaching destination private network the SPVLAN Tag of the public network will be deleted to offer user a relatively simple two-layer VPN tunnel. SPVLAN Tag is embedded after Ethernet source MAC address and destination MAC address, which also contains a 12 bits SPVLAN ID that supports 4096 VLAN. SPVLAN CoS domain contains 3 bits, supports 8 priority. In the network based on Q-in-Q, the operator allocates a SPVLAN ID for each VLAN, then maps user's CVLAN ID to these SPVLAN ID. Thus, user's C-VLAN ID can be protected.

19.2 Switch VLAN Function Configuration

19.2.1 VLAN based on port

VLAN division based on port is the most simple and effective way for VLAN division. It defines VLAN member according to the equipment port, and when the given port enters the given VLAN, it can transmit messages from the given VLAN

19.2.1.1 VLAN port mode interview

Port member mode	VLAN member attributes
Access	Under this mode, the port can be allocated to a single VLAN, packet sent from Access port does not have no 802.1Q tag, Access ports within different VLANs cannot communicate with each other.
Hybrid	Under this mode, the port can be allocated to multiple VLANs, you can also determine if packet sent out from Hybrid port carries related 802.1Q tag or not. Meanwhile, you can also classify the non-802.1Q packets that enter the port into different VLANs by setting the Native attribute of the port.

Trunk	Trunk port can be allocated with different VLANs by default, packet forwarded from it carries 802.1Q tag expect for Native VLAN. However, you can limit the packets through which VLAN they are forwarded by using *allowed vlans*
Dot1q-tunnel	TUNNEL port mode can only be designated to one VLAN by user, the data packet transmitted from TUNNEL port do not contain out layer TAG, TUNNEL port of different VLAN can not interflow. The data packet entered from TUNNEL port can be added two layer TAG.
Trunk double-tagging	Configure port to TRUNK mode, and enable the port the ability of recognizing and handling out layer TAG (that is SP VLAN TAG).
Hybrid dot1q-tunnel	Configure the port to HYBRID mode, enable the port the ability of adding outer layer TAG (that is SP VLAN TAG) for the packet entering the port (ignoring the out-layer/inner-layer TAG in the data packet)

19.2.1.2 Default VLAN configuration

Function	Default
Create stable VLAN	There are default VLAN and cluster VLAN in the system, that is VLAN 1 and VLAN 2, all the ports exists in VLAN 1 in access mode
VLAN name	The default system VLAN (VLAN 1) is 'Default', cluster VLAN name is 'Cluster-Vlan', other stable VLAN name is 'VLAN' adding VLAN ID(four figures number)
Configure the activity state of stable VLAN	The new created stable VLAN activity state is suspend.
Configure the port mode	Access
Configure the VLAN number that is allowed to pass in HYBRID mode	All VLAN
Configure the VLAN number that is allowed to pass in TRUNK mode	VLAN1
Configure Native VLAN for Trunk, Hybrid port	VLAN1
VLAN filtration attribute	Enable
Port protection	The port is not protected port
Transmission port list	All the other ports except its own port
VLAN priority	No priority

19.2.1.3 Configure VLAN Attribute

VLAN attribute configuration includes the VLAN configuration of creation, deletion, name and activity state. The configuration steps are as follows:

Step	Command	Command parameter explain
1	**config**	Enter global configuration mode
2	**create vlan** *{2-4094}*	Create VLAN and make sure the state:

	(active|suspend) priority {*0-7*}	active/suspend 0-7: VLAN priority {2-4094}: VLAN ID
3	**vlan** <*1-4094*>	Create VLAN and enter the configuration mode <*1-4094*> VLAN ID
4	**name** *WORD*	Dominate VLAN *WORD* VLAN name, no longer than 15 characters
5	**state** {**active	suspend**}	Configure VLAN state: active/suspend
6	**exit**	Return to global configuration mode
7	**exit**	Return to privileged EXEC mode
8	**show vlan**	Show VLAN configuration

Use **no vlan** <*2-4094*> to delete VLAN.

Notice:

- The new created VLAN using VLAN <1-4094> is in suspend state, if user wishes to activate it in the system, the command **state** that would be introduced later is needed to activate VLAN.
- By default there are VLAN existed in the system, that is default VLAN (VLAN 1) and cluster VLAN (VLAN 2), all the ports are Access mode belongs to the default VLAN. VLAN priority range is 0-7.
- The new created VLAN, has no priority by default, is shown as N/A. VLAN priority range is 0-7.
- By default, default VLAN (VLAN 1) name is 'Default', cluster VLAN (VLAN 2) name is 'Cluster-VLAN', other VLAN name is character stream 'VLAN' added four figures VLAN ID. For example, the default VLAN 1 name is 'VLAN0001', the default VLAN 4094 name is 'VLAN4094'.
- All the VLAN configuration can no take effect until the VLAN is activiated. When VLAN activity state is suspend, user can still configure the VLAN, like delete/add port, configure VLAN name and so on, the system will keep the configuration, once the VLAN is activated, the configuration will take effect in the system.

19.2.1.4 Configure VLAN priority

By default, when VLAN is created, there is no priority, shown as N/A, the VLAN priority range is 0-7. The configuration steps are as follows:

Step	Command	Command parameter example
1	**config**	Enter global configuration mode
2	**vlan** {*2-4094*} **priority** <0-*7*>	Configure VLAN priority {*2-4094*} VLAN ID <0-*7*> VLAN priority
3	**exit**	Return to privileged EXEC mode
4	**show vlan**	Shown VLAN configuraion

Use **no vlan** {2-4094} **priority** to restore VLAN priority to default state, or VLAN without priority.

19.2.1.5 Configure port VLAN mode

Each mode and the configuration is shown below:

1. Configure port VLAN mode

Port VLAN mode configuration must be done in physical interface configuration mode, the steps are as follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface line/client** *portid*	Enter the corresponding physical port configuration mode *portid*: port number
3	**switchport mode** *{access | hybrid [double-tagging]| trunk [double-tagging]| [hybrid] dot1q-tunnel}*	Configure port VLAN mode access ACCESS mode, that is port exists in the unique VLAN in the form of UNTAG; hybrid HYBRID mode, port can exist in several VLAN in both UNTAG or TAG mode hybrid double-tagging Configure the port to HYBRID mode, and enable the port the ability of recognizing and handing outer layer Tag (or SP VLAN Tag) hybrid dot1q-tunnel configure the port to HYBRID mode, and enable the port the ability of compulsively adding outer layer Tag (or SP VLAN Tag) for the packets. trunk TRUNK mode, port exists in several VLAN in TAG mode, and exists in Native Vlan in UNTAG mode. trunk double-tagging configure the port to TRUNK mode so that it is able to recognize and handle outer layer Tag (or SP VLAN Tag) dot1q-tunnel TUNNEL mode, the data packet enters from theis port can be added double Tag
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface line/client** [*port-list*] **switchport**	Show port VLAN attribute configuraion

Use **no switchport mode** to restore port VLAN mode to default value, that is port VLAN mode is Access mode.

2. Configure Access, dot1q-tunnel port Access VLAN, the steps are as follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface line/client** *portid*	Enter physical port configuration mode

3	**switchport access vlan** *<1-4094>*	Configure VLAN that is allowed to pass Hybrid port
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface line/client** [*port-list*] **switchport**	Show port VLAN attribute configuration

Use **no switchport access vlan** command to restore Access VLAN to default value, or port Access VLAN is VLAN 1.

3. Configure VLAN that is allowed to pass through Hybrid port ,the steps are as follows:

Step	Comamnd	Description
1	**config**	Enter global configuration mode
2	**interface line/client** <1-26>	Enter the corresponding physical port configuration mode
3	**switchport hybrid allowed vlan { all** | *vlan-list* | **add** *add-vlan-list* | **remove** *remove-vlan-list***}**	Configure the allowed VLANs for the Hybrid port All: allow all vlan vlan-list: allow all VLAN, rewrite the primary configuration Add: add-vlan-list: add vlan base on the existent vlan Remove: remove-vlan-list, remote vlan base on the existent vlan
4	**switchport hybrid untagged vlan { all** | *vlan-list* | **add** *add-vlan-list* | **remove** *remove-vlan-list***}**	Configure the allowed VLANs for the Untagged port All: allow all vlan vlan-list: allow all VLAN, rewrite the primary configuration Add: add-vlan-list: add vlan base on the existent vlan Remove: remove-vlan-list, remote vlan base on the existent vlan
5	**exit**	Back to global configuration mode
6	**exit**	Back to privileged EXEC mode
7	**show interface line/client** [{*1-26*}] **switchport**	Show the port VLAN attributes configuration

Use **no switchport hybrid allowed vlan** to restore Hybrid port allowed VLAN to default value, that is, all the VLAN is allowed to pass.

Use **no switchport hybrid untagged vlan** to restore Hybrid port allowed Untagged VLAN to default value, that is, only VLAN is allowed to pass.

4. Configure VLAN that is allowed to pass Trunk port, the steps are as follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface line/client** *portid*	Enter corresponding physical port configuration mode
3	**switchport trunk allowed vlan** { **all** | *vlan-list* | **add** *add-vlan-list* | **remove** *remove-vlan-list***}**	Configure the allowed VLAN for the Trunk port All: allow all vlan vlan-list: allow all VLAN, rewrite the primary configuration Add: add-vlan-list: add vlan base on the existent vlan Remove: remove-vlan-list, remote vlan base on the existent vlan
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface line/client [***port-list***] switchport**	Show port VLAN attribute configuration

Use **no switchport trunk allowed vlan** to restore Trunk port allowed VLAN list to default value, that is, all the VLAN.

5. Configure Native VLAN of Trunk and Hybrid port, the steps are as follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface line/client** *portid*	Enter corresponding physical port configuration mode
3	**switchport native vlan** *<1-4094>*	Configure Native VLAN of Trunk and Hybrid port
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface line/client** [*port-list*] **switchport**	Show port VLAN attribute configuration

Use **no switchport native vlan** to restore Native VLAN of Trunk and Hybrid port to default value, or VLAN1.

19.2.1.6 VLAN filtration enable/disable function

The configuration of VLAN filtration enable/disable function is shown below:

Step	Command	Command parameter introduction

1	**config**	Enter global configuration mode
2	**interface line/client** *portid*	Enter corresponding physical port configuration mode
3	**switchport ingress-filtering** *(enable| disable)*	Configure port VLAN filtration attribute : enable/diable
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface line/client** [*port-list*] **switchport**	Show port VLAN attribute configuration

19.2.1.7 Configure port protection

The configuration steps are as follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface line/client** *portid*	Enter corresponding physical port configuration mode
3	**switchport protect**	Configure the physical port to protected port **Protect** the protected port
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface line/client protected**	Show physical port protection attribute

Use **no switchport protect** to cannel port protection configuration.

19.2.1.8 Configure port transmission

By default, the port can transmit messages to other ports except its own one, port transmission function supports port list configuration under port, so that the range of the ports that are able to transmit messages can be confined.

To configure transmission port, you need to enter the given port or port range mode, the corresponding commands are as follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface line/client** *portid*	Enter port mode
3	**switchport forwarding allowed portlist** *port-list*	Configure transmission list under port *Port-list*: port list

4	**exit**	Quit from interface mode
5	**exit**	Quit from global configuration mode
6	**show interface line/client** [*port-list*] **switchport**	Show port transmission list

Use **no switchport forwording allowed portlist** to restore port transmission list to default value, that is, all the ports except its own one.

19.2.1.9 Monitoring and maintenance

Command	Command parameter introduction
show interface line/client [*port-list***] switchport**	Show port VLAN attribute configuration
show interface line/client protected	Show physical port protection attribute
show vlan	Show port VLAN attribute configuration

19.2.1.10 Typical configuration example

The topology structure is shown below:

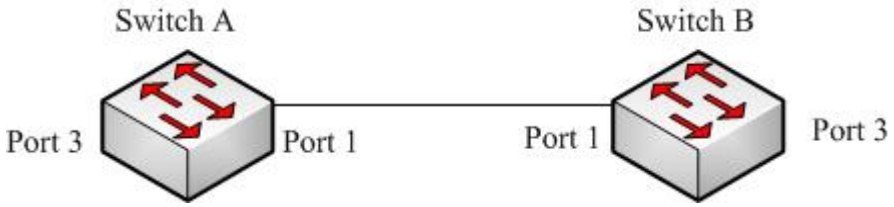


Fig 19-1 topology structure

As is shown in figure 1, the SwitchA and SwtichB use Port1(SwtichA) and Port1(SwitchB) to connect each other, configure Port1 of the two equipments to Trunk port, allowVLAN1-VLAN100 to pass, Port3(SwtichA) and Port3(SwtichB) are Access port, Access VLAN is VLAN6. The configuration of SwitchA and SwitchB are totally the same, now SwitchA configuration will be shown.

SwitchA configuration is as follows:

Raisecom#**config**

Raisecom(config)**#vlan** *6*

Raisecom(config-vlan)**#state** *active*

Raisecom(config-vlan)**#exit**

Raisecom(config)#**interface line/client** *1*

Raisecom(config-port)#**switchport mode trunk**

Raisecom(conifg-port)#**switchport trunk allowed vlan** *1-100*

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

Raisecom(config)#**interface line/client** *3*

Raisecom(config-port)#**switchport mode access**

Raisecom(config-port)# **switchport access vlan** *6*

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

Raisecom(config)#**exit**

Raisecom#**show vlan**

Outer TPID: 0x9100

VLAN	*Name*	*Status*	*VLAN-Priority*	*Ports*
1	*Default*	*active*	*N/A*	*1,2,4-26*
6	*VLAN0006*	*active*	*0*	*3*

Raisecom#**show interface line/client** *1* **switchport**

Port 1:

Administrative Mode: trunk

Operational Mode: trunk

Access Mode VLAN: 1(default)

Tunnel Mode VLAN: 1(default)

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-100

Operational Trunk Allowed VLANs: 1,3-100

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

Raisecom#**show interface line/client** *3* **switchport**

Port 3:

Administrative Mode: access

Operational Mode: access

Access Mode VLAN: 6

Tunnel Mode VLAN: 6

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

19.2.2 VLAN mapping function

VLAN mapping offers CVID for message modification, if the equipment has configured the corresponding mapping rules, the new CVID or SVID that has been mapped will do learning and transmission as transmission VLAN.

19.2.2.1 Default VLAN mapping configuration

Function	Default
Enable/disable port VLAN mapping function	Disable to all

19.2.2.2 Configure VLAN mapping

The steps to enable/disable VLAN mapping function and configure VLAN Mapping rules are shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**vlan-mapping** *vlan-list1* **to** *vlan-list2*	Configure VLAN mapping rule *Vlan-list1* the VLAN ID before mapping *Vlan-list2* the VLAN ID afeter mapping
3	**interface line/client** *portid*	Enter interface configuration mode
4	**vlan-mapping** *{enable|disable}*	Enable VLAN mapping function *Enable* enable VLAN mapping *Disable* disable VLAN mapping
5	**exit**	Quit from physical port mode
6	**exit**	Quit from global configuration mode
7	**show vlan-mapping**	Show VLAN mapping rules
8	**show port** {*all*|*port-list*} **vlan-mapping**	Show all/specified port VLAN mapping function state

	All: all the ports *Port-list*: the specified port or port list

Notice:

- If the number relationship of vlan-list1 and vlan-list2 is N(N>1) to 1, the command will map several VLAN to one VLAN; if it is N to N, then vlan-list1 and vlan-list2 need to be the same in amount in configuration, when doing VLAN mapping the principle of one-one correspondence.
- By default VLAN mapping function is disabled. When VLAN mapping function of the specified port is enabled, the corresponding mapping rule will take effect on the port.

19.2.2.3 Monitoring and maintainenance

Command	Command parameter introduction
show interface line/client [*port-list***] switchport**	Show the transmission list under specified port
show vlan-mapping	Show VLAN mapping rules
show port {*all*|*port-list*} **vlan-mapping**	Show all/ the specified ports VLAN mapping function state *All:* all the ports *Port-list*: specified port or port list

19.2.2.4 Typical configuration example

The topology structure is shown in figure 2:

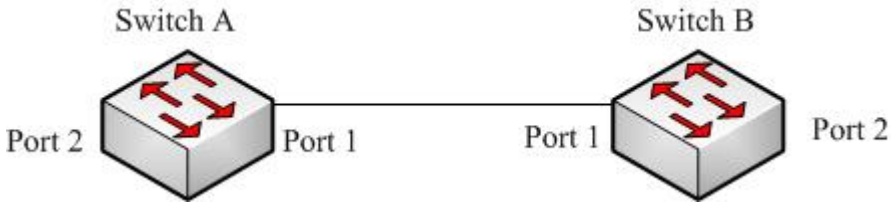


Fig 19-2 the topology structure

As is shown in figure 2, SwitchA and SwitchB use port 1 for connection, the Port1 and Port2 of the two equipments are both trunk port, create VLAN10-20 and 110-120, map vlan10-20 to vlan110-120, enable VLAN mapping function on Port2. The configuration of SwtichA and SwitchB is totally the same, now SwtichA configuration will be shown.

The configuration of SwitchA:

Raisecom#**config**

Raisecom(config)#**create vlan** *10-20, 110-120 active*

Raisecom(config)# **vlan-mapping** *10-20 to 110-120*

Raisecom(config)#**interface line/client** *1*

Raisecom(config-port)# **switchport mode trunk**

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

Raisecom(config)# **interface line/client** *2*

Raisecom(config-port)# **switchport mode trunk**

Raisecom(config-port)#**vlan-mapping** *enable*

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

Raisecom(config)#**exit**

Raisecom#**show vlan-mapping**

Global vlan mapping rules:

Original VLAN IDs Translated VLAN IDs

10-20 110-120

Raisecom#**show port** *1-2* **vlan-mapping**

Vlan Mapping Status:

PORT VLAN-MAPPING STATUS

---

1 disable

2 enable

19.2.3 Basic Q-IN-Q function

19.2.3.1 Default Q-IN-IN configuration

Function	Default
Configure TPID value of outer layer Tag is HHHH	Default TPID value of outer layer Tag is 0x9100
Configure the port ACCESS VLAN ID	1
Configure port VLAN mode	All the ports exists in ACCESS mode in VLAN1.

19.2.3.2 Basic Q-IN-Q configuration

The steps of configuring Q-IN-Q includes: Tpid, access vlan, tunnel port and double tagging configuration, as is shown below:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**mls double-tagging tpid** *HHHH*	Configure the outer layer Tag TPID value to HHHH; *HHHH:* hex outer layer Tag TPID value, it is 1~4 figures hex number, range is 0x0-oxFFFF.
3	**interface line/client** *portid*	Enter port mode

4	**switchport mode** *{access | hybrid [double-tagging|dot1q-tunnel]|trunk [double-tagging]| dot1q-tunnel [hybrid]}*	Configure port VLAN mode **access** ACCESS mode, port exists in the form of UNTAG in the only VLAN; **hybrid** HYBRID mode, the port can exist in several VLAN in UNTAG or TAG mode; **hybrid double-tagging** configure the port to HYBRID mode, so that it can recognize and handle outer layer Tag (SP VLAN Tag); **hybrid dot1q-tunnel** configure the port to HYBRID mode, can make it enable to compulsively adding outer layer Tag(SP VLAN Tag) for the packet entering the port; **trunk** TRUNK mode, the port exists in several VLAN in TAG mode, and exists in Native Vlan in UNTAG mode; **trunk double-tagging** configure the port to TRUNK mode, and enable it the ability to recognize and handle outer layer Tag; **dot1q-tunnel** TUNNEL mode, the data packet entering the port can be added double Tag.
4	**switchport access vlan** *<1-4094>*	Configure the port ACCESS VLAN ID. *<1-4094>* specific port's ACCESS VLAN ID in ACCESS and DOT1Q-TUNNEL mode.
5	**exit**	Return to global configuration mode
6	**show vlan**	Show VLAN configuration
7	**show interface line/client [***port-list***] switchport**	Show port VLAN attribute information

Use **no mls double-tagging tpid HHHH** to restore outer layer Tag TPID to default value:0x9100.

Use **no switchport mode** to restore port VLAN mode to default value, that is ACCESS mode.

Use **no switchport access vlan** mode to restore Access VLAN to default value, that is, port Access VLAN is VLAN 1.

19.2.3.3 Monitoring and maintenance

Command	Command parameter instruction
show vlan [*{1-4094}*]	Show stable VLAN configuration
show interface line/client [*port-list***] switchport**	Show port VLAN attribute configuration

19.2.3.4 Typical configuration example

The topology structure is shown in figure 3:

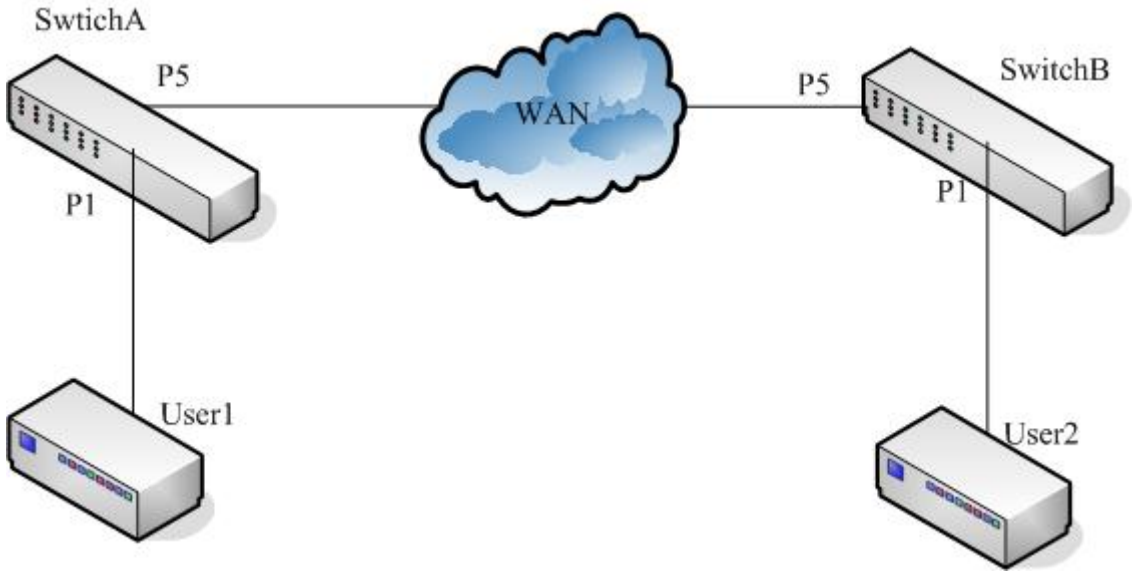


Fig 19-3 topology structure

As is shown in figure 3, SwitchA and SwitchB are operator's access switches, belong to operator network's VLAN100 and VLAN200 respectively. User1 and User2 are user access equipment, SwitchA use P5 port to connect to MAN (metro area network), p1 port connect ot User1, SwitcB use P5 to connect to MAN. P1 connect to User2. MAN TPID is ox8600. Configure SwitchA and SwtichB to realize QinQ function.

SwitchA configuration is shown below:

Raisecom#**config**

Raisecom(config)#**mls double-tagging** *tpid 8600*

Raisecom(config)#**interface line/client** *1*

Raisecom(config-port)#**switchport mode** *dot1q-tunnel*

Raisecom(config-port)#**switchport access vlan** *100*

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

Raisecom(config)#**interface line/client** *5*

Raisecom(config-port)#**switchport mode** *trunk double-tagging*

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

Raisecom(config)#**exit**

Raisecom#**show interface line/client** *1* **switchport**

Port 1:

Administrative Mode: dot1q-tunnel

Operational Mode: dot1q-tunnel

Access Mode VLAN: 100

Tunnel Mode VLAN: 100

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

Raisecom#**show interface line/client** *5* **switchport**

Port 5:

Administrative Mode: trunk double-tagging

Operational Mode: trunk double-tagging

Access Mode VLAN: 1(default)

Tunnel Mode VLAN: 1(default)

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: 1,100

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

SwitchB configuration is shown below:

Raisecom#**config**

Raisecom(config)#**mls double-tagging** *tpid 8600*

Raisecom(config)#**interface line/client** *1*

Raisecom(config-port)#**switchport mode** *dot1q-tunnel*

Raisecom(config-port)#**switchport access vlan** *200*

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

Raisecom(config)#**interface line/client** *5*

Raisecom(config-port)#**switchport mode** *trunk double-tagging*

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

Raisecom(config)#**exit**

Raisecom#**show interface line/client** *1* **switchport**

Port 1:

Administrative Mode: dot1q-tunnel

Operational Mode: dot1q-tunnel

Access Mode VLAN: 200

Tunnel Mode VLAN: 200

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

Raisecom# **show interface line/client** *5* **switchport**

Port 5:

Administrative Mode: trunk double-tagging

Operational Mode: trunk double-tagging

Access Mode VLAN: 1(default)

Tunnel Mode VLAN: 1(default)

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: 1,200

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

19.2.4 Flexible Q-IN-Q function

19.2.4.1 Default flexible Q-IN-Q configuration

Function	Default
Configure port flexible Q-IN-Q VLAN mapping relationship	None

19.2.4.2 Configure flexible Q-IN-Q

Flexible Q-in-Q function is to add outer layer TAG according to inner TAG. Configuring port flexible Q-in-Q function must be within physical port configuration mode, the steps are as follows:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**interface line/client** *portid*	Enter corresponding physical port configuration mode
3	**switchport vlan mapping** *vlan-list* **add-outer** *outer-vlan-list*	Configure the VLAN mapping relationship of port flexible Q-in-Q *vlan-list* inner: layer VLAN ID from client network *outer-vlan-list*: added outer layer VLAN ID
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show vlan mapping**	Show all the VLAN mapping configuration
7	**show interface line/client** [*port-list*] **switchport**	Show port VLAN attribute configuration

Use **no switchport vlan mapping** {all | vlan-list} to delete the VLAN mapping relationship of port Q-in-Q.

Notice:

- To ISCOM2924GF/2926, 768 VLAN mapping can be configured at the most.
- The VLAN mapping relationship of flexible Q-in-Q function configure by this command takes effect only on TUNNEL port, that is, only when the interface mode is TUNNEL, can flexible Q-in-Q function takes effect. The port enters command configured outer layer VLAN in the way of UGTAG, if VLAN do not exist, it will be created automatically. When deleting one Q-in-Q VLAN mapping relationship, if other mapping do not user this outer layer VLAN, delete the port from outer layer VLAN.

19.2.4.3 Monitoring and maintenance

Command	Command parameter instruction
show vlan mapping	Show all the VLAN mapping configuration
show interface line/client [*port-list*] **switchport**	Show port VLAN attribute configuration

19.2.4.4 Typical configuration example

The topology structure is shown below:

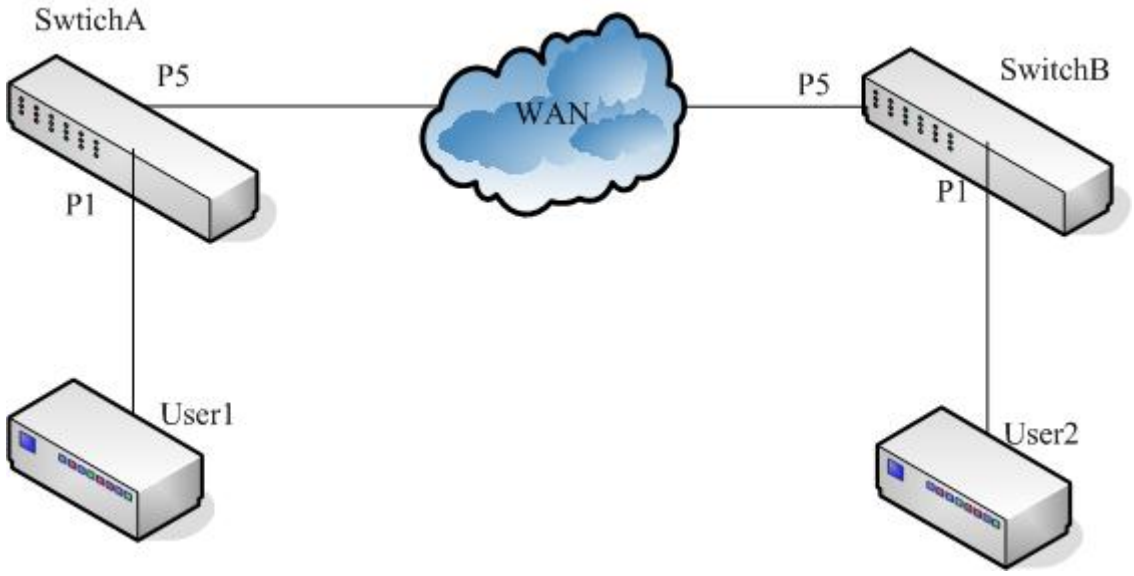


Fig 19-4 topology structure

As is shown in figure 4, SwitchA and SwitchB are operator access switches, they belong to VLAN 100 and VLAN 200 of the operator's network respectively. User1 and User2 are user access equipments, SwitchA user P5 port to connect to MAN (metro area network), P1 connect to User1, SwtichB connect to MAN using P5, P1 connect to User2. MAN TPID is 0x8600. User1 belongs VLAN10, User2 belong to VLAN20, configure SwitchA and SwitchB to relalize flexible Q-in-Q function.

SwitchA configure is shown below:

Raisecom#**config**

Raisecom(config)#**mls double-tagging** *tpid 8600*

Raisecom(config)#**interface line/client** *1*

Raisecom(config-port)#**switchport mode** *dot1q-tunnel*

Raisecom(config-port)#**switchport vlan mapping** *10* **add-outer** *100*

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

Raisecom(config)#**interface line/client** *5*

Raisecom(config-port)# **switchport mode trunk double-tagging**

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

Raisecom(config)#**exit**

Raisecom#**show vlan mapping**

Port Inner VLAN Outer VLAN Hardware

---

1 10 100 Yes

Raisecom#**show interface line/client** *1* **switchport**

Port 1:

Administrative Mode: dot1q-tunnel

Operational Mode: dot1q-tunnel

Access Mode VLAN: 4

Tunnel Mode VLAN: 4

Administrative Tunnel Mode OUTER VLANs of vlan mapping: 100

Operational Tunnel Mode OUTER VLANs of vlan mapping: 100

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

Raisecom# **show interface line/client** *5* **switchport**

Port 5:

Administrative Mode: trunk double-tagging

Operational Mode: trunk double-tagging

Access Mode VLAN: 1(default)

Tunnel Mode VLAN: 1(default)

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: 1,3-6,100

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

SwtichB configuration is shown below:

Raisecom#**config**

Raisecom(config)#**mls double-tagging tpid** *8600*

Raisecom(config)#**interface line/client** *1*

Raisecom(config-port)#**switchport mode dot1q-tunnel**

Raisecom(config-port)#**switchport vlan mapping** *20* **add-outer** *200*

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

Raisecom(config)#**interface line/client** *5*

Raisecom(config-port)# **switchport mode trunk double-tagging**

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

Raisecom(config)#**exit**

Raisecom#**show vlan mapping**

Port Inner VLAN Outer VLAN Hardware

---

1 20 200 Yes

Raisecom#**show interface line/client** *1* **switchport**

Port 1:

Administrative Mode: dot1q-tunnel

Operational Mode: dot1q-tunnel

Access Mode VLAN: 4

Tunnel Mode VLAN: 4

Administrative Tunnel Mode OUTER VLANs of vlan mapping: 200

Operational Tunnel Mode OUTER VLANs of vlan mapping: 200

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

Raisecom# **show interface line/client** *5* **switchport**

Port 5:

Administrative Mode: trunk double-tagging

Operational Mode: trunk double-tagging

Access Mode VLAN: 1(default)

Tunnel Mode VLAN: 1(default)

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: 1,3-6,200

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

19.3 VLAN Function Configuration

19.3.1 Configure VLAN

19.3.1.1 Switching mode introduction

Switching mode can be sorted to 3 types:

- **transparent :**transparent mode
- **vlan:** VLAN transmission mode
- **double-tagged-vlan:** Q-in-Q VLAN mode

In transparent mode, stable VLAN and port VLAN configuration do not take effect actually. When the system transforms from transparent mode to VLAN transmission mode, stable VLAN and port VLAN configuration can actually take effect.

In VLAN transmission mode, stable VLAN and port VLAN configuration take effect directly.

19.3.1.2 Default VLAN configuration

Function	Default value
Create VLAN	Default VLAN
Configure switching mode	Transparent mode
Configure the filtration mode of physical port ingress data packet	No ingress be abandoned.
Configure the data packets that are allowed to be received by physical port	All the data packets are allowed to be received
Configure the handling mode of physical port ingress data packet	No modification to outgress data packet

19.3.1.3 Configure switching mode

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**switch-mode** *{transparent| dot1q-vlan|double-tagged-vlan}*	Configure switching mode **transparent**: transparent mode **vlan**: VLAN transmission mode **double-tagged-vlan:** Q-in-Q VLAN mode
3	**exit**	Return to privileged EXEC mode
4	**show vlan**	Show stable VLAN configuration

Notice:

- In transparent mode, stable VLAN and port VLAN configuration do not take effect actually. In this mode, the system record the configuration done by the commands below, but do not actually carry out them:
  - Vlan
  - Pvid
  - Vlan accept-frame
  - Vlan double-tag
  - Vlan egress default
  - Vlan ingress-filtering
- When the system transforms from transparent mode to VLAN transmission mode, the configuration commands above can really take effect. In VLAN transmission mode, the configurations above will be carried out and take effect directly.

19.3.1.4 Configure VLAN attribute

VLAN attribute configuration includes creating and deleting VLAN.

1. Create VLAN

Create VLAN, and define if out port is UNTAG port in VLAN member group, the steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration
2	**vlan**<2-4094>**{client**[*clientid*]|**line** [*lineid*]**} untagged {client** [*clientid*]|**line** [*lineid*]**}**	Create VLAN Untagged: only out port is allowed to let go data packet without TAG; Client: user end port; Line: line side port *<2-4094>***:** VLAN ID; *Clientid:* user port number *lineid* line port number
3	**exit**	Return to privileged EXEC mode
4	**show vlan**	Show VLAN configuration

2. Delete VLAN

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

Step	Command	Command parameter introduction
1	**config**	Enter global configuration mode
2	**no vlan** {*all* | *<2-4094>*}	Delete VLAN *<2-4094>*: VLAN ID; All: all the stable VLAN except default VLAN (VLAN ID is 1)
3	**exit**	Return to global configuration mode
4	**show vlan**	Show VLAN configuration

19.3.1.5 Enable/disable VLAN filtration

The steps to configure the physical port ingress data packet filtration mode are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {client** *clientid* **| line** *lineid***}**	Enter corresponding physical port configuration mode
3	**vlan ingress-filtering {unknown-vlan| not-member}**	Configure the filtration mode of physical port ingress data packet
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface {client** *client-list* **| line** *line-list***} switchport**	Show VLAN configuration

Use **no vlan ingress-filtering** to restore ingress data packet filtration mode to default value, that is, no ingress packet will be dropped.

19.3.1.6 Configure VLAN accept-frame tagging type

The steps to configure VLAN accept-frame tagging type are as follows:

Step	Command	Command parameter instruction
1	**config**	Enter global configuration mode
2	**interface {client** *clientid* **| line** *lineid***}**	Enter corresponding physical port configuration mode
3	**vlan accept-frame** *{tag|untag}*	Configure physical port accepted data packet Tag: accept only the data packets with TAG Untag: accept only the data packet without TAG
4	exit	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface {client** *client-list* **| line** *line-list***} switchport**	Show VLAN configuration

Use **no vlan accept-frame** to restore VLAN accept-frame tagging type to default value, that is, all the data packets are allowed to receive.

19.3.1.7 Configure outgress mode

The steps to configure the processing mode of physical port outgress data packet are as follows:

Step	Command	Command parameter instruction
1	**config**	Enter global configuration mode
2	**interface {client** *clientid* **| line** *lineid***}**	Enter corresponding physical interface configuration mode
3	**vlan egress default** *{tag| untag|unmodify}*	Configure the processing mode to physical port outgress data packets **Tag** outgress data packet adding TAG **Untag** outgress data packet without TAG **Unmodify** do not modify outgress data packet
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface {client** *client-list* **| line** *line-list***} switchport**	Show VLAN configuration

Notice: If double TAG function is enabled on physical port, the processing mode to physical port outgress data packet will not take effect.

19.3.1.8 Configure PVID

The steps to create and delete port VLAN ID are shown below:

Step	Command	Command parameter introduction
1	**config**	Enter global configuration
2	**interface {client** *clientid* **| line** *lineid***}**	Enter corresponding physical configuration mode
3	**[no] pvid** *<1-4094> [override]*	Create and delete port VLAN ID *<1-4094>*: port VLAN ID number *override*: use PVID value to recover the VLAN ID in the message
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface {client** *client-list* **| line** *line-list***} switchport**	Show VLAN configuration

Use **no pvid** to delete PVID.

19.3.1.9 Monitoring and maintenance

Command	Description
show vlan [{*1-4094*}]	Show stable VLAN configuration
show interface client [*client-list*] **switchport**	Show user port VLAN configuration
show interface line [*line-list*] **switchport**	Show line port VLAN configuration

19.3.1.10 Typical configuration example

Topology structure is shown as figure 5:

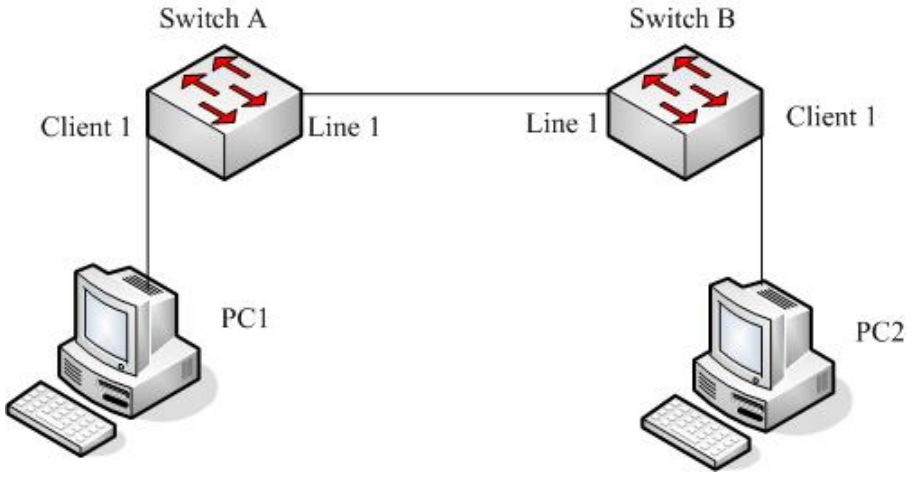


Fig 19-5 topology structure

As is shown in figure 5, Line1 of SwtichB connects with Line1 of SwtichA, configure SwitchA switching mode to vlan transmission mode, and configure Client1 outgress data packet filtration and VLAN accept-frame tagging type.

SwitchA configuration is shown below:

Raisecom#**config**

Raisecom(config)#**vlan** *3* **line** *1* **client** *1*

Raisecom(config)#**switch-mode dot1q-vlan**

Raisecom(config)#**interface client** *1*

Raisecom(config-port)#**vlan accept-frame** *untag*

Raisecom(config-port)#**vlan egress default** *untag*

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

Raisecom(config)#**exit**

Raisecom#**show vlan**

Switch mode: dot1q-vlan

Core tag type: 0x9100

VLAN Ports Untag Ports Priority

---

1 L:1;C:1 L:1;C:1 --

3 L:1;C:1 n/a --

Raisecom#**show interface client** *1* **switchport**

Port client1:

PVID: 1

PVID override: Disabled

Double tag: Disabled

Vlan accept-frame: Untagged

Vlan ingress filtering: None

Egress default : Untagged

SwitchB configuration is shown below:

Raisecom#**config**

Raisecom(config)#**vlan** *3-5* **line** *1* **client** *1*

Raisecom(config)#**switch-mode dot1q-vlan**

Raisecom(config)#**interface client** *1*

Raisecom(config-port)#**vlan accept-frame** *untag*

Raisecom(config-port)#**vlan egress default** *untag*

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

Raisecom(config)#**exit**

Raisecom#**show vlan**

Switch mode: dot1q-vlan

Core tag type: 0x9100

VLAN Ports Untag Ports Priority

---

1 L:1;C:1 L:1;C:1 --

3 L:1;C:1 n/a --

4 L:1;C:1 n/a --

5 L:1;C:1 n/a --

Raisecom#**show interface client** *1* **switchport**

Port client1:

PVID: 1

PVID override: Disabled

Double tag: Disabled

Vlan accept-frame: Untagged

Vlan ingress filtering: None

Egress default : Untagged

19.3.2 Basic Q-in-Q function

19.3.2.1 Basic Q-in-Q default configuration

Function	Default
Configure outer layer Tag TPID value	The default TPID value of outer layer Tag is 0x9100
Enable/disable physical port double TAG function	Double TAG function is disabled

19.3.2.2 Configure basic Q-in-Q

Q-in-Q configuration includes: switching mode, Tpid, PVID and double tagging configuration, the configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**switch-mode** { *transparent*| *dot1q-vlan*|*double-tagged-vlan}*	Configure switching mode to double-tagged-vlan mode **Transparent:** transparent mode **Vlan**: VLAN Transmission mode **double-tagged-vlan**: Q-in-Q VLAN mode
3	**mls double-tagging tpid** *HHHH*	Configure outer layer Tag TPID value to HHHH *HHHH:* hex outer layer Tag TPID value, which is 1~4 figures hex number, range is 0x0-0xFFFF
4	**interface {client** *clientid* **| line** *lineid***}**	Enter corresponding physical interface configuration mode
5	**pvid** *<1-4094> [override]*	Create port VLAN ID *<1-4094> :* port VLAN id override*:* use PVID value to recover message VLAN ID
6	**vlan double-tag**	Enable physical port double TAG function
7	**exit**	Return to global configuration mode
8	**exit**	Return to privileged EXEC mode
9	**show vlan**	Show stable VLAN configuration
10	**show interface {client** *client-list* **| line** *line-list***} switchport**	Show VLAN configuration

Use **no mls double-tagging tpid HHHH** to restore outer layer Tag TPID to default value, 0x9100.

Use **no vlan double-tag** to stop physical port double TAG function.

19.3.2.3 Monitoring and maintenance

Command	Description
show vlan [*{1-4094}*]	Show stable VLAN configuration
show interface client [*client-list*] **switchport**	Show user port VLAN configuration
show interface line [*line-list*] **switchport**	Show line port VLAN configuration

19.3.2.4 Typical configuration example

Topology structure:

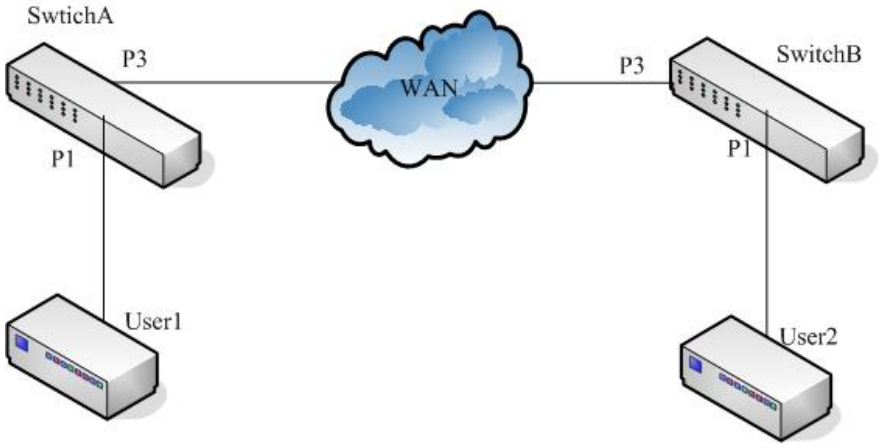


Fig 19-6 topology structure

As is shown in the topology structure, SwitchA and SwtichB are operator access switches, which belongs to VLAN100 and VLAN200 of the operator network. User1 and User2 are user access equipments, SwitchA use P5 to connect to MAN (metro area network), P1 connect to User1, SwitchB use P5 to connect to MAN, P1 connect to User2. Among them, MAN TPID is 0x9600. Configure SwtichA and SwtichB to realize basic Q-in-Q function.

SwitchA configuration is as follows:

Raisecom#**config**

Raisecom(config)#**switch-mode double-tagged-vlan**

Raisecom(config)#**mls double-tagging tpid** *9600*

Raisecom(config)#**interface client** *3*

Raisecom(config-port)#**pvid** *100*

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

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

Raisecom(config)#**exit**

Raisecom#**show vlan**

Switch mode: double-tagged-vlan

Core tag type: 0x9600

VLAN Ports Untag Ports Priority

---

1 L:1;C:1-4 L:1;C:1-4 --

3 C:3 n/a --

5 L:1 n/a --

Raisecom#**show interface client** *3* **switchport**

Port client3:

PVID: 100

PVID override: Disabled

Double tag: Enabled

Vlan accept-frame: All

Vlan ingress filtering: None

Egress default : Unmodify

SwitchB configuration is as follows:

Raisecom#**config**

Raisecom(config)#**switch-mode double-tagged-vlan**

Raisecom(config)#**mls double-tagging tpid** *9600*

Raisecom(config)#**interface client** *3*

Raisecom(config-port)#**pvid** *200*

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

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

Raisecom(config)#**exit**

Raisecom#**show vlan**

Switch mode: double-tagged-vlan

Core tag type: 0x9600

VLAN Ports Untag Ports Priority

---

1 L:1;C:1-4 L:1;C:1-4 --

5 L:1 n/a --

6 C:2 n/a --

Raisecom#**show interface client** *3* **switchport**

Port client3:

PVID: 200

PVID override: Disabled

Double tag: Enabled

Vlan accept-frame: All

Vlan ingress filtering: None

Egress default : Unmodify

19.4 VLAN configuration

19.4.1 VLAN based on port

The device switch mode can be configured into two types, transparent mode and dot1q-vlan mode.

In transparent mode, static VLAN and VLAN configuration under port does not actually work. Only when the system transforms from transparent mode to dot1q-vlan mode can static VLAN and port VLAN configuration under port takes effect.

In dot1q-vlan mode, static VLAN and VLAN configuration under port takes effect directly.

19.4.1.1VLAN port mode introduction

Member port mode	VLAN member attribution
ACCESS	In Access mode, by default only VLAN1 data packets are allowed to pass the port, and the data packets sent from the port do not take VLAN 1 tag. Access port mode can be designated to multi-VLAN, but the data packets sent from access port do not take VLAN tag. Access port is mainly used to connect terminal user.
TRUNK	In trunk mode, all the VLAN packets are allowed to pass by default, and all the data packets except VLAN 1 transmitted from the have tag. Trunk mode can be designated to multi-VLAN, and user can configure if the data packet with a certain VLAN tag should be transmitted from the port. When the switch is used as the uplink tag port, it can be configured to trunk mode

19.4.1.2Default VLAN configuration

Function	Default
Device switch mode	transparent
Create static VLAN	Default VLAN and cluster VLAN exist in the system, that is VLAN1 and VLAN2, all the ports exist in VLAN1.
VLAN name	System default VLAN name is ‘default’, other static VLAN name is ‘VLAN’ added its 4 figures VLAN ID
Static VLAN activity state	Newly created static VLAN activity state is suspend.
VLAN priority	No priority
Port mode	Access
ACCESS VLAN	VLAN 1
ACCESS VLAN override	Disable

The VLAN that is allowed to pass the port in access mode	VLAN 1
The Native VLAN of trunk port	VLAN 1
The VLAN that is allowed to pass VLAN in port VLAN mode	All VLAN
The UNTAG VLAN that is allowed to pass VLAN in port trunk mode	VLAN 1

19.4.1.3Configure switch mode

Step	Command	Description
1	**config**	Enter global configuration mode
2	**switch-mode** *{transparent| dot1q-vlan}*	Configure switch mode
3	**exit**	Return to privileged EXEC mode
4	**show vlan**	Show static VLAN configuration

Attention:

- In transparent mode, the device transmits data packets without the limitation of VLAN, the system records but do not actually execute the following configuration:
  - Static VLAN will be created and enabled
  - VLAN priority
  - Port access VLAN and override
  - Port access egress-allowed VLAN
  - Port trunk native VLAN
  - Port trunk allow VLAN, port trunk untag VLAN
  - Port mode
  - QinQ configuration

19.4.1.4Configure VLAN attribution

VLAN attribution includes to create, delete VLAN, configure VLAN name, priority, and active state. The steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**create vlan** {2-4094} **(active|suspend) [priority** <0-7>**]**	Create VLAN, confirm the state (active/suspend),configure the priority Active: active state Suspend: hang-up state 0-7: VLAN priority {2-4094}: VLAN ID
3	**name** *WORD*	Name VLAN *WORD* VLAN name, no longer than

		15 characters
4	**state** *{active | suspend}*	Configure VLAN activity state
5	**exit**	Return to global configuration mode
6	**exit**	Return to privileged EXEC mode
7	**show vlan**	Show VLAN configuration

Use **no vlan** *<2-4094>* to delete VLAN in global configuration mode.

Attention:

- The newly created VLAN using VLAN <1-4094> is in suspend state, if user hopes to make it active in the system, the command **state** that will be introduced later can help.
- By default there are two VLAN in the system, that is default VLAN (VLAN1) and cluster VLAN (VLAN2), all the ports belongs to the default VLAN. Default VLAN is not allowed to be deleted. To learn more about cluster VLAN, ref. 19-cluster management function.
- By default, the default VLAN (VLAN1) name is 'Default', other static VLAN name is 'VLAN' added with 4 figure VLAN ID, for example the default name of VLAN 3is 'VLAN0003', the default name of VLAN 4094 is 'VLAN4094'.
- Only when a VLAN be activated in the system can it be active. When VLAN active status is suspend, user can configure the VLAN, like to delete/add port, configure VLAN priority, the system will keep the configuration, once the VLAN is activated, the configuration will take effect in the system.

19.4.1.5Configure VLAN priority

By default, there is no priority when creating VLAN, N/A will be shown, VLAN priority range is 0-7. The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**vlan** *<1-4094>*	Create VLAN and enter its configuration mode *<1-4094>* VLAN ID
3	**priority** *<0-7>*	Configure VLAN priority 0-7: VLAN priority
4	**exit**	Return to privileged EXEC mode
5	**show vlan**	Show VLAN configuration

Use **no vlan***{2-4094}* **priority** in global configuration mode, or **no priority** in VLAN mode to delete VLAN priority.

Attention:

- Default VLAN (VLAN1) has no configuration priority.
- The new created VLAN has no priority be default, and shows N/A. VLAN priority range is 0-7.
- VLAN priority takes effect only when the VLAN is activated. When VLAN is not created or when the state is suspend, user can configure the VLAN priority for still, and the system will keep the configuration and enable the configuration when the VLAN is activated.
- When VLAN priority is configured, the device uses VLAN priority to form a queue or cover message COS value when transmitting VLAN messages. Use **mls qos vlan (priority-set |**

cos-voerride) and **mls qos vlan priority-set cos-override** for specific configuration. If VLAN priority is deleted or if VLAN is not activated, the commands above will not take effect either. Ref. 27-QoS configuration guide for QoS commands.

19.4.1.6Configure port VLAN mode

Port VLAN mode configuration includes port mode, ACCESS VLAN, ACCESS mode allowed VLAN list, TRUNK local VLAN, TRUNK allowed VLAN list, TRUNK UNTAG VLAN list and so on.

You must to configure port VLAN mode in physical interface configuration mode, the steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface line/client** *portid*	Enter corresponding physical interface configuration mode
3	**switchport mode {access | trunk}**	Configure port VLAN mode
4	**switchport access vlan** *<1-4094>* **[override]**	Configure port ACCESS VLAN 1-4094: VLAN ID Override: VLAN override
5	**Switchport access egress-allowed vlan** { **all** | *vlan-list* | **add** *add-vlan-list* | **remove** *remove-vlan-list***}**	Configure the VLAN that Access port allows to pass **All**, all the VLAN are allowed to pass; *Vlan-list*, VLAN that is allowed to pass, the existed configuration will be covered directly **Add** *add-vlan-list*, add allowed VLAN on the base of existed allowed VLAN **Remove** *remove-vlan-list*, delete allowed VLAN on the base of existed allowed VLAN
6	**switchport native vlan** *<1-4094>*	Configure Native VLAN for Trunk port
7	**switchport trunk allowed vlan** { **all** | *vlan-list* | **add** *add-vlan-list* | **remove** *remove-vlan-list***}**	Configure the VLAN that is allowed to pass Trunk port **All** allow all the VLAN to pass *Vlan-list*, allow the passed VLAN ,cover the existed configuration directly; **Add** *add-vlan-list*, add allowed VLAN on the base of the existed allowed VLAN **Remote** *remote-vlan-list*, delete allowed VLAN on the base of the existed allowed VLAN
8	**switchport trunk untagged vlan** { **all** | *vlan-list* | **add** *add-vlan-list* | **remove** *remove-vlan-list***}**	Configure the Untagged VLAN that is allowed to pass Trunk port, **All**, all the VLAN are allowed to pass; *Vlan-list*, the VLAN that are allowed to pass, the existed configuration will be covered directly

9	**exit**	Return to global configuration mode
10	**exit**	Return to privileged EXEC mode
11	**show interface line/client** *[port-list]* **switchport**	Show port VLAN attribution configuration

Use **no switchport mode** to restore port VLAN to default value. Use **no switchport access vlan** to restore Access VLAN to default value, which is to configure port Access VLAN to VLAN1. Use **no switchport trunk native vlan** to restore the Native VLAN of Trunk port to default value, or VLAN1. Use **no switchport trunk allowed vlan** to restore the VLAN that is allowed to pass through Trunk port to default value, all the VLAN can pass. Use **no switchport trunk untagged vlan** to restore the Untagged VLAN that is allowed to pass Trunk port, only VLAN1 shall pass.

When the user is configured the VLAN or UNTAG VLAN that is allowed to pass, user will be noticed 'please input 'y' to confirm the allowed VLAN', input 'y/Y' or press ENTER directly for confirmation, then the configured value will take effect, or the configuration will not take effect when user input other value.

Notice:

- By default, all the ports allow default VLAN (VLAN1) to pass, and all the data packets of the default VLAN transmitted from the ports do not take the corresponding VLAN TAG.
- In port Access mode, no matter how the VLAN list that is allowed to pass Access port is configured, the port allows the data packets of Access VLAN to pass, and the packets sent out do not take corresponding VLAN TAG.
- In port Access mode, when configuring Access VLAN, if the VLAN is not created and activated, the system will create and enable the VLAN automatically.
- In port Access mode, if Access VLAN is deleted or hanged up by user, the system will configure the port Access VLAN to default VLAN (VLAN1).
- In port Trunk mode, no matter the configuration of the VLAN list that is able to pass Trunk port and Untagged VLAN list, the port allows the data packets of NATIVE VLAN to pass, and the transmitted data packets do not take corresponding VLAN TAG.
- In port Trunk mode, when configured Native VLAN, if the VLAN is not created or enabled, the system will create and enable the VLAN automatically.
- In port Trunk mode, if Native VLAN is deleted or blocked by user, the system will set the port Trunk Native VLAN to default VLAN (VLAN1) automatically.
- In port Trunk mode, if the configured Native VLAN is not default VLAN, while the VLAN list that allows passing Trunk port includes not default VLAN, then the port will not allow default VLAN data packets pass.
- Configuring Trunk allowed VLAN list and Trunk Untagged VLAN list is related. When configuring Trunk allowed VLAN list, the system will delete the not allowed VLAN in Trunk Untagged VLAN list; when configuring Trunk Untagged VLAN list, the system will add all Untagged VLAN to Trunk allowed VLAN.
- Access VLAN and Trunk Native VLAN can not be configured to cluster VLAN.
- The VLAN list that is allowed to pass Access port, Trunk allowed VLAN list and Trunk Untagged VLAN list takes effect only to static VLAN, not to cluster VLAN, GVRP static VLAN.

19.4.1.7Configure port protection

The steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode

2	**interface line/client** *portid*	Enter corresponding physical interface configuration mode
3	**switchport protect**	Configure physical port to protected port **Protect** protected port
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show interface line/client protected**	Show physical port protection attribution

Use **no switchport protection** to cancel port protection configuration.

19.4.1.8Configure port forwarding

By default, the port is able to transmit messages to all other ports except to the port itself. The function supports configuring port list under port to limit the port range that could transmit messages.

To configure forwarding port, you need to enter the designated port or range port mode, the commands are shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface line/client** *portid*	Enter port mode
3	**switchport forwarding allowed portlist** *port-list*	Configure port forwarding list
4	**exit**	Quit from port mode
5	**exit**	Quit from global mode
6	**show interface line/client [*port-list*] switchport**	Show port forwarding list

Use **no switchport forwarding allowed** *portlist* to restore the forwarding list under port to default value, that is all the other ports except the port itself.

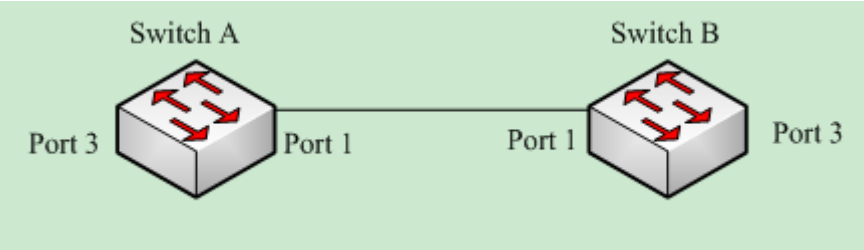
19.4.1.9Monitoring and maintenance

Command	Description
show interface line/client [*port-list***] switchport**	Show port VLAN attribution configuration
show interface clinet clinetid switchport	Show the client port VLAN attribution
show interface line lineid switchport	Show line port VLAN attribution
show interface line/client protected	Show the protected port attribution of the physical port

show vlan	Show port VLAN attribution

19.4.1.10 Typical configuration

The topology:



As is shown in the figure above, SwitchA and SwtichB use Port1(SwitchA) and Port1(SwitchB) to connect each, configure Port1 of the two devices to Trunk port, allowing VLAN1-VLAN100, configure Port3(SwitchA) and Port3(SwitchB) to Access port, Access VLAN to VLAN6. The configuration of SwitchA and SwtichB is totally the same. The configuration step of SwtichA is shown below:

Configuration of SwitchA:

Raisecom#**config**

Raisecom(config)**#vlan 6**

Raisecom(config-vlan)**#state active**

Raisecom(config-vlan)**#exit**

Raisecom(config)#**interface line/client 1**

Raisecom(config-port)#**switchport mode trunk**

Raisecom(conifg-port)#**switchport trunk allowed vlan 1-100**

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

Raisecom(config)#**interface line/client 3**

Raisecom(config-port)#**switchport mode access**

Raisecom(config-port)# **switchport access vlan 6**

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

Raisecom(config)#**exit**

Raisecom#**show vlan**

VLAN Name State Status Ports Untag Ports Priority Creation Time

---

1 Default active static 1-26 1-26 -- 0:0:32

2 active other 1-26 n/a -- 0:0:35

6 VLAN0006 active static 1,3 3 -- 4:32:23

Raisecom#**show interface line/client** *1* **switchport**

Port 1:

Administrative Mode: trunk

Operational Mode: trunk

Access Mode VLAN: 1

Administrative Access Egress VLANs: 1

Operational Access Egress VLANs: n/a

Trunk Native Mode VLAN: 1

Administrative Trunk Allowed VLANs: 1-100

Operational Trunk Allowed VLANs: 1,6

Administrative Trunk Untagged VLANs: 1

Operational Trunk Untagged VLANs: 1

Raisecom#**show interface line/client** *3* **switchport**

Port 3:

Administrative Mode: access

Operational Mode: access

Access Mode VLAN: 6

Administrative Access Egress VLANs: 1

Operational Access Egress VLANs: 1,6

Trunk Native Mode VLAN: 1

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Trunk Untagged VLANs: 1

Operational Trunk Untagged VLANs: n/a

Chapter 20 Storm Control

20.1 Storm control introduction

A packet storm occurs when a large number of broadcast, unicast, or DLF packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. Storm control is configured for the switch as a whole but operates on a per-port basis. By default, storm control is enabled.

20.2 The default configuration for storm control function

By default, storm control is enabled for unicast DLF packets, broadcast packets and mulicast packets.

20.3 Storm control function configuration

20.3.1 Enable/disable storm control function

The configuration is to enable/disable storm control

Step	Command	Description
1	**config**	Global configuration mode
2	**storm-control {***broadcast* | *multicast* | *dlf* | *all***}** *{enable | disable}*	Enable/disable broadcast packet, multicast packet and DLF packet Broadcast DLF broadcast packet Multicast DLF multicast packet Dlf DLF packet All broadcast, multicast and DLF unicast packets.
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show storm-control**	Show storm control state

20.3.2 Storm control number

Configure storm control threshold, unit is kbps (kbit per second).

Step	Command	Description
1	**config**	Enter global configuration mode
2	**storm-control bps** *value*	Set storm control threshold. Value stands for the kbit number that is allowed to pass per second, range can be found on the command manual.

3	**exit**	Quit global configuration mode and enter privileged EXEC mode.
4	**show storm-control**	Show storm control state.

Configure storm control threshold, unit is pps (packet per second).

Step	Command	Description
1	**config**	Enter global configuration mode
2	**storm-control pps** *value*	Set storm control threshold. Value the storm packet number that is allowed to pass per second, range is 0-262143.
3	**exit**	Quit global configuration mode and enter privileged EXEC mode.
4	**show storm-control**	Show storm control state.

Set storm control threshold for broadcast, multicast and DLF packets, unit is %

Step	Command	Description
1	**config**	Enter global configuration mode
2	**torm-control ratio** *<1-100>* **[** *<0-512>* **]**	Set storm control threshold for broadcast, multicast and DLF packets, unit is % 1-100 the bandwidth proportion of the storm packet 0-512 burst value, unit is Kbps;
3	**exit**	Quit global configuration mode and enter privileged EXEC mode.
4	**show storm-control**	Show storm control state.

20.4 Monitoring and maintaining

Command	Description
show storm-control	Show storm control state

20.5 Typical configuration example

Example 1: disable storm control to broadcast packet

Raisecom#**config**

Raisecom(config)# **storm-control broadcast** *disable*

Raisecom(config)#**exit**

Raisecom#**show storm-control**

Broadcast: Disable

Multicast: Enable

Unicast destination lookup failed(DLF): Enable

Threshold: 1024 pps

Example 2: set storm control threshold value to 200kbps

Raisecom#**config**

Raisecom(config)# **storm-control** *bps 200*

Raisecom(config)#**exit**

Raisecom#**show storm-control**

Broadcast: Disable

Multicast: Enable

Unicast destination lookup failed(DLF): Enable

Threshold: 200 Kbps

Example 3: set storm control threshold to 2000.

Raisecom#**config**

Raisecom(config)# **storm-control** *bps 2000*

Raisecom(config)#**exit**

Raisecom#**show storm-control**

Broadcast: Disable

Multicast: Enable

Unicast destination lookup failed(DLF): Enable

Threshold: 2000 pps

Chapter 21 QoS

21.1 Configuration Description

This configuration paper is suit to the following situations:

For transceiver device: to guide the user to configuration QoS function except for Policy and class function;

For Switch device: to guide the user to configuration most Qos function on the most Switch device , except for some exception. User can look up the QoS function command one to the QoS function command nine to see the details.

21.2 QoS Introduction

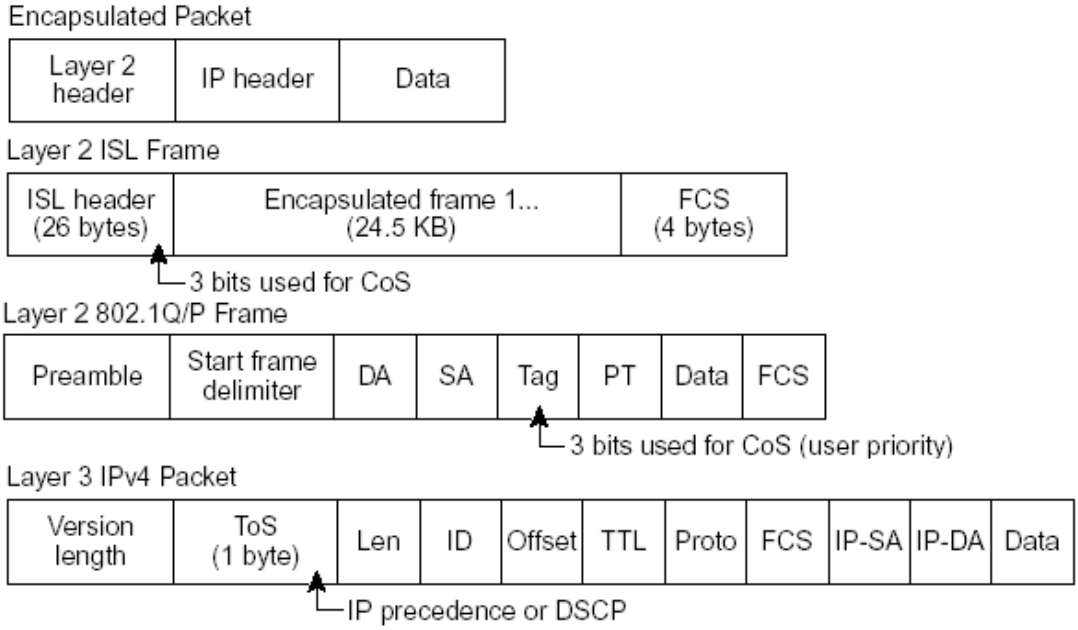
21.3.1 Introduction

Generally speaking, Internet (Ipv4 standard) provides users only “best effort” service, cannot guarantee a real-time and complete packets transmission, and the quality of services either. Since user always has different requirements for the transmission quality of separate multi-media applications, network resources should be redistributed and scheduled according to user’s demands. By using network quality of service, user is able to process specific data traffic with higher priority, or applies particular management schedule strategy to make the network more predictable and the bandwidth management more effective.

1. QoS Basis

ISCOM2800 mechanism realizes layer-2 packets classification based on 802.1P and 802.1Q standards. 802.1Q defines VLAN, though QoS is not defined in this standard, the given mechanism which mention than the frame precedence can be modified configures a strong groundwork to realize QoS. 802.1P standard defines priority mechanism. If packets with high priority have not been transmitted, packets with low priority will not be transmitted.

In Layer-2 802.1Q frame header, there are 2 bytes of TAG control information string, the first 3 bits carry CoS (Class of Service) value, the values is from 0 to 7, shown in the figure below:



The 8 priority defined by CoS can be considered as the following 8 kinds of packets: Priority	Message type	Application
000	Routine	Level 0 corresponds to the default of the best efforts of the information delivery
001	Priority	Level 1 ~ 4 are corresponds for the definition of multi-media data or important enterprise data.
010	Intermediate	
011	Flash	
100	Flash Override	
101	Critical	Level 5 or 6 is used in the sensitive-delay inter-act video/audio data
110	Internet Control	
111	Network Control	Level 7 is applied for the important high-level network data stream, such as routing information

2. QoS basic mode

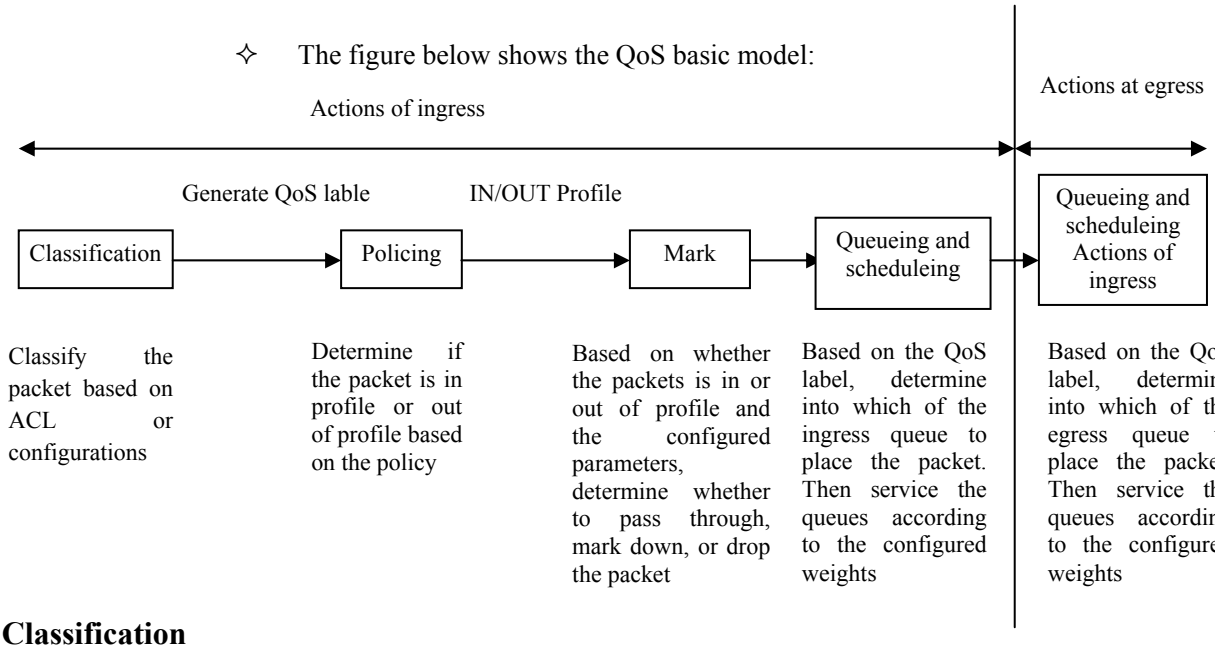
✧ Actions at ingress ports include traffic classification, policing and marking:

- Classifying: to classify the traffic. This process generates a inner DSCP to identify the data's QoS characteristics.
- Policing: Comparing inner DSCP and configured policies to determine whether the packet goes into the policy profile or out. Policy limits the occupied bandwidth. The results will be sent to marker.
- Marking: Evaluates the policy and configuration information for the action to be taken when a packet is out of profile and determines what to do with the packet (pass through a packet without modification, mark down the QoS label in the packet, or drop the packet).

✧ Actions at the egress port include queueing and scheduling:

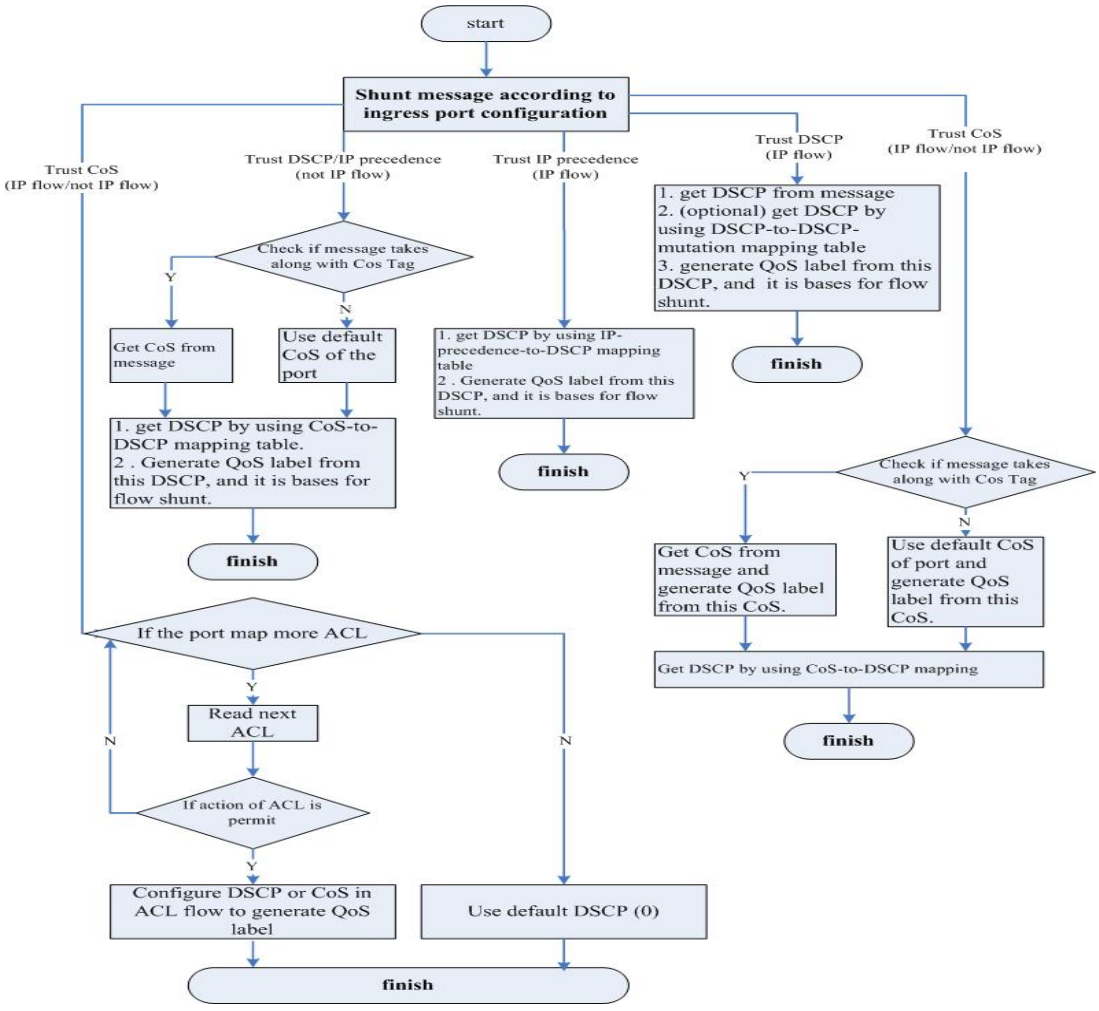
- Queueing: evaluates the QoS packet label and the corresponding DSCP before selecting which queues to use. The DSCP value is mapped to an inner CoS value for the seletion of an output queue.
- Scheduling: based on configured WRR (Weighted round robin) and threshold to provide service for output queue.

✧ The figure below shows the QoS basic model:



21.3.2 Classification

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet.Classification works only when the global QoS function is enabled. QoS is disabled by default.You specify which fields in the frame or packet that you want to use to classify incoming traffic.



Description:

✧ For none-IP traffic, the classification procedure is as follows:

- Use port default value: if the data frame does not have CoS value, assign the incoming frame with the port default Cos value, and then use CoS-to-DSCP map to generate inner DSCP value.
- TRUST the CoS value of input frame (configure the port as TRUST COS): use configurable CoS-to-DSCP mapping table to generate inner DSCP value. For none-IP traffic, whether to configure it as DSCP TRUST and IP precedence TRUST is meaningless, system will use port default CoS value.
- Based on configured Layer-2 MAC ACL classification, check the source MAC, destination MAC and Ethernet field. If there is no configured ACL, assign the default DSCP value as 0. Otherwise, assign DSCP value to the incoming frame based on policy mapping table.

  ✧ For IP traffic:

- TRUST IP DSCP value of incoming packets (configure the port as TRUST DSCP): use DSCP of IP packets as the inner DSCP value. You can use DSCP-to-DSCP mapping table to modify the DSCP value if the port is edge port of two QoS domains.
- TRUST IP precedence of incoming packet (configure the port as TRUST IP precedence): use IP-precedence-to-DSCP mapping table to generate DSCP value.
- TRUST CoS value of incoming packets: use CoS-to-DSCP mapping table to generate DSCP value.
- Based on configured IP ACL for classification, check every field in IP packet header. If no ACL is configured, assign the default DSCP value as 0 to the packet. Otherwise, to assign DSCP value to the packet according to policy map.

As described in the diagram, not only we can classify the traffic by different traffic configuration port "TRUST", and the message CoS, DSCP, IP-precedence; but also we can classify the traffic more flexible by the ACL function, class-map.

Attention: The use of two classification ways are multually exclusive and later configuration will take effects.

Class-map mechanism describe data flow classification on ACL:

1. Classification based on QoS ACL:

1) If a matched permit ACL (the first one) is found, related QoS actions will be activated.

2) If a matched deny ACL is found, ignore this one, and go on to the next one.

3) If all ACLs are checked but no matched permit ACL, packet will not be processed.

4) When matching multiple ACLs, implement QoS processing as the first permit ACL is found.

5) After defining an ACL claasification, user can bond it to a policy. Policies include class classification (such as aggregation) or rate limiting, bond the policy to a port before taking effects.

2. Classification based on class-map:

A class map is a mechanism that you use to isolate and name a specific traffic flow (or class) from all other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it:

1) by ACL match

2) by DCSP, IP priority match.

21.3.3 Policy and Marking

1. Policy map

Each policy may have a lot of class-maps, to identify those flow movements.

2. Policy action

In each policy, different actions identify different flow movements. So far, there are 6 actions:

- TRUST: the TRUST status of flow as TRUST CoS, DSCP and ToS;
- Set: modify the data packets of flow into new value include CoS, DSCP, ToS;
- Policy: limit the speed of streams and modify them, also notice what actions are going to use if the flow is over speed limit.
- Set VLAN: VLAN coverage.
- Re-direct to port: redirect message.
- Copy-to-mirror:flow image.

3. Policy Application

A policy mapping is needed to binding on the IN/OUT port to be effective.

21.3.4 Bit-Rate Limitation and Reshaping

QoS uses policy for speed limiting and reshaping, also modify the DSCP data packet or byte losing.

1. Three types of policy:

single-policy: each rule of class-map is using this policy individually.

class-policy: all rules of each class-map are sharing this policy.

aggregate-policy: all class-map of one policy-map are sharing this policy.

If the flow bit rate is out profile, each policy will have two actions: either drop or marked down DSCP value.

2. Policy uses token bucket algorithm

When the switch receives a frame, a token will be added on the bucket. According to the indicated average bit rate, each token is added on the bucket after the swtich checked the available space on the bucket. If not, the packet will be marked as nonconforming, then follow the policy actions(drop or modify). Moreover, burst will cause the actions as well.

21.3.5 Mapping Table

During QoS processing, switch describes the inner DSCP precedence for all traffics:

1. During the classification procedure, QoS use configured map table (CoS-to-DSCP 、IP-precedence-to-DSCP), based on the CoS or IP precedence value in the incoming packet to obtain an inner DSCP value; To configure DSCP TRUST status on port, if the DSCP values are different in the two QoS domains, use can use DSCP-to-DSCP-mutation map to modify DSCP value.
2. During the policing procedure, QoS can assign new DSCP values to IP or non-ip packets (if the packet is out of profile and the policy has indicated mark down action), this map is called policed-DSCP mapping.
3. Before traffics go into the scheduling, QoS use DSCP-to-CoS map to obtain CoS value according to inner DSCP value, and then use CoS-to-egress-queue map to select the egress queuing.

Attention: If the map table of DSCP-to-DSCP-mutation and policed-DSCP is empty, the default will be the DSCP value of incoming packet;

DSCP-to-DSCP-mutation mapping table is applied for the port, other mapping tables are applied for the

switch.

21.3.6 Queueing and Scheduling

Queueing and scheduling will be carried out for packets processing after policing and marking. ISCOM switch realizes two kinds of processing according to different classified packets:

1. Regenerate packet COS value according to the defined rules while maintaining the packet's native COS value

2. The policy is effective only when the rules are configured as relying on TOS value, that is to say: modify the packet's native COS value according to TOS value.

ISCOM series switches support 4 kinds of priority output queues, the priority values are 0-3. The highest priority is level 3; the switch also supports 3 kinds of queue scheduling policies: strict priority scheduling, control forward weight scheduling and control forward delay scheduling.

ISCOM serises switches also support the processing of untagged Layer-2 frame. Every port has default priority which is COS value. When the port receives an untagged packet, the switch will consider the port default priority as the packet's COS value for queue dispatching and scheduling. After the packet goes out of the switch, it will Renew to the original format.

21.3.7 QoS Default Configuration

No.	Attribute	Default configuration
1	QoS enable	Disable
2	Global QoS Trust Status	UNTRUST
3	Port QoS Trust Status	UNTRUST
4	Port Default CoS	0
5	Port Default DSCP	0
6	Port Default CoS override	Disable
7	Port Default DSCP override	Disable
8	class-map match type	match-all
9	Policy Trust Status	DSCP
10	Queue scheduling policy	Strict priority secheduling SP

CoS-DSCP default map:

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

IP-Precedence-DSCP default map:

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

DSCP-CoS default map:

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

DSCP-to-DSCP-Mutation default map(default-dscp):

DSCP	0	1	2	3	4	5	6	7
0	8	9	10	11	12	13	14	15
1	16	17	18	19	20	21	22	23
2	24	25	26	27	28	29	30	31
3	32	33	34	35	36	37	38	39
5	40	41	42	43	44	45	46	47
6	48	49	50	51	52	53	54	55
7	56	57	58	59	60	61	62	63

Inner CoS to queue map:

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

21.3 QoS Enable and Disable

21.3.1 QoS Start and Stop Default Configuration

No.	Attributes	Default configuration
1	QoS start	Disable

21.3.2 QoS Start and Close Default Configuration

Under the default situation, QoS is disabled. Use the command below to enable QoS function under global configuration mode.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mls qos**	Enable QoS
3	**Exit**	Back to privileged EXEC mode
4	**show mls qos**	Show QoS configuration status

In order to diable QoS, implement command **no mls qos**.

Before enabling QoS, some functions are still effective, such as port default CoS, port default DSCP, queue scheduling mode, CoS to queue map and so on. Users are suggersted to disable the flow control function before enabling QoS.

21.3.3 Monitoring and Maintenance

Command	Description
show mls qos	Show QoS switch status

21.3.4 Configuration Examples

Open QoS function:

Raisecom#**config**

Raisecom(config)#**mls qos**

Raisecom#**show mls qos**

Show as below:

QoS is enabled.

21.4 Classification Function Configuration

21.4.1. Classification Default Configuration

Function	Default
Global QoS TRUST status	UNTRUST
Port QoS TRUST status	UNTRUST
Port default CoS	0
Port default DSCP	0
Port default CoS override	Disable
Port default DSCP override	Disable
Class-mapbmatch type	match-all

21.4.2. Flow Classification Configuration Based on Port TRUST Status

Attention:

- Port TRUST status and ACL/Class-map flow classifation are mutually exclusive, and later configuration will take effects.
- Global and port QoS TRUST status configurations are used for different devices. So far, it is not capable for those two configurations in one equipement.
- QoS TRUST status configuration and TRUST policy status configuration are mutually exclusive, and later cofniguration will take effects

21.4.2.1 Configuring Global QoS TRUST status

Configure QoS TRUST status for all ports. Reverse command: **no mls qos TRUST.**

Steps	Command	Description
1	**Config**	Entry to global configuration mode
2	**mls qos TRUST [***cos* | *dscp* | *ip-precedence***]**	All QoS TRUST status ports configuration *cos*: configuration the switch as TRUST CoS status *dscp*: configuartion the switch as TRUST DSCP status *ip-precedence*: configuration the switch as TRUST IP priority status.
3	**Exit**	Return to privileges mode
4	**show mls qos port**	Show QoS port configuration

Configuration example:

Raisecom#**config**

Raisecom(config)#**mls qos** *TRUST* **cos** //**configure port** *TRUST* **status**

Raisecom(config)#**exit**

Raisecom# **show mls qos port**

Show results as:

TRUST state: TRUST CoS

Port Id Default CoS

---

1 0

2 0

……

21.4.2.2 Configuring QoS port TRUST status

configure QoS port TRUST status. In default situation, the switch TRUST status is UNTRUST. Reverse Command is: **no mls qos TRUST.**

Steps	Command	Description
1	**config**	Entry to global configuration mode
2	**interface line/client** *portid*	Entry to port configuration mode
3	**mls qos TRUST [***cos* | *dscp***]**	Set QoS TRUST mode cos: set port as TRUST CoS status dscp:set port as TRUST DSCP status
4	**Exit**	Return to global configuration mode
5	**Exit**	Return privileges mode
6	**Show mls qos port** *portid*	Show QoS port configuration

21.4.2.3 Configuring CoS port default

Only if the port TRUST status is CoS, configuring default CoS takes effects. When the message is untag, CoS default port as CoS value. In default situation, that value will be 0。Reverse command: **no mls qos default-cos**。It can be set under port mode.

Steps	Command	Description
1	**config**	Entry to global configuration mode
2	**interface line/client** *portid*	Entry to port cofiguration mode
3	**mls qos default-cos** *cos-value*	Set default CoS value CoS-value: set default port CoS value 0-7
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileges mode
6	**Show mls qos port** *portid*	Show QoS port configuration

Configuration example: in Port 1, configure TRUST status as CoS, and when the incoming message is as untag, the CoS value will be 2.

Raisecom#**config**

Raisecom(config)#**inter port** *1*

Raisecom(config-port)#**mls qos** *TRUST cos* //configure port TRUST status

Raisecom(config-port)# **mls qos default-cos** *2* //configure CoS port default

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

Raisecom(config)#**exit**

Raisecom# **show mls qos port** *1*

Show results as:

Raisecom#**sh mls qos port** *1*

Port 1:

TRUST state: TRUST CoS

Default CoS: 2

Default DSCP: 0

DSCP override: Disable

DSCP mutation map: default-dscp

21.4.2.4 Configuring default port DSCP

Only if the port TRUST status is DSCP, the default configuration DSCP takes effect. When the incoming message of DSCP is 0, default port DSCP is used as DSCP value. In default situation, that value is 0. reverse command is: no mls qos default-dscp. It can be set up in port mode:

Steps	Command	description
1	**config**	Entry into global configuration mode
2	**interface port** *portid*	Entry into port configuration mode
3	**mls qos default-dscp** *dscp-value*	Set default DSCP value dscp-value: est default port DSCP value as 0-63
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privilege mode
6	**show mls qos port** *portid*	Show QoS port configuration mode

The configuration is similar to CoS port default configuration.

21.4.2.5 Configuring port CoS override (Support equipment is not available)

Only if the port TRUST status is CoS, port CoS override configuration takes effect. Whether incoming message is untag or tag, CoS override value is used as CoS value. In Default situation, there will be no override. Reverse command: **no mls qos default-cos override**。It can be set up in port mode:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**interface port** *portid*	Entry into port configuration mode
3	**mls qos default-cos override**	Set CoS override value
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privilege mode
6	**show mls qos port** *portid*	Show QoS port configuration

21.4.2.6 Configuring port DSCP override

Only if port TRUST status is DSCP,that configuration takes effect. Whatever the incoming message DSCP is, DSCP override value is used as DSCP value. In default situation, there will be no override. Reverse command: **no mls qos default-dscp override**.It can be set in port mode:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**interface line/client** *portid*	Entry into port configuration mode
3	**mls qos default-dscp override**	Set default DSCP value
4	**Exit**	Entry into global configuration mode
5	**exit**	Return to privilege mode
6	**show mls qos port** *portid*	Show QoS port configuration

Configuration example: set TRUST status as DSCP in port 1 and port DSCP override value as 2.

Raisecom#**config**

Raisecom(config)#**inter port** *1*

Raisecom(config-port)#**mls qos** *TRUST dscp* //set port TRUST status

Raisecom(config-port)# **mls qos default-dscp** *2*

Raisecom(config-port)# **mls qos default-dscp** *override* //set port DSCP override value as 2

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

Raisecom(config)#**exit**

Raisecom# **show mls qos port** *1*

Show results:

Raisecom#**sh mls qos port** *1*

Port 1:

TRUST state: TRUST DSCP

Default CoS: 0

Default DSCP: 2

DSCP override: Enable

DSCP mutation map: default-dscp

21.4.3. Configuring Flow Classification on ACL/class-map

21.4.3.1 Create delete class-map

Class-map is used to isolate the specific data stream, matching conditions include ACL, IP priority and DSCP, VLAN and class.

Creating **class-map** follows the steps below:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**Class-map** *class-map-name* **[***match-all*|*match-any***]**	Create name as aaa, class-map and entry into config-cmap mode. *class-map-name:* class-map name, Max 16 characters match-all: satisfy all rules in class match-any: satisy only one rule in class
3	**description** *WORD*	Description of information *WORD*: description of information in class map, max 255 characters.
4	**exit**	Return to global configuration mode
5	**exit**	Return to privilege mode
6	**show class-map [**WORD**]**	Show CLASS MAP WORD: class-map name, max 16 characters

Class-map has two matching types: match-all runs AND operation, as multi match statements and operation. If there is conflict, then the match states fail; match-any is run or operation and default is match-all.

Configuration examples:

Raisecom#**config**

Raisecom(config)# **class-map** *aaa* **match-all**

Raisecom(config-cmap)# **description this-is-test-class**

Raisecom(config-cmap)#**exit**

Raisecom(config)#**exit**

Raisecom#**show class-map**

Show results as:

Class Map match-all aaa (id 0)

Description:this-is-test-class

Match none

If **class-map** is needed to delete, run **no**, as **no class-map** *class-map-name***.**

Attention:

- If class-map is quoted by policy in the port, then it is not able to be deleted.
- When matching configuration of class-map is match-all, the configuration may fail becasue the matching message may have conflicts.
- When a ACL is matched, ACL must be indetified and its type must be permit.
- When a class-map is matched, sub class-map must be match-all type.

21.4.3.2 Configuring match statements

Steps	Command	Description

1	**config**	Entry into global configuration mode
2	**class-map** *class-map-name*	Entry into config-cmap mode *class-map-name:* class-map name, max 16 characters
3	**match** {*ip-access-list* | *mac-access-list* | *access-list-ma*} *acl-index*	Match ACL *ip-access-list*: match IP access list *mac-access-list*: match MAC access list *access-list-map*: match access control list map table *acl-index*: acess control list index
4	**match ip dscp** {*0-63*}	Match DSCP value
5	**match ip precedence** {*0-7}*	Match ToS value
6	**match vlan** {*1-4094*}	Match VLAN
7	**match class-map** *WORD*	Match class map WORD: match class-map name, max16 characters
8	**exit**	Return to global configuration mode
9	**exit**	Return to privilege mode
10	**show class-map** ***[****WORD***]***	Show CLASS MAP WORD: class-map name, max 16 characters

Attention:

- When access control list is matched, ACL must be created first.
- When class map is matched, class-map must be created first.
- If the match type of class-map is match-all, the configuration may fail because there be conflicts in matched messages.
- If the same class-map has been applied for some port, then it is not allowed to modify the match statement.

To delete some match statement:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**class-map** *class-map-name*	Entry into config-cmap mode *class-map-name:* class-map name, max 16 characters
3	**no match** {*ip-access-list* | *mac-access-list* | *access-list-map*} *acl-index*	Match ACL *ip-access-list*: match IP access list *mac-access-list*: match MAC access list *access-list-map*: match access control list map ta ble *acl-index*: access control list index
4	**no match ip dscp** {*0-63*}	Match DSCP value
5	**no match ip precedence** {*0-7*}	Match ToS value
6	**no match vlan** {*1-4094*}	Match VLAN
7	**no match class-map** *WORD*	Match class map WORD: Match class-map name, max 16 characters
8	**exit**	Return to global configuration mode

9	**exit**	Return to privilege mode
10	**show class-map [***WORD***]**	Show CLASS MAP message *WORD*: class-map name, max 16 characters

Attention: If the class-map has already been applied for some other port, it is not allowed to delete the match statement.

21.4.4. Monitering and Maintenance

Command	Description
show mls qos port ***[****portlist****]***	Show QoS port information *portlist*: port number list
show class-map ***[****WORD****]***	Show CLASS MAP information *WORD*: class-map name, max 16 characters

Show QoS port information

Attention: Show different information according to the supports of different equipements. There are the examples for supports of all configurations as show below.

Raisecom#**show mls qos port** *1*

port 1:

Attached policy-map: aaa

TRUST state: not TRUSTed

default COS: 2

default DSCP: 3

DSCP override: disable

DSCP Mutation Map: aaa

If all port information is needed to check:

Raisecom#**show mls qos port**

port 1:

Attached policy-map: aaa

TRUST state: not TRUSTed

default COS: 2

default DSCP: 3

DSCP override: disable

DSCP Mutation Map: aaa

port 2:

Attached policy-map: aaa

TRUST state: not TRUSTed

default COS: 2

default DSCP: 3

DSCP override: disable

DSCP Mutation Map: aaa

……

port 26:

TRUST state: not TRUSTed

default COS: 0

default DSCP: 0

DSCP override: disable

DSCP Mutation Map: default-dscp

Show QoS class-map information:

Raisecom#**show class-map**

Class Map match-all aaa (id 0)

Match ip-access-list 1

Match ip dscp 2

Match class-map bbb

Match vlan 1

Class Map match-all bbb (id 1)

Match ip-access-list 2

If it is needed to show the specific name of class-map, use commands as below:

Raisecom#**show class-map** *aaa*

Class Map match-all aaa (id 0)

Match ip-access-list 1

Match ip dscp 2

Match class-map bbb

Match vlan 1

21.4.5. Typical Configuration Examples

Configuration examples: classify the flow and satisfy the flow in aaa condition: in VLAN1, DSCP is 2 and the messages are from 10.0.0.2 and 10.0.0.3.

Raisecom#**config**

Raisecom(config)# **ip-access-list** *1* **permit ip** *10.0.0.2 255.255.255.0* **any**

Raisecom(config)# **ip-access-list** *2* **permit ip any** *10.0.0.3 255.255.255.0*

Raisecom(config)# **class-map** *bbb* **match-all**

Raisecom(config-cmap)#**match ip-access-list** *2*

Raisecom(config)# **class-map** *aaa* **match-all**

Raisecom(config-cmap)#**match ip-access-list** *1*

Raisecom(config-cmap)#**match ip dscp** *2*

Raisecom(config-cmap)#**match vlan** *1*

Raisecom(config-cmap)#**match class-map** *bbb*

Raisecom(config-cmap)# **exit**

Raisecom(config)#**exit**

Raisecom#**show class** *aaa*

Show results as:

Raisecom#**show class** *aaa*

Class Map match-all aaa (id 0)

Match ip-access-list 1

Match ip dscp 2

Match class-map bbb

Match vlan 1

21.5 Policy and Marking Function Configuration

21.5.1. Policy and Marking Default Configuration

Function	Default value
Policy TRUST status	DSCP

21.5.2. Policy and Marking Configuration

21.5.2.1 Create delete policy-map

Use **policy-map** command to encapsulate and classify the data flow of class-map. Create **policy-map** as the steps below:

Steps	Command	Description

1	**Config**	Entry into global configuration mode
2	**policy-map** *policy-map-name*	Create name as bbb, policy-map and entry into config-pmap mode. policy-map-name: policy map name, max 16 characters
3	**description** *WORD*	Description informaiton WORD: policy map description information, max 255 characters
4	**Exit**	Return to global configuraiton mode
5	**Exit**	Return to privilege mode
6	**show policy-map [***WORD***]**	Show POLICY MAP information *WORD*: policy map name, max 16 characters

Configuration examples:

Raisecom#**config**

Raisecom(config)# **policy-map** *bbb*

Raisecom(config)# **exit**

To check wether the configuration is right, use show command:

Raisecom#**show policy-map**

Policy Map bbb

Description:this-is-test-policy

If it is needed to delete a **policy-map**, use **command no**, **no policy-map** *policy-map-name***.**

Attention: If a policy-map is applied for other ports, then it is not able to be deleted.

21.5.2.2 Define policy map

To define one or more defined class-map as a policy, following steps below are used:

Steps	Command	Descriptions
1	**config**	Entry into global configuration mode
2	**policy-map** *policy-map-name*	Entry into config-pmap mode policy-map-name: policy map name, max 16 characters
3	**class-map** *class-map-name*	Encapsulate cuclass-map aaa into policy aaa, and entry into config-pmap-c mode *class-map-name:*class-map name, max 16 characters
4	**exit**	Return to config-pmap mode

5	**exit**	Return to global configuration mode
6	**exit**	Return to privilege mode
7	**show policy-map [WORD]**	Display POLICY MAP information WORD : policy map name, max 16 characters
8	**show policy-map class** {*WORD*}	Display POLICY MAP some classification information *WORD:* class-map name, max 16 characters

One class can be applied for many policy.

Configuration examples:

Raisecom#**config**

Raisecom(config)# **policy-map aaa**

Raisecom(config-pmap)# **class-map aaa**

Raisecom(config-pmap-c)#**exit**

Raisecom(config-pmap)#**exit**

Raisecom(config)# **exit**

To check wether the configuration is right, use show command:

Raisecom#**show policy-map**

Policy Map aaa

Class aaa

To delete class-map from a policy:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**policy-map** *policy-map-name*	Entry into config-pmap mode policy-map-name: policy map name, max 16 characters
3	**no class-map** *class-map-name*	Delete class-map from policy *class-map-name:* class-map name, max 16 characters
4	**exit**	Return privilege mode
5	**show policy-map [***WORD***]**	Display POLICY MAP information *WORD*: policy map name, max 16 characters

Attention: It is not allowed to delete class-map if the policy-map has been applied for some other port.

21.5.2.3 Define policy action

Different actions are used for different data flow in policy, show as below:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**policy-map** *policy-name*	Entry into config-pmap mode policy-name: policy map name, max 16 characters
3	**Class-map** *class-name*	Encapsulate class-map into policy, and entry into config-pmap-c mode *class-name:* class-map name, max 16 characters
4	**police** *policer-name*	Use policer for the policy data flow for bit-rate limiting and reshaping, check the link for more infomaiton: bit-Rate Limitation and reshaping function configuration policer-name: policer name, max 16 characters
5	**TRUST** [*cos* | *dscp* | *ip-precedence*]	Policy TRUST status, default use DSCP *cos*: set switch TRUST CoS status *dscp*: set switch TRUST DSCP status *ip-precedence*: set switch TRUST IP priority
6	**set** {**ip dscp** *new-dscp* | **ip precedence** *new-precedence* | **cos** *new-cos* }	Set new value for data flow *new-dscp*: DSCP value, 0-63; *new-precedence*: IP priority value, 0-7 *new-cos*: set CoS value, 0-7
7	**set vlan** <*1-4094*>	Set VLAN override
8	**redirect-to port** *to-port*	Redirect the ports to-port: redirect the ports numbers
9	**copy-to-mirror**	Data flow mirror image
10	**exit**	Return to config-pmap mode
11	**exit**	Return to global configuration mode
12	**exit**	Return to privilege mode
13	**show policy-map [***WORD***]**	Display POLICY MAP information *WORD*: policy map name, max 16 characters

Attention:

- So far, policy TRUST (TRUST command) functions are not supported
- Set command and policy TRUST command are mutually exclusive.
- In one class-map, set command can only be configured in one. Later configuration will take effect

Configuration examples:

Raisecom#**config**

Raisecom(config)#**policy-map** *aaa*

Raisecom(config-pmap)#**class-map** *aaa*

Raisecom(config-pmap-c)#**police** *aaa*

Raisecom(config-pmap-c)#**set cos** *6*

Raisecom(config-pmap-c)#**set ip dscp** *5*

Raisecom(config-pmap-c)#**set ip precedence** *4*

Raisecom(config-pmap-c)#**set vlan** *10*

Raisecom(config-pmap-c)#**redirect-to port** *3*

Raisecom(config-pmap-c)#**exit**

Raisecom(config-pmap)#**exit**

Raisecom(config)#**exit**

Raisecom# **show policy-map** *aaa*

Show as:

Policy Map aaa

Class aaa

police aaa

set ip precedence 4

set vlan 10

redirect-to port 3

To delete or modify data flow actions:

Steps	Command	Description
1	**Config**	Entry into global configuration mode
2	**policy-map** *policy-name*	Entry into config-pmap mode *policy-name*: policy map name,max 16 characters
3	**class-map** *class-name*	Encapsulate class-map aaa into policy aaa, and entry into config-pmap-c mode *class-name:* class-map name, max 16 characters
4	**no police** *policer-name*	Apply policer in this policy data flow *policer-name*: policer name, max 16 characters
5	**no TRUST** [*cos* | *dscp* | *ip-precedence*]	Data flow TRUST status, default use DSCP *cos*: set switch as TRUST CoS status *dscp*: set switch as TRUST DSCP status *ip-precedence*: set switch as TRUST IP priority status
6	**no set** {*ip dscp*|*ip precedence*|*cos*}	Set new value for data flow *new-dscp*: DSCP value, 0-63; *new-precedence*: IP priority value, 0-7 *new-cos*: set CoS value, 0-7
7	**no set vlan**	Set VLAN override
8	**no redirect-to port**	Redirect to port

9	**no copy-to-mirror**	Data flow mirror image
10	**exit**	Return to config-pmap mode
11	**exit**	Return to global configuration mode
12	**exit**	Return to privilege mode
13	**show policy-map [WORD]**	Display POLICY MAP WORD: policy map name, max 16 characters

Attention: It is not allowed to modify the action if its policy-map has been applied for other ports

21.5.2.4 Apply policy service-policy in ports

It actually does not take effect after all data flow and policy defined. They need to be applied for the ports. The steps for the apply policy are as below:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**service-policy** *policy-name* **ingress** *portid* **[egress** *portlist* **]**	Apply policy on in/out port. *policy-name*: policy map name, max 16 characters *portid*: in port number *portlist*: out port list
3	**exit**	Return to privilege mode
4	**show policy-map port [***portlist* **]**	Display port policy application information *portlist*: port number

Attention:

- QoS must start before appling policy;
- When the configuring data flow becomes big, it may fail because it may get the biggest rule of capacity based on those 256 rules for 8 ports.
- The TRUST status are mutually exclusive if the TRUST status of the applied front port is not UNTRUST status. After applied, the status will become UNTRUST status.

Application examples:

Raisecom#**config**

Raisecom(config)#**service-policy** *aaa* **ingress** *2* **egress** *1-5*

Raisecom(config)#**service-policy** *bbb* **egress** *1*

Raisecom(config)#**exit**

Raisecom#**show policy-map port**

Display as:

port 2 on ingress:

Policy Map aaa:

Egerss:1-5

Class Map :aaa (match-all)

port 1 on egress:

Policy Map bbb:

21.5.3. Monitoring and Maintenance

Command	Description
show policy-map [*WORD***]**	Display POLICY MAP information *WORD*: policy map name, max 16 characters
show policy-map class {*WORD***}**	Display some classified information of POLICY MAP *WORD:* class-map name, max 16 characters
show policy-map port [*portlist* **]**	Display port policy application information *portlist*: port numbers

1. Display QoS policy-map information

Raisecom#**show policy-map**

Policy Map aaa

Class aaa

police aaa

set ip precedence 4

Class bbb

police aaa

To display the specifi name of policy-map information:

Raisecom#**show policy-map** *aaa*

Policy Map aaa

Class aaa

police aaa

set ip precedence 4

Class bbb

police aaa

2. Display some classified information of POLICY MAP

If wanted to show specific policy-map name、indicated class-map name information:

Raisecom#**show policy-map** *aaa* **class-map** *aaa*

Policy Map aaa

Class aaa

police aaa

set ip precedence 4

3. Display QoS policy-map application information

If wanted to check which policy-map information applied on which ports:

Raisecom#**show policy-map port** *1*

port 1:

Policy Map aaa:

Egerss:1-5

Class Map :aaa (match-all)

Class Map :bbb (match-all)

If wanted which policy-map information applied on all ports:

Raisecom#**show policy-map port**

port 1:

Policy Map aaa:

Egerss:1-5

Class Map :aaa (match-all)

Class Map :bbb (match-all)

21.5.4. Specific Configuration Examples:

Raisecom#**config**

//Define ACL

Raisecom(config)# **ip-access-list** *1* **permit ip** *10.0.0.2 255.255.255.0 10.0.0.3 255.255.255.0*

Raisecom(config)# **ip-access-list** *2* **permit ip** *10.0.0.3 255.255.255.0 10.0.0.2 255.255.255.0*

//classify data flow

Raisecom(config)# **class-map** *aaa* **match-all**

Raisecom(config-cmap)#**match ip-access-list** *1*

Raisecom(config-cmap)# **exit**

Raisecom(config)# **class-map** *bbb* **match-all**

Raisecom(config-cmap)#**match ip-access-list** *2*

Raisecom(config-cmap)# **exit**

//bit-rate limitation and reshapeing definition, details see: bit-Rate Limitation and reshaping function

configuration

Raisecom(config)#**mls qos class-policer** *p-aaa 4000 100* **exceed-action** *drop*

Raisecom(config)# **mls qos class-policer** *p-bbb 8000 200* **exceed-action** *drop*

//define policy

Raisecom(config)#**policy-map** *wmj*

Raisecom(config-pmap)#**class-map** *aaa* //define data flow classification aaa in policy

Raisecom(config-pmap-c)# **set ip dscp** *5* //define policy action---set IP DSCP

Raisecom(config-pmap-c)#**police** *p-aaa* //define policy action——bit-rate limited reshaping

Raisecom(config-pmap-c)#**exit**

Raisecom(config-pmap)#**class-map** *bbb* //define data flow bbb in policy

Raisecom(config-pmap-c)# **set ip dscp** *6* //define policy action——set IP DSCP

Raisecom(config-pmap-c)#**police** *p-bbb* //define policy action——bit-rate limited reshaping

Raisecom(config-pmap-c)#**exit**

Raisecom(config-pmap)#**exit**

Raisecom(config)#**mls qos**

Raisecom(config)#**service-policy** *wmj* **ingress** *1* **egress** *2* //apply policy in ports

21.6 Bit-Rate Limitation and Reshaping Function Configuration

21.6.1. Bit-Rate Limitation and Reshaping Default Configuration

None

21.6.2. Configuration Based on Bit-Rate and Reshaping of Data Flow

Create policer as following steps:

Steps	Command	Description
1	**config**	Entry into global configuration mode

2	**mls qos single-policer** *policer-name rate burst* **exceed-action {drop | policed-dscp-transmit** *marked-dscp* **}**	Create policer in type of single *policer-name*: set policer name *rate*: bit-rate value (Kbps), 8－2000000 *burst:* Burst value (KBps), 8－512000 *drop*: droped packets once it is over bit-rate value *policed-dscp-transmit*: modified DSCP value once it is over bit-rate value *marked-dscp*: modified DSCP value once it is over bit-rate value
3	**mls qos class-policer** *policer-name rate burst* **exceed-action {drop | policed-dscp-transmit** *marked-dscp* **}**	Create policer as type of class *policer-name*: set policer name *rate*: bit-rate value(Kbps), 8－2000000kbps *burst*: burst value (KBps), 8－512000 *drop*: droped packets once it is over bit-rate value *policed-dscp-transmit*: modify DSCP once it is over bit-rate value *marked-dscp*: modified DSCP value once over bit-rate value
4	**mls qos aggregate-policer** *policer-name rate burst* **exceed-action {drop | policed-dscp-transmit** *marked-dscp* **}**	Create policer as type of aggregate *policer-name*: set policer name *rate*: bit-rate value(Kbps), 8－2000000kbps *burst:* burst value (KBps), 8－512000 *drop*: droped packets once it is over bit-rate value *policed-dscp-transmit*: modify DSCP once it is over bit-rate value *marked-dscp*: modified DSCP value once over bit-rate value
5	**exit**	Return to global configuration mode
6	**show mls qos policer** *[single-policer | class-policer | aggregate-policer]*	Display policer information *single-policer*: display single policer *class-policer*: display class policer *aggregate-policer*: display aggregate policer

To delete a policer, use command no, **no** {*single-policer*|*class-policer*|*aggregate-policer*} *placer-name*.

Attention: When delete a policer, it is not allowed to delete it if its policy is applied for other ports.

21.6.3. Monitering and Maintenance

Command	Description
show mls qos policer [*single-policer* **|** *class-policer* **|** *aggregate-policer* **]**	Display policer information *single-policer*: Display single policer *class-policer*: Display class policer *aggregate-policer*: display aggregate policer

Raisecom#**show mls qos policer**

single-policer aaa 44 44 exceed-action policed-dscp-transmit 4

Used by policy map aaa

To show which port is using policer, use the commands below:

Raisecom#**show mls qos port policers**

Port id 1

policymap name: aaa

policer type: Single, name: aaa

rate: 44 kbps, burst: 44 kbyte, exceed action: policed-dscp-transmit, dscp:4

21.6.4. Specific Configuration Examples

Configuration examples:

Raisecom#**config**

Raisecom(config)# **mls qos single-policer** *aaa 44 44* **exceed-action policed-dscp-transmit** *4*

Raisecom(config)# **exit**

Raisecom#**show mls qos policer**

Display results as:

single-policer aaa 44 44 exceed-action policed-dscp-transmit 4

Not used by any policy map

If aaa is applied for a port:

Raisecom#**show mls qos port policers**

Port id 1

policymap name: aaa

policer type: Single, name: aaa

rate: 44 kbps, burst: 44 kbyte, exceed action: policed-dscp-transmit, dscp: 4

21.7 Map Function Configuration

21.7.1 Map Default Configuration

COS-DSCP default configuration relationship as:

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

IP-Precedence-DSCP default map relation as:

ToS value	0	1	2	3	4	5	6	7

DSCP value	0	8	16	24	32	40	48	56

DSCP-COS default map relation as:

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

DSCP-to-DSCP-Mutation default map relation (default-dscp) as:

DSCP value	0	1	2	3	4	5	6	7
0	8	9	10	11	12	13	14	15
1	16	17	18	19	20	21	22	23
2	24	25	26	27	28	29	30	31
3	32	33	34	35	36	37	38	39
5	40	41	42	43	44	45	46	47
6	48	49	50	51	52	53	54	55
7	56	57	58	59	60	61	62	63

Internal COS – queuing default map relation as:

Internal CoS value	0	1	2	3	4	5	6	7
Queuing ID	1	1	2	2	3	3	4	4

21.7.2 CoS-DSCP map List Configuration

CoS-DSCP map list maps incoming packet COS value as a DSCP value. QoS is used to describe data flow priority. It default map relation as:

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

To modify the map relations, the following steps are set:

Steps	Commands	Description
1	**config**	Entry into global configuration mode
2	**mls qos map cos-dscp** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Set new map relation Dscp1-8: DSCP value

3	**exit**	Return to privilege mode
4	**show mls qos maps cos-dscp**	Show QoS COS-DSCP map list

Configuration examples:

Configuration cos-dscp map 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**

Show results as:

Cos-dscp map:

cos: 0 1 2 3 4 5 6 7

---

dscp: 2 3 4 5 6 7 8 9

To backup COS-DSCP map list to default map relation,use command **no**.

Steps	Command	description
1	**config**	Entry into global configuration mode
2	**no mls qos map cos-dscp**	Backup to default map relation
3	**exit**	Return to privilege mode
4	**show mls qos maps cos-dscp**	Display QoS COS-DSCP map list

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

21.7.3 IP-Procedence-DSCP Map List Configuration

IP-Procedence-DSCP map-list configuration maps incoming packet ToS into a DSCP value. QoS is used to describe the data flow priority. Its default map relation as show below:

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

To modify that map relation, set as the following steps:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**mls qos map ip-prec-dscp** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Set new map relationship Dscp1-8: DSCP value
3	**exit**	Return to privilege mode
4	**show mls qos maps ip-prec-dscp**	Display QoS IP-Procedence-DSCP map list

Configuration example:

Configure ip-prec-dscp map as 2 4 6 8 10 12 14 16:

Raisecom#**config**

Raisecom(config)# **mls qos map ip-prec-dscp** *2 4 6 8 10 12 14 16*

Raisecom(config)#**exit**

Raisecom# **show mls qos maps ip-prec-dscp**

Show results as:

Ip Precedence-dscp map:

ipprec: 0 1 2 3 4 5 6 7

---

dscp: 2 4 6 8 10 12 14 16

Backing up IP-Procedence-DSCP map list to default map relation, use command **no**.

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**no mls qos map ip-prec-dscp**	Backup to default map relation
3	**Exit**	Return to privilege mode
4	**show mls qos maps ip-prec-dscp**	Show QoS IP-Procedence-DSCPmap list

Raisecom#**show mls qos maps ip-prec-dscp**

Ip Precedence-dscp map:

ipprec: 0 1 2 3 4 5 6 7

---

dscp: 0 8 16 24 32 40 48 56

21.7.4 DSCP-CoS Map List Configuration

DSCP-CoSmap list maps the incoming packet DSCP value into a cos value. QoS use its description data flow priority. The default map relation 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

To modify that map relation, follows the steps below:

Steps	Command	Description
1	**Config**	Entry into global configuration mode
2	**mls qos map dscp-cos** *dscplist* **to** *cos*	set new map relation Dscplist: DSCP list Cos: cos value
3	**exit**	Return to privilege mode
4	**show mls qos maps dscp-cos**	Show QoS DSCP- CoSmap list

Configuration examples:

configure **dscp-cos** map, mapping 1-10 into 7:

Raisecom#**config**

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

Raisecom(config)#**exit**

Raisecom# **show mls qos maps dscp-cos**

show results as:

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

Renewing DSCP-CoSmap list to default mapping relation, use command **no:**

steps	command	description
1	**config**	Entry into global configuration mode
2	**no mls qos map dscp-cos**	Back to the default mapping relation

3	**exit**	Return to privilege mode
4	**show mls qos maps dscp-cos**	showQoS DSCP-CoSmap list

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

21.7.5 DSCP-MUTATION Map List Configuration

To get the IP data flow with QoS characters in two indepent QoS domain, the ports in the edge of those domains should be set as DSCP TRUST status. Then the receiving port receive the trust DSCP value to avoid QoS classification. If the DSCP values of those two domains are different, they can be converted through DSCP-to-DSCP converting map list.

DSCP-MUTATIONmap list maps the DSCPvalue into a new DSCP value. QoS uses its description data flow priority. There is a default map listdefault-DSCP in the system and this list could not be modified and deleted.

To modify that mapping relation, set the following steps:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**mls qos map dscp-mutation** *dscpname dscplist* **to** *dscp*	Create new DSCP mapping relation Dscpname: DSCP mutation name Dscplist: output port DSCP Dscp: DSCP value
3	**exit**	Return to privilege mode
4	**show mls qos maps dscp-mutation**	showQoS DSCP-MUTATIONmap list

Configuration examples:

Set **dscp-mutation** mapping, map 1-10, 20-30 into 30:

Raisecom#**config**

Raisecom(config)# **mls qos map dscp-mutation** *aaa 1-10* **to** *30*

Raisecom(config)# **mls qos map dscp-mutation** *aaa 20-30* **to** *30*

Raisecom(config)#**exit**

Raisecom# **show mls qos maps dscp-mutation**

Show results as:

Dscp-dscp mutation map:

default-dscp:

d1 : d2	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0 :	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1 :	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*
2 :	*20*	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*
3 :	*30*	*31*	*32*	*33*	*34*	*35*	*36*	*37*	*38*	*39*
4 :	*40*	*41*	*42*	*43*	*44*	*45*	*46*	*47*	*48*	*49*
5 :	*50*	*51*	*52*	*53*	*54*	*55*	*56*	*57*	*58*	*59*
6 :	*60*	*61*	*62*	*63*						

Dscp-dscp mutation map:

aaa:

d1 : d2	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
0 :	*0*	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*
1 :	*30*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*
2 :	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*	*30*
3 :	*30*	*31*	*32*	*33*	*34*	*35*	*36*	*37*	*38*	*39*
4 :	*40*	*41*	*42*	*43*	*44*	*45*	*46*	*47*	*48*	*49*
5 :	*50*	*51*	*52*	*53*	*54*	*55*	*56*	*57*	*58*	*59*
6 :	*60*	*61*	*62*	*63*						

To delete DSCP-MUTATION map list, use command **no**.

Steps	command	description
1	**config**	Entry into global configuration mode
2	**no mls qos map dscp-mutation** *dscpname*	Delete DSCP mapping relation Dscpname: DSCP mutation name
3	**exit**	Return to privilege mode
4	**show mls qos maps dscp-mutation**	showQoS DSCP-CoSmap list

To apply the map list for DSCP-mutation, it could be used in port mode. Port default uses default-dscp

mapping relation.

Steps	command	description
1	**config**	Entry into global configuration mode
2	**interface line/client** *portid*	Entry into port mode
3	**mls qos dscp-mutation** *dscpname*	Apply DSCP mapping relation *dscpname*: DSCP mutation name, max 16 characters
4	**exit**	Return to configuraton mode
5	**exit**	Return to privilege mode
6	**show mls qos port** *portid*	Show QoS port configuration information

Configuration examples:

Raisecom#**config**

Raisecom(config)#**interface line/client** *1*

Raisecom(config-port)# **mls qos dscp-mutation aaa**

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

Raisecom(config)#**exit**

Raisecom#**show mls qos port** *1*

To check wether the configuration is right, use command show:

Raisecom#**show mls qos port** *1*

port 1:

TRUST state: not TRUSTed

default COS: 0

default DSCP: 0

DSCP override: disable

DSCP Mutation Map: aaa

Attention: In ISCOM2800 series, DSCP-MUTATION map list uses fiter list to get hardware. In hardware, port 1-8 use same filter list (same as 9－16, 17－24, port 25, port 26 are using one filter list individually, 5 filter list in total). Thus, as any port in port 1-8 is using DSCP-MUTATION map list, the rest ports of port 1－8 are using DSCP-MUTATION map list as well.

To decline DSCP-MUTATION map list application in the port, use command **no**.

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**interface line/client** *portid*	Entry into port mode

3	**no mls qos dscp-mutation** *dscpname*	Decline using DSCP map relation dscpname: DSCP mutation name, max 16 characters
4	**exit**	Return to configuration mode
5	**exit**	Return to privilege mode
6	**show mls qos port** *portid*	showQoS port configuration information

To check whether the configuration is right, use command show:

Raisecom#**show mls qos port** *1*

port 1:

TRUST state: not TRUSTed

default COS: 0

default DSCP: 0

DSCP override: disable

DSCP Mutation Map: default-dscp

Attention: When dscp-mutationmap list is used in some other port, its map list could not be deleted; only the map list is not used, it could be deleted.

21.7.6 CoS-queue Map List Configuration

CoS-queuemap list is sent to the output queue which is decided by the incoming packet CoS value. QoS uses its description data flow priority, and its default map relation is:

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

To modify the map relation, set up with the following relation:

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**queue cos-map** *queueid coslist*	set new map relation, packets CoS value in 1-4 are sent to Queue 1 Queueid: Queue number Coslist: CoS value
3	**exit**	Return to privilege mode
4	**show mls qos queuing**	Show QoS queue map list

Configuration examples:

Raisecom#**config**

Raisecom(config)# **queue cos-map** *1 1-4*

Raisecom(config)#**exit**

Raisecom#**show mls** *qosqueueing*

show results as:

the queue schedule mode: strict priority(SP)

Cos-queue map:

cos-queueid

0 - 1

1 - 1

2 - 1

3 - 1

4 - 1

5 - 3

6 - 4

7 - 4

To renew CoS-queue map list to default map relation, use command **no**.

Steps	Command	Description
1	**config**	Entry into global configuration mode
2	**no queue cos-map**	Renew default map relation
3	**exit**	Return to privilege mode
4	**show mls qos queuing**	Show QoS queuing map list

To check wehter the configuration is correct, use command show:

Raisecom#**show mls** *qos queueing*

the queue schedule mode: strict priority(SP)

Cos-queue map:

cos-queueid

0 - 1

1 - 1

2 - 2

3 - 2

4 - 3

5 - 3

6 - 4

7 - 4

21.7.7 Set Ports Based on smac, dmac, vlan's Frame Priority and Priority Override Function

Ports can be based on smac、dmac、vlan entering switch's message farme priority and queue priority override.

Configuration steps as below:

Steps	Command	Description
1	**config**	entry into global configuration mode
2	**interface {** port-list **}** *<1-MAX_PORT_NUM >*	Entry into Ethernet physic interface mode *1-MAX_PORT_NUM* equipement port numbers
3	**mls qos {***smac* | *dmac***}** **{***priority-set*|*cos-override***}**	set up ports based onsmac, dmac's frame priority or queue priority override function Smac: source MAC Dmac: destination MAC *cos-override*: frame priority *priority-set*: queuepriority
4	**mls qos {***smac*|*dmac***}** *priority-set cos-override*	set up ports based onsmac,dmac's frame priority and queue priority override function Smac: source MAC Dmac: destination MAC *cos-override*: frame priority *priority-set*: queue priority
5	**mls qos vlan** {*priority-set*|*cos-override***}**	set up ports based onvlan's frame priority or queue priority override function *cos-override*: frame priority *priority-set*: queue priority
6	**mls qos vlan** *priority-set cos-override*	set up ports based on vlan's frame priority and queue priority override function *cos-override*: frame priority *priority-set*: queue priority
7	**exit**	Exit
8	**show mls qos port-list** *{1-MAX_PORT_NUM }*	Display QoS configuration information *1-MAX_PORT_NUM* equipement port numbers

To use command no Renew all priority override based on smac、dmac、vlanto default configuration(even both of them are not override).

21.7.8 Monitering and Maintenance

Command	Description
show mls qos maps *[cos-dscp |*	Display all map list's configuration content。

ip-prec-dscp | *dscp-cos* | *dscp-mutation]*	*cos-dscp*: COS to DSCP map *ip-prec-dscp*: Ip priority to DSCP map *dscp-cos*: DSCP to CoS map *dscp-mutation*: DSCP mutation map
show mls qos queuing	Display QoS queue map list
show mls qos port-list *{1-MAX_PORT_NUM }*	Display QoS configuration information *1-MAX_PORT_NUM:* equipement port numbers

1. Map list information maps

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

Ip Precedence-dscp map:

ipprec: 0 1 2 3 4 5 6 7

---

dscp: 0 8 16 24 32 40 48 56

Dscp-dscp mutation map:

default-dscp:

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

---

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

1 : 10 11 12 13 14 15 16 17 18 19

2 : 20 21 22 23 24 25 26 27 28 29

3 : 30 31 32 33 34 35 36 37 38 39

4 : 40 41 42 43 44 45 46 47 48 49

5 : 50 51 52 53 54 55 56 57 58 59

6 : 60 61 62 63

Dscp-dscp mutation map:

aaa:

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

---

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

1 : 30 30 30 30 30 30 30 30 30 30

2 : 30 21 22 23 24 25 26 27 28 29

3 : 30 31 32 33 34 35 36 37 38 39

4 : 40 41 42 43 44 45 46 47 48 49

5 : 50 51 52 53 54 55 56 57 58 59

6 : 60 61 62 63

2. Queue map list information queueing

Raisecom#**show mls qos queueing**

t*he queue schedule mode: bounded delay*

wrr queue weights:

queueid-weights-delay

1 - 1 - 100

2 - 3 - 100

3 - 5 - 100

4 - 7 - 100

Cos-queue map:

cos-queueid

0 - 1

1 - 1

2 - 2

3 - 2

4 - 3

5 - 3

6 - 4

7 - 4

3. display QoS configuration information:

Raisecom#**show mls qos port-list** *2*

port	*smac-policy*	*dmac-policy*	*vlan-policy*
2	*priority-set*	--	--

21.7.9 Specific Configuration Examples

See the sections for details.

21.8 Queue and Adjust Function Mode

So far, the equipements support four queue adjust modes: strict priority (SP), weighted priority (WRR), BOUND-DELAY mode and SP+WRR's mixed mode. Default set is priority mode.

21.8.1 Queue and Adjust Default Configuration

Function	Default
Queue adjust policy	Strict priority adjust SP

21.8.2 SP Configuration

Configuration steps as:

Steps	Command	Description
1	**config**	entry into global configuration mode
2	**queue strict-priority**	Configuration is strict priority
3	**exit**	Return to privilege mode
4	**show mls qos queuing**	display QoS queuing information

21.8.3 WRR Configuration

Configuration steps as:

Steps	Command	Description
1	**config**	entry into global configuration mode
2	**queue wrr-weight** *weight0 weight1 weight2 weight3*	Set ports' adjust mode as WRRmode Weight 0-3: set queue 0-3 weight value
3	**exit**	Return to privilege mode
4	**show mls qos queuing**	display QoS queuing information

21.8.4 SP+WRR Configuration

Configuration steps as:

Steps	Command	Description
1	**config**	entry into global configuration mode
2	**queue preemp-wrr** *weight1 weight2 weight3*	Set port adjust mode as PREEMP-WRR mode, like queue1 is strict priority, rest queues follow the weights Weight 1-3: set queue1-3 weight value
3	**queue preemp-wrr** *weight0 weight1*	Set ports adjust mode as PREEMP-WRR mode, like queue 0, 1 are strict priority, rest queue follow the weights
4	**exit**	Return to privilege mode
5	**show mls qos queuing**	display QoS queuing information

21.8.5 Monitering and Maintenance

Command	Description
show mls qos queuing	Display QoS's queuemap list

- Queue map list information queueing

Raisecom#**show mls qos queueing**

the queue schedule mode: bounded delay

wrr queue weights:

queueid-weights-delay

1 - 1 - 100

2 - 3 - 100

3 - 5 - 100

4 - 7 - 100

Cos-queue map:

cos-queueid

0 - 1

1 - 1

2 - 2

3 - 2

4 - 3

5 - 3

6 - 4

7 - 4

21.8.6 Specific Configuration Examples

Configuration examples: set queue as WRR mode, weight as 1:2:4:8:

Raisecom#**config**

Raisecom(config)# **queue wrr-weight** *1 2 4 8*

Raisecom(config)#**exit**

Raisecom#**show mls qos queuing**

Display results:

Raisecom#**show mls qos queuing**

the queue schedule mode: weighted round robin(WRR)

wrr queue weights:

Queue ID - Weights - Delay

1 - 1 - 0

2 - 2 - 0

3 - 4 - 0

4 - 8 - 0

21.9 QoS Trouble Shoot

- Port TRUST status and policy configuration are mutually exclusive.
- Data flow TRUST status and SET actions are mutually exclusive.
- To delete class-map、policy-map、policer, it will be failed if they have been applied for the ports.
- If class-map、policy-map have been applied for the ports, then modification for match statements and data flow actions (as set action) will fail.
- Before apply data flow policy, QoS must be started first; data flow policy will be failed if QoS is stopped.
- If class-map match type is matcha-all, the configuration may fail because there might be conflicts between matching information.
- To match a ACL, ACL must be defined first and its type must be permit.
- To match a class-map, sub class-map must be type of match-all.
- As configuration data flow become more, it may be failed in applying because it is getting the capacity biggest rule. (8 ports have 256 rules)
- To start QoS policy, it is suggested to turn off data flow control function;

21.10 QoS Command Reference

Command	Description
[no] mls qos	Run and Stop QoS
[no] mls qos trust [**cos** | **dscp** | **ip-precedence**]	Set ports TRUST status
mls qos default-cos *default-cos*	Set QoS ports Default CoS value

no mls qos default-cos	Renew QoS ports Default CoS value
mls qos map dscp-mutation *dscp-name dcp-list* **to** *dscp*	Create DSCP-mutaion map list
no mls qos map dscp-mutation *dscp-name*	Delete DSCP-mutaion map list
[no] mls qos dscp-mutation *dscp-name*	Apply or decline DSCP-mutaion map application
class-map *class-map-name* **[match-any | match-all]**	Create class-map
no class-map *class-map-name*	Delete class-map
[no] policy-map *policy-map-name*	Create delete policy map
description *WORD*	Set policy map and class-map description information
[no] class *class-map-name*	apply class map on policy
match { **ip-access-list** *acl-index* | **mac-access-list** *acl-index* | **access-list-map** *acl-index* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list* | **class** *calss-name* | **vlan** *vlanlist*}	Set match statements
no match { **ip-access-list** *acl-index* | **mac-access-list** *acl-index* | **access-list-map** *acl-index* | **ip dscp** | **ip precedence** | **class** *calss-name* | **vlan** *vlanlist* }	Delete match statements
[no] trust [**cos** | **dscp**]	Set data flow TRUST status
set {**ip dscp** *new-dscp* | **ip precedence** *new-precedence* | **cos** *new-cos* }	Set actions
no set {**ip dscp** | **ip precedence** | **cos** }	Delete set value
mls qos {aggregate-policer |class-policer | single-policer } *policer-name rate burst* **[exceed-action { drop | policed-dscp-transmit** *dscp* **}]**	Create policer
no mls qos {aggregate-policer |class-policer | single-policer } *policer-name*	Delete policer
[no] police *policer-name*	Apply policer
service-policy *policy-map-name* **ingress** *portid* **[egress** *portlist*]	Apply policy
no service-policy *policy-map-name* **ingress** *portid*	Decline apply policy
mls qos map cos-dscp *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	configurationCoS to DSCP map
no mls qos map cos-dscp	Renew CoS to DSCP map
mls qos map ip-prec-dscp *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Configuration ToS to DSCP map
no mls qos map ip-prec-dscp	Renew ToS to DSCP map
mls qos map dscp-cos *dscp-list* **to** *cos*	Configuration DSCP to switch internal priority map
no mls qos map dscp-cos	Renew DSCP to switch internal priority map
queue cos-map *queue-id cos-list*	Configuration switch internal priority to queue map

no queue cos-map	Renew switch internal priority to queue map
queue wrr-weight *weight0 weight1 weight2 weight3*	Configuration switch queue adjust mode as WRR
queue bounded-delay *weight0 weight1 weight2 weight3 delaytime*	Set port adjust mode as BOUNDDELAY mode
queue preemp-wrr *weight1 weight2 weight3*	Set port adjust mode as PREEMP-WRR mode
queue strict-priority	Set port adjust mode as strict priority mode
show mls qos	Display QoS on/off status
show mls qos policer [*policename* | *aggregate-policer* |*class-policer* | *single-policer* **]**	Display policer information
show mls qos maps [*cos-dscp* | *dscp-cos* | *dscp-mutation* | *ip-prec-dscp*]	Display every map list configuration content
show mls qos queueing	Display in/out queue configuration information
show mls qos port *portid* [**policers**]	Display port strategy configuration, policer,etc information
show class-map [*class-map-name*]	Display class-map information
show policy-map [*policy-map-name* | [**port** *portId*] [**class** *class-name*]	Display policy information

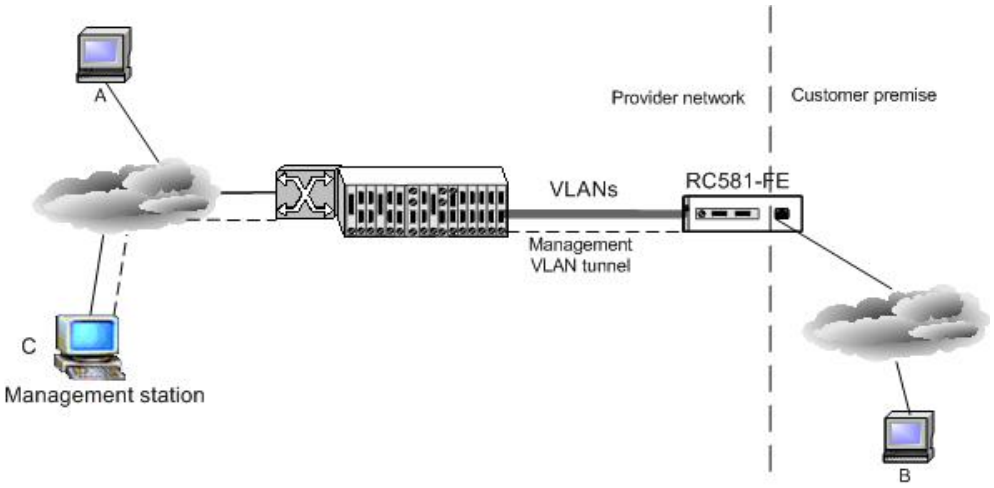
Chapter 22 User Network Configuration

This chapter is mainly about user network function and the configuration. With user network function, user can diagnose client data channel connectivity, including:

- ✧ User network interview
- ✧ User network configuration
- ✧ Monitoring and maintenance
- ✧ Typical configuration example

22.1 User network overview

5x1 serious media converter divides the client and ISP, providing NID/UNI. RC5x1-FE has flexible network diagnose function. As NID it is able to diagnose the connectivity among the ISP's network equipments. As UNI(user network interface), it is also able to diagnose the client data channel connectivity.



In the topology above, RC5x1-FE is take as UNI, it can diagnose the connectivity between A and B using ping function, or login A or B for management using telnet function. As NID it can diagnose the connectivity between RC5x1-FE and ISP's management station C. Using telnet function, it can login C for management.

22.2 User management configuration

This part is about how to use network function on media converter and diagnose the connectivity of the client data channel, including:

- ✧ Default user network configuration
- ✧ Entering user network
- ✧ Configuring user network IP address

✧ Configuring user network diagnoses

22.2.1 Default user network configuration

Function	Default
ARP mapping table item	No mapping
ARP dynamic table item living time	1200s
User network IP address	0.0.0.0
Configure user network default gateway	0.0.0.0
Port diagnoses function	Disabled
Port diagnoses MAC address	The switch MAC address
Port diagnoses received outer-layer/inner-layer tag configuration	untag
Port diagnoses sending packet TAG configuration	untag

22.2.2 Entering user network

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

Only one user is allowed to enter user network at the same time

In user network mode, user network show command exit from user network mode and clear the configuration automatically, except that **exit save-diagconfig** is used.

The configuration in user network mode do not support configuration loading.

22.2.3 Configure user network IP address

Step	Command	Description
1	**config**	Enter global configuration mode
2	**user-network diagnostics**	Enter user network mode
3	**ip address** *ipaddress [mask]*	Configure user network IP address
4	**ip default-gateway** *A.B.C.D*	Configure user network default gateway
5	**show interface ip**	Show IP interface configuration

6	**exit save-diagconfig**	Save user network configuration and return to global configuration mode (only in this can you save the configuration)

User network three-layer port is based on VLAN virtual port configuration, use **ip address** to configure interface IP address and create three-layer interface, use **no ip address** to delete three-layer interface.

Use **ip default-gateway** to configure default gateway, use **no ip default-gateway** to delete default gateway.

User network supports only one virtual three-layer port.

When three-layer interface is configured, with user network interface diagnoses configuration, you can diagnose network connectivity with ping tools, and manage remote host system with telnet tools.

22.2.4 Configure user network interface diagnose configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**user-network diagnostics**	Enter user network mode
3	**diagnose** {**line** *line_list* | **client** *client_list*}	Enable port diagnoses function
4	**diagnose mac-address** *HHHH.HHHH.HHHH*	Configure port diagnoses MAC address
5	**diagnose** {**line** *line_list* | **client** *client_list*} **receive-tag** *HHHH {1-4094}* [**inner-tag** *HHHH {1-4094}*]	Enable port diagnoses received out-layer/inner-layer tag configuration
6	**diagnose** {**line** *line_list* | **client** *client_list*} **send-tag** *HHHH <0-4094> <0-7>* [**inner-tag** *HHHH <0-4094> <0-7>*]	Configure port diagnoses sending packet TAG.
7	**show interface setting**	Show user diagnoses mode configuration
8	**exit save-diagconfig**	Save user network configuration and return to global configuration(only in this way can the network configuration be saved)

User network diagnoses configuration includes: user network virtural MAC configuration, enable port diagnose, receiving message outer layer tag configuration, receiving inner layer tag configuration, sending message tag configuration.

Diagnose that the MAC address the one diagnoses messaged used, by default the front three byte is 000e5f, the last three byte is the same with that of equipment MAC.

Only when port diagnose is enabled can the port receive/send diagnose messages.

Receiving message VLAN configuration means the configuration of specified port receiving/handling message, by default it means to handle all the messages, but if the message includes inner layer tag, user diagnose protocol stack can not recognize it. Use **no diagnose** {**line** *line_list* | **client** *client_list*} **vlan** to restore it the default value. **diagnose {line** *line_list* **| client** *client_list***} receive-tag** HHHH {1-4094}. Use **diagnose {line** *line_list* **| client** *client_list***} receive-tag** HHHH {1-4094} to open port diagnose receied outer layer TAG TPID and VLAN list. The message whose TPID is not in correspondence or VLAN list will not be handled by user diagnose protocol stack. Use **diagnose {line** *line_list* **| client** *client_list***} receive-tag** HHHH {1-4094} **inner-tag** HHHH {1-4094} to enable port diagnoses receiving outer-layer/inner-layer TAG configuration. In this situation, user diagnoses protocol stack handles and

configures only the messages that are coincident with outer-layer/inner-layer TAG.

Sending message TAG configuration is the TAG configuration of sending messages, by default it means sending UNTAG message, use **no diagnose {line** *line_list* **| client** *client_list***} send-tag** to restore it to default value, and send out diagnoses message in UNTAG. Use **diagnose {line** *line_list* **| client** *client_list***} send-tag** HHHH <0-4094> <0-7> to configure port diagnose sending packet outer layer tag, and send out diagnoses message in TAG mode. TAG value include tpid, vlan and cos. Use **diagnose {line** *line_list* **| client** *client_list***} send-tag** HHHH <0-4094> <0-7> **inner-tag** HHHH <0-4094> <0-7> to configure port diagnoses sending packet outer layer TAG and inner layer TAG, and send out diagnose message in double TAG.

Show interface setting shows the current diagnoses configuration.

22.3 Monitoring and maintenance

Use some show commands to look over switch user network configuration for monitoring and maintenance. To do this, follow the commands below:

Command	Description
show arp	Use show arp to show all the items in ARP address mapping table, each item includes: IP address, corresponding MAC address and the table item type.
show interface ip	Use the command to show three layer interface configuration in user diagnoses mode
show interface setting	Show current diagnoses configuration

Use **show arp** to show ARP table items in user diagnoses mode:

Raisecom(config-usrnet)#**show arp**

ARP table aging-time: 1200 seconds(default: 1200s)

Ip Address Mac Address Type

10.0.0.5 0050.8d4b.fd1e static

10.0.0.6 0050.0a3c.ac2e dynamic

10.0.0.7 0050.1c4e.15a7 dynamic

Use **show interface ip** to show three layer interface configuration in user diagnoses mode

Raisecom(config-usrnet)#**show interface ip**

IP Address NetMask Gateway Vid Ports Status

10.0.0.9 255.0.0.0 0.0.0.0 1 1,2 active

Use **show interface setting** to show current diagnose configuration

Raisecom(config-usrnet)#**show interface setting**

diagnose mac-address: 000E.5F01.C2F7

Port : L:1

Diagnose : disable

Received packet : untag

send packet : all

Port : C:1

Diagnose : disable

Received packet : untag

send packet : all

22.4 Typical configuration example

2826 port 3 connects to PC2, ACCESS mode, VLAN is 3, native VLAN is 3; 2826 port 4 connects to PC1, ACCESS mode, VLAN is 4, native VLAN is also 4; the port connected with RC551 is TRUNK port, VLAN is 1-4. By default RC551 system root and login with default user raisecom, and enable all the ports' user diagnose function.

PC1 can telnet to 551, RC551 can ping PC2.

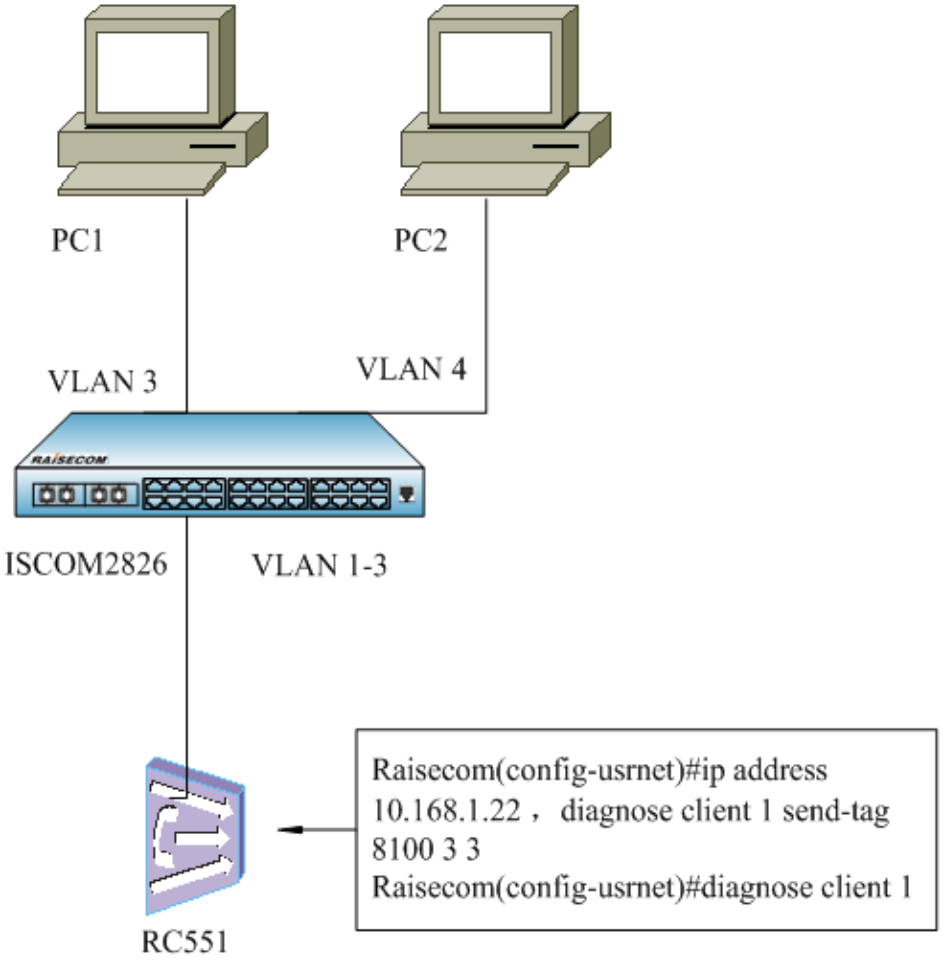


Fig 22-1 user network typical configuration

Chapter 23 Loopback Configuration

This chapter is about how to configure Loopback on the switch, including:

- ✧ Loopback overview
- ✧ Default Loopback configuration list
- ✧ Configuration guide and limit
- ✧ Configuration list and instruction
- ✧ Monitoring and maintenance
- ✧ Typical configuration

23.1 Loopback overview

Loopback is used to examine the network connection. The function is to return the messages that fit the configured rules or the corresponding parameters from the receiving port to sending device. Loopback function should not affect the services, that is to say, the messages that fit the rules can not only doing Loopback, but also going to CPU.

23.1.1 Loopback module

- ✧ Loopback parameter

Stable concept, it is used to record the configuration parameter information related to Loopback under port, including source MAC address, destination MAC address, SVLAN ID, CVLAN ID, when user has configured Loopback parameter and enabled the Loopback of the corresponding rule, the messages that fit the rules will do Loopback. For example, configure the destination MAC to 1234.1234.1234, and enable Loopback based on DMAC, then all the messages with destination MAC address 1234.1234.1234 will do Loopback.

- ✧ Enable Loopback rule

Dynamic principle, use the command to enable Loopback under one rule. Now there are six Loopback rules:

- ➢ Loopback based on port: all the messages entering the port will do Loopback
- ➢ Loopback based on destination MAC address: the messages entering the port whose destination MAC address is the same to the configured parameter will do Loopback
- ➢ Loopback based on source MAC address: the message entering the port whose source MAC address is the same to the configured parameter will do Loopback
- ➢ Loopback based on CVLAN: the messages entering the port whose CVLAN is the designated VLAN ID will do Loopback
- ➢ Loopback based on SVLAN: the messages entering the port whose SVLAN is the designated VLAN ID will do Loopback
- ➢ Loopback based on Double-VLAN (SVLAN, CVLAN): the messages entering the port whose SVLAN and CVLAN are the designated VLAN ID will do Loopback

- ✧ Loopback duration

User can set the duration to 0-30 minutes, and the Loopback of a certain rule under port will be closed

automatically when it comes to a configured time. If user set the duration to 0, Loopback will keep on forever till it is stopped manually.

- ✧ Multicast/broadcast destination MAC address conversion

Address conversion is to transform the destination MAC address of Loopback message to the source MAC address of former sending message, that is to transform Loopback message from multicast/broadcast message to unicast message. By default multicast/broadcast MAC address is configured to conversion enable.

23.1.2 Basic Loopback function

As is shown in 1.1, user configure Loopback rule and enable Loopback function on RC_A port 17, messages from RC_B port 5 reach RC_A port 17, the switch will examine current Loopback rule, and Loopback the messages, return them to RC_B from port 17. User can compare the sending and receiving messages from RC_B to examine the network connection state.

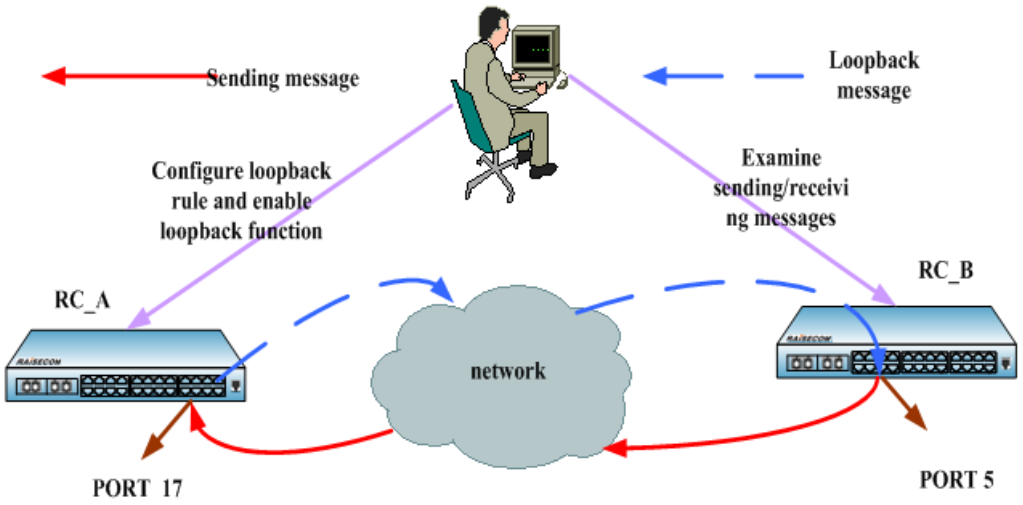


Fig 23-1 Loopback function usage

23.2 Default Loopback configuration list

No.	Attribution	Default value
1	Multicast/broadcast destination MAC address transform	Enable
2	Loopback duration	When Loopback is enabled, default duration time is 0, that is all the time
3	Loopback rule	Loopback based on port when it is enabled

23.3 Loopback configuration restriction and limit

- ➢ Only one Loopback rule of a port can be enabled to one switch at the same time
- ➢ When you have enabled a Loopback of some rule, the parameter of the rule should not be modified
- ➢ When a random port Loopback is enabled, multicast/broadcast destination MAC address transformation is not allowed to be modified.
- ➢ Destination MAC address rule parameter is not allowed to be messages that start with 01-80-c2

- Source MAC address rule parameter should is not allowed to set to multicast/broadcast MAC address
- If port rule configuration does not fit Loopback, it is a configuration problem. To make sure that Loopback function is normally used, you must close other conflicted function.

23.4 Loopback configuration list and instruction

- Configure Loopback parameter
  - Configure Loopback DMAC rule parameter
  - Configure Loopback SMAC rule parameter
  - Configure Loopback CVLAN rule parameter
  - Configure Loopback SVLAN rule parameter
- Enable/disable Loopback multicast/broadcast destination MAC address transformation
- Select and enable Loopback of a certain rule

23.4.1 Configure Loopback DMAC rule parameter

Use **no Loopback** *dmac* to delete Loopback DMAC rule parameter

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface line/client** port-id	Enter port mode
3	**Loopback dmac** *mac-address*	Configure Loopback DMAC rule parameter *Mac-address* destination MAC address, format is HHHH.HHHH.HHHH
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
4	**show interface line/client** [port-id] **Loopback**	Show Loopback related configuration information

The example below is to configure port 2 DMAC rule parameter to 1234.1234.1234

Raisecom#**config**

Raisecom (config)# **interface line/client** *2*

Raisecom(config-port)# **loopback dmac** *1234.1234.1234*

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

Raisecom (config)#**exit**

Raisecom# **show interface line/client** *2* **Loopback**

23.4.2 Configure Loopback SMC rule parameter

Use **no Loopback** *smac* to delete Loopback SMAC rule parameter

Step	Command	Description
1	**config**	Enter global configuration mode

2	**interface line/client** *port-id*	Enter port mode
3	**Loopback smac** *mac-address*	Configure Loopback SMAC rule parameter *Mac-address* source MAC address, format is HHHH.HHHH.HHHH
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
4	**show interface line/client** *[port-id]* **loopback**	Show Loopback related information

The example below is to configure port 3 SMAC rule parameter to 1111.1111.1111

Raisecom#**config**

Raisecom (config)# **interface line/client** *3*

Raisecom(config-port)# **Loopback smac** *1111.1111.1111*

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

Raisecom (config)#**exit**

Raisecom# **show interface line/client** *3* **loopback**

23.4.3 Configure Loopback CVLAN rule parameter

Use **no Loopback** *cvlan* to delete Loopback CVLAN rule parameter.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface line/client** port-id	Enter port mode
3	**Loopback cvlan** *vlan-id*	Configure Loopback CVLAN rule parameter *Vlan-id* user class VLAN ID, range is 1-4094
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
4	**show interface line/client [**port-id] **Loopback**	Show Loopback related information

The example below is to configure port 2 CVLAN rule parameter to 2:

Raisecom#**config**

Raisecom (config)# **interface line/client** *2*

Raisecom(config-port)# **Loopback cvlan** *2*

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

Raisecom (config)#**exit**

Raisecom# **show interface line/client** *2* **Loopback**

23.4.4 Configure Loopback SVLAN rule parameter

Use **no Loopback** *svlan* to delete Loopback SVLAN rule parameter.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface line/client** *port-id*	Enter port mode
3	**Loopback svlan** *vlan-id*	Configure Loopback SVLAN rule parameter *Vlan-id* carrier class VLAN ID, range is 1-4094
4	**Exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
4	**show interface line/client [***port-id***] Loopback**	Show Loopback related configuration

The example below is to configure port 2 SVLAN rule parameter to 3:

Raisecom#**config**

Raisecom (config)# **interface line/client** *2*

Raisecom(config-port)# **Loopback svlan** *3*

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

Raisecom (config)#**exit**

Raisecom# **show interface line/client** *2* **Loopback**

23.4.5 Enable/disable multicast/broadcast destination MAC address transformation

Step	Command	Description
1	**config**	Enter global configuration mode
2	**Loopback dmac-swap** *(enable |disable)*	Enable /disable multicast/broadcast destination MAC address transformation
3	**exit**	Return to privileged EXEC mode
4	**show interface line/client [***port-id***] Loopback**	Show Loopback related configuration

The example below is to enable multicast/broadcast destination MAC address transformation

Raisecom#**config**

Raisecom(config)#**Loopback dmac-swap** *enable*

Raisecom(config)#**exit**

Raisecom# **show interface line/client** *2* **Loopback**

23.4.6 Select Loopback rule and enable Loopback function

Use **no Loopback** to disable Loopback

Step	Command	Description
1	**config**	Enter global configuration mode
2	**Loopback [mode** *{dmac|smac|cvlan|svlan|dvlan}*] **[timeout** *time-num*]	Select Loopback rule and enable Loopback *Time-num* Loopback duration, range is 0-30min
3	**exit**	Return to privileged EXEC mode
4	**show interface line/client [***port-id***] Loopback**	Show Loopback related configuration

The example below is to configure port 2 SVLAN rule parameter to 3, select SVLAN rule and enable Loopback, set the duration time to 5min:

Raisecom#**config**

Raisecom (config)# **interface line/client** *2*

Raisecom(config-port)# **Loopback svlan** *3*

Raisecom(config-port)# **Loopback mode svlan timeout** *5*

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

Raisecom (config)#**exit**

Raisecom# **show interface line/client** *2* **Loopback**

23.5 Loopback monitoring and maintenance

Command	Description
show interface line/client [*port-id***] Loopback**	Show Loopback related configuration

23.5.1 Show Loopback related configuration

Format: **show interface line/client** *[port-id]* **Loopback**

Function: show port Loopback basic configuration and Loopback state

Result:

Set port 3 SVLAN rule parameter to 3, select SVLAN rule, enable Loopback, set duration time to 5min:

IC_A# **show interface line/client** *2* **Loopback**

Port port1:2

Loopback enable: Enable

DMAC Swap: Enable

Loopback rule: SVLAN

Loopback lasting time: 5 m

DMAC: 0000.0000.0000

SMAC: 0000.0000.0000

CVLAN: 0

SVLAN: 3

23.6 Typical example

As is shown in fig 1.1, user can set Loopback rule parameter on RC_A port 17 and enable Loopback function. Set SVLAN parameter to 5, CVLAN parameter to 10, select and enable DVLAN rule Loopback, set the duration time to 10min, disable multicast/broadcast destination MAC address transformation.

Raisecom#**config**

Raisecom(config)#**Loopback dmac-swap** *disable*

Raisecom (config)# **interface line/client** *17*

Raisecom(config-port)# **Loopback svlan** *5*

Raisecom(config-port)# **Loopback cvlan** *10*

Raisecom(config-port)# **Loopback mode dvlan timeout** *10*

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

Raisecom (config)#**exit**

Raisecom# **show interface line/client** *17* **Loopback**

Results:

Port port1:17

Loopback enable: Enable

DMAC Swap: Disable

Loopback rule: DVLAN

Loopback lasting time: 10 m

DMAC: 0000.0000.0000

SMAC: 0000.0000.0000

CVLAN: 10

SVLAN: 5

The messages entering port 17 with CVLAN 10, SVLAN 5 and double TAG will do Loopback, and be sent out from port 17. Loopback message source MAC address will transform to local MAC of RC_A, destination MAC address will be configured according to the transforming rules, which is as follows:

- Unicast message, the destination MAC of egress message is the source MAC of ingress message;
- Multicast/broadcast message is determined by the user enabling/disabling multicast/broadcast message destination MAC address transformation. By default it is enabled, that is the message destination MAC is ingress message SMAC.

Chapter 24 802.3ah OAM

24.1 802.3ah OAM Principle Introduction

IEEE802.3ah OAM (Operation Administration Maintenance) is used to provide more efficient Ethernet link operation, management and maintenance. As the efficient complimentarity of the high managing tool, OAM enhances the Ethernet management and monitoring.

24.1.1 OAM mode

The process of Ethernet OAM connecting is also called Discovery, which is the process of one OAM entity discovers another one in the remote device for creating a stable conversation.

In the process, the connected Ethernet OAM (OAM Function port) entity sends the Ethernet configuration information and local node support Ethernet OAM ability information by switching the information OAM PDU to the opposite in two way. Once OAM receives the configuration data from the opposite, it will decide whether build the OAM connection up. If both ends are agreed to build up the OAM connections, Ethernet OAM protocol will start to run on the LAN Layer.

There are two modes for building up Ethernet OAM connection: active mode and passive mode. The connection can only be active by OAM entity and passive OAM entity has to wait for the connecting request from the opposite OAM entity.

After the Ethernet OAM is connected, OAM entities from both ends send information OAMPDU to keep the connection. If the Information OAMPDU is not received by the OAM entity from opposite in 5 seconds, it will be considered as connection time-out. Thus OAMs are needed to reconnect.

Information OAMPDU packet is sent by internal counter control with maximum rate of 10 packets/second.

24.1.2 OAM loop-back

OAM loop-back can only be achieved after Ethernet OAM connection is built up。 In connected situation, active mode OAM will send OAM loop-back command and opposite will response for that command. As remote is in loop-back mode, all packets but OAMPDU packet will be sent back in the original route.

Periodical loop-back detection can detect network failure on time and find out the failure happened location by subsection loop-back detection. It can help users to remove failure.

24.1.3 OAM events

It is difficult to detect the Ethernet failure, especially when the physical network communicational is in no-breakdown but low network. OAMPDU states a Flag Domain which allows Ethernet OAM entity sends the failure information to the opposite. That Flag also states the threshold events as shown below:

Link Fault: Signal lost in the opposite link.

Dying Gasp: Unpredict states happen, as power cut-down.

Critical Event:Uncertain critical events happen.

Ethernet OAM connecting process is continually sending the Information OAMPDU. Local OAM entity can send the local threshold event information to opposite OAM entity through Information OAMPDU. The Administrators can always notice the link status and solve the related problems on time.

Ethernet OAM monitors the link by Event Notification OAMPDU switchs。Once the link fails, the local link will monitor the failure. And it will send monitors the Event Notification OAMPDU to opposite Ethernet OAM entity to inform the threshold events. Administrator can notice the network status by monitoring the link.

- Error frame event:error frame number in unit time is over stated threshold number.
- Error frame period event:states frame number N as a period; it means in the period of received N error frames, the error fame number is over stated threshold one.
- Error frame second event: indicated in M seconds, the error frame's time in seconds are over the stated threshold number.(error frame second states: an error frame happens in a specific second and this second is called error frame second.)

24.1.4 OAM mib

Devices can gain opposite device link configration/ statistics value through OAM and then get link status/ data.

24.2 802.3ah OAM Mode Configuration

OAM supports two modes: active mode and passive mode. Active mode starts OAM opposite discover process, supports functions but non-response remote loop-back command and variable gained requests; passive mode does not start OAM opposite discover process, does not send remote loop- back command and veriable gained request. Different devices use different mode supports and default configurations. If the device supports passive mode, then its default mode will be passive mode or it will be active mode. If the device only supports one mode, then it does not support mode configuration. OAM mode. OAM mode is all OAM port link share, and users can set mode configuration on the devices which support both two mode as shown below:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**oam** *{active|passive}*	Set OAM as active/passive mode
3	**Exit**	Return to privilege use mode
4	**show oam**	Show OAM loop-back information

Set device OAM as active mode:

Raisecom#**config**

Raisecom(config)#**oam** *active*

Raisecom(config)#**exit**

Raisecom#**show oam**

24.3 802.3ah OAM Active Mode Function

24.3.1 OAM default configuration

Function	Default Value
OAM Enable\Disable	Enable
Opposite OAM event alarm	Disable

24.3.2 OAM enable/disable configuration function

✧ OAM Enable\Disable

OAM is Ethernet point to point link protocal. Enable/Disable is used for all the link ports. In default situation, all ports OAM are Enable, user can Enable/ Disable OAM by the following steps:

Steps	Command	Description
1	**Config**	Entry global configuration mode
2	**interface line/client** *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**oam** {*disable* | *enable*}	Enable or Disable OAM
4	**Exit**	Return Global Configuration mode
5	**Exit**	Return privileged EXEC mode
6	**show oam**	Show OAM Configuration state

Disable port 2 OAM:

Raisecom#**config**

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)#**oam** *disable*

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

Raisecom(config)#**exit**

✧ Show OAM local link status

Privilege mode command: show oam can display OAM link local configuration and status include mode configuration, management status, working status, maximum packet length, configuration version and function support , etc. Through this command, users can understand OAM link configuration, running status, etc.

Raisecom#**show oam**

Port: 1

Mode: Passive

Administrate state: Enable

Operation state: Disabled

Max OAMPDU size: 1518

Config revision: 0

Supported functions: Loopback, Event, Variable

Port: 2

Mode: Passive

Administrate state: Disable

Operation state: Disable

Max OAMPDU size: 1518

Config revision: 0

Supported functions: Loopback, Event, Variable

✧ Show OAM opposite link status

Privilege mode command: show oam peer can display the opposite device information on OAM link, include: opposite MAC address, manufactory OUI, manufactory information, mode configuration, maximum packet length, configuration version and function support information. If OAM link is not connected, then there no information will be displayed.

Raisecom#**show oam peer**

Port: 1

Peer MAC address: 000E.5E00.91DF

Peer vendor OUI: 000E5E

Peer vendor info: 1

Peer mode: Active

Peer max OAMPDU size: 1518

Peer config revision: 0

Peer supported functions: Loopback, Event

24.3.3 Run OAM loop-back function

OAM provide link layer remote loop-back system, which can be used for located link error position, performance and quality test. Under link loop-back status, devices will loop-back all link received packets to the opposite devices except OAM packet. Local device uses OAM remote command to enable or disable remote loop-back. Opposite device will use loop-back configuration command to control whether response loop-back command.

In central office end , users can build up remote loop-back through remote loop-back

command.

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface line/client** *port_number*	Entry Ethernet physical interface mode, *port_number* is physical interface number
3	**oam remote-loopback**	Build up remote loop-back
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam loopback**	Show OAM loop-back situation

Build remote loop-back on port link 2:

Raisecom#**config**

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)#**oam remote-loopback**

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

Raisecom(config)#**exit**

Raisecom#**show oam loopback**

Users can remove remote loop-back as below:

Steps	Command	Description
1	**Config**	Entry global configuration mode
2	**interface line/client** *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**no oam remote-loopback**	Remove remote loop-back
4	**Exit**	Return global configuration mode
5	**Exit**	Return privileged EXEC mode
6	**show oam loopback**	Show OAM loop-back state

Remote loop-back on remove end link 2:

Raisecom#**config**

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)#**no oam remote-loopback**

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

Raisecom(config)#**exit**

Raisecom#**show oam loopback**

Note: Remote loop-back only can be achieved after Ethernet OAM is connected.

24.3.4 Opposite OAM event alarm function

By default, when opposite link monitor event is received, device will not inform network managing center through SNMP TRAP. Users can use Enable/Disable opposite monitor events is informed to the network managing center.

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface line/client** *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**oam peer event trap** *{disable | enable}*	Enable or Disable opposite OAM monitor event is informed network managing center
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam trap**	show OAM TRAP information

Enable port 2 opposite link monitoring event informed to network managing center:

Raisecom#**config**

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)# **oam peer event trap** *enable*

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

Raisecom(config)#**exit**

Raisecom#**show oam trap**

24.3.5 View opposite IEEE 802.3 Clause 30 mib

OAM variable gain is a link monitoring measure. It allows local device to get opposite device current variable value thus get current link status. IEEE802.3 Clause30 particulary states the variables which support OAM gain and their representing way. Variable can be divided into its biggest unit -- object which include package and attribute. Package also is combined by sereval attribute. Attribute is variable's smallest unit. OAM variable gain uses Clause 30 to state object/package/attribute's branch descriped requesting objects. And branches plus the variable value are used to represent object response variable request. Now, all devices have supported both OAM information and port statistics as object variable gain. EPON OLT device also supports MPCP and OMPEmulation object information gain.

When device OAM work as active mode, users can gain opposite devices OAM information or port statistics variable values as the steps below:

Steps	Command	Description

1	**show oam peer** *{link-statistics| oam-info} {port-list|client|line} port_number*	Gain opposite device OAM information or port statistics variable value *port_number* is physical interface number

Gain port 2 opposite device OAM information value is shown as below:

Raisecom(debug)#**show oam peer oam-info port-list** *2*

Note: OAM variable gain is only achieved if and only if Ethernet OAM connection is built up.

24.3.6 OAM statistics clear function

OAM calculates the number of all different types of OAM packets which are sent/received on each OAM port link. The types of packets are:information, link event information, loop-back control, variable gain request, variable gain response, organise using, uncertain type and repeated event information. Users can clear port link OAM statistics information as follow steps:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface line/client** *port_number*	Entry Ethernet physical interface mode *port_number*is physical interface number
3	**clear oam statistics**	Clear OAM port link statistics information
4	**exit**	Entry global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam statistics**	show OAM link statistics information

Clear port 2 OAM link statistics information as below:

Raisecom#**config**

Raisecom(config)#**interface line/client** 2

Raisecom(config-port)#**oam clear statistics**

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

Raisecom(config)#**exit**

Raisecom#**show oam statistics**

24.3.7 Monitoring and maintenance

Command	Description
show oam	show OAM link's local configuration and status
show oam peer	show OAM link's opposite device information

show oam loopback	Show remote loop-back information
show oam peer event	show opposite device informed event
show oam trap	Show OAM related SNMP TRAP information and its configuration situation.
show oam statistics	show all OAM port link statistics information

24.3.8 Configuration example

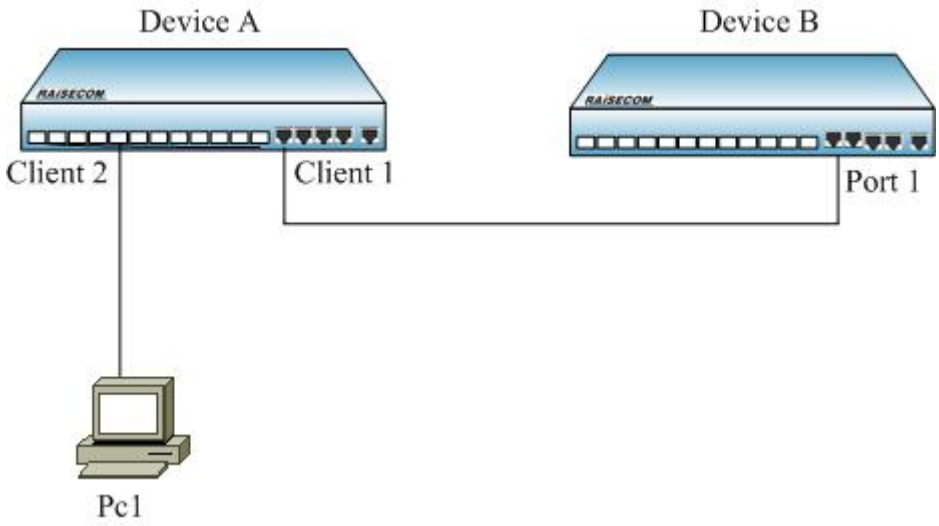


Figure 24-1

As figure 1-1, to set remote loop-back as following configuration:

Raisecom#**config**

Raisecom (config)#**interface line/client** *1*

Raisecom(config-port)#**oam** *enable*

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

Raisecom#**show oam port-list** *1*

Port: 1

Mode: Active

Administrate state: Enable

Operation state: Operational

Max OAMPDU size: 1518

Config revision: 0

Supported functions: Loopback, Event

Raisecom#**config**

Raisecom (config)#**interface line/client** 1

Raisecom(config-port)#**oam remote-loopback**

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

Raisecom(config)#**exit**

Raisecom#**show oam loopback**

Port: 1

Loopback status: Remote

Loopback react: Ignore

24.4 802.3ah OAM Passive Function

24.4.1 OAM default configuration

Function	Default Value
Oam Enable\Disable	Enable
Oam mode	Passive
Response\Ignore opposite oam loop-back Configuration	Response
Local oam event alarm	Disable
Oam failure indication	Enable
Error frame periodical event window and threshold.	window 10 (s) Threshold 1 (unit)
Error frame event window and threshold	Window 10 (s) Threshold 1 (unit)
Error frame second statitics event window and threshold	Window 600 (s) Threshold 1 (unit)

24.4.2 OAM enable/disable configuration

- OAM Enable\Disable

OAM is Ethernet point to point link protocal, Enable/Disable is for different link port. In default situation, all ports OAM are Enable. Users can enable/disable OAM by following steps:

Steps	Command	Description
1	**Config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**oam** {**disable** | **enable**}	Enable or Disable OAM
4	**Exit**	Return to global configuration mode
5	**Exit**	Return to privileged EXEC mode

6	**show oam**	show OAM configuration situation

Disable port 2 OAM as follow:

Raisecom#**config**

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)#**oam** *disable*

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

Raisecom(config)#**exit**

- Show OAM local link status

Privileged EXEC mode command: show oam can show OAM link local configuration and status, displayed information is include mode configuration, managing status, running status, maximum packet length, configuration version and function support information. By this command, users can understand OAM link configuration, running status such information.

Raisecom#**show oam**

Port: 1

Mode: Passive

Administrate state: Enable

Operation state: Disabled

Max OAMPDU size: 1518

Config revision: 0

Supported functions: Loopback, Event, Variable

Port: 2

Mode: Passive

Administrate state: Disable

Operation state: Disable

Max OAMPDU size: 1518

Config revision: 0

Supported functions: Loopback, Event, Variable

- Show OAM opposite link status

Privileged EXEC mode command: show oam peer can show OAM link's opposite device information, include opposite MAC address, manufactory OUI, manufactory information, mode configuration, maximum packet length, configuration version and function support information. If OAM link is not built up, then it will not show any information.

Raisecom#**show oam peer**

Port: 1

Peer MAC address: 000E.5E00.91DF

Peer vendor OUI: 000E5E

Peer vendor info: 1

Peer mode: Active

Peer max OAMPDU size: 1518

Peer config revision: 0

Peer supported functions: Loopback, Event

24.4.3 Response/ignore opposite OAM loop-back configuration function

OAM provide link layer remote loop-back system, can be used for locating link error position, function and quality testing. In link loop-back status, all packets received from the link but OAM packet loop-back to opposite device. Local device use OAM remote loop-back command enable or disable remote loop-back, opposite device uses loop-back configuration command control to response loop-back command.

In default situation, device loop-back responses as Enable, users set loop-back response configuration as below:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**oam loopback** {**ignore** | **process**}	Enable or Disable OAM loop-back response
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam loopback**	show OAM loop-back situation

Disable response port link 2 OAM remote loop-back:

Raisecom#**config**

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)#**oam loopback ignore**

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

Raisecom(config)#**exit**

Raisecom#**show oam loopback**

24.4.4 OAM link monitor configuration function

OAM link monitor is used to detect and report different link errors. When link errors are detected, device informs opposite error cause time, window and threshold configuration by OAM event information packets. Opposite reports events to network managing center by SNMP TRAP. Local device reports events directly to network managing center by SNMP TRAP. OAM link monitoring supports events below:

Error frame events: indicates periodical error frames over threshold. When indicated time periodicaly error frames over threshold, device will have that event.

Error frame periodical event: lately N frames' error are over threshold, N is indicated value; once laterly N frames' error over threshold is detected, device will release that event.

Error frame second statistics event: lately M seconds, the error frams' second number over threshold. M is the indicated value. When error frame second number is over indicated threshold in M seconds, device releases that event.

OAM named the previous monitoring period, frame calculate number and second statistics number as monitoring window.

Users can set the link monitoring configuration as steps below:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Enter Ethernet physical interface mode *port_number* is physical interface number
3	**oam errored-frame window** <*1-60*> **threshold** <*0-65535*>	Config error frame monitoring window and threshold <*1-60*> is monitoring window, unit is second, <*0-65535*> is threshold.
4	**oam errored-frame-period window** <*100-60000*> **threshold** <*0-65535*>	Config error frame periodical event monitoring window and threshold <*100-60000*> is monitoring window, unit is second, <*0-65535*>is threshold.
5	**oam errored-frame-seconds window** <*10-900*> **threshold** <*0-900*>	Config error frame statistics monitoring window and threshold <*10-900*> is monitoring window, unit is second, <*0-900*> is threshold.
6	**exit**	Return to global configuration mode
7	**exit**	Return to privileged EXEC mode
8	**show oam notify**	show OAM events configuration situation

Configuration port 2 error frame event monitoring window is 2 seconds, threshold is 8 error frame: error frame period event monitoring window is 100 ms, threshold is 128 error frames; error frame second statistics event monitoring window is 100 seconds, threshold is 8 seconds.

Raisecom#**config**

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)# **oam errored-frame window** *2* **threshold** *8*

Raisecom(config-port)# **oam errored-frame-period window** *100* **threshold** *128*

Raisecom(config-port)# **oam errored-frame-second window** *100* **threshold** *8*

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

Raisecom(config)#**exit**

Raisecom#**show oam notify**

Using physical layer interface configuration command **no oam errored-frame** can resume error frame event monitoring window and threshold as Default Value

Using physical layer interface configuration command **no oam errored-frame-period** can resume error frame event monitoring window and threshold as Default Value

Using physical layer interface configuration command **no oam errored-frame-second** can resume error frameevent monitoring window and threshold as Default Value.

24.4.5 OAM fault indication function

OAM fault indication function is used to inform opposite device local device with abnormal event as link-fault, power break, abnormal temperature, etc. Those will cause the faults as link disable, device restart, ect. Now stated faults are link-fault, dying-gasp and critical-event caused by abnormal temperature. In default, device fault indicated as Enable status, thus when fault happened, device informs opposite by OAM. Users can Enable or Disable faults (except link-fault fault indicated must inform opposite) by following steps:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**oam notify** {*dying-gasp* | *critical-event*} {*disable*|*enabl*}	Enable or Disable OAM error indicated opposite
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam notify**	show OAM event configration situation

Disable port 3 critical-event fault indication:

Raisecom#**config**

Raisecom(config)#**interface line/client** *3*

Raisecom(config-port)# **oam notify critical-event** *disable*

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

Raisecom(config)#**exit**

Raisecom#**show oam notify**

24.4.6 Local OAM event alarm function

In Default, when link monitoring event is detected, device will not inform network managing center by SNMP TRAP. Users can use Enable or Disable to inform network managing center the monitor events by

following steps:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**oam event trap** *{disable | enable}*	Enable or Disable OAM monitoring event to inform network managing center
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam trap**	show OAM TRAP information

Enable port 2 link monitoring event inform to network managing center:

Raisecom#**config**

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)# **oam event trap** *enable*

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

Raisecom(config)#**exit**

Raisecom#**show oam trap**

24.4.7 IEEE 802.3 Clause 30 mib support

OAM variable gain is a link monitoring measure. It allows local device to gain opposite device lately variable value. Thus it can gain lately link status. IEEE802.3 Clause30 detailly states support OAM gain variable and its representation. Object is the biggest division of variable. Each object has package and attribute. Package is include many attribute. Thus attributes are the smallest variable unit. OAM variable gain states object/package/attribute branches description as request objects, and branches plus variable value are used to represent as object response variable request. Now, all devices can support OAM information and port statistics variable gain. EPON OLT device also supports MPCP and OMPEmulation object information gain.

When device OAM is in active mode, users can gain opposite device OAM information or port statistics variable value by following steps:

Steps	Command	Description
1	**show oam peer** {**link-statistics** | **oam-info**} { **client** | **line**} *port_number*	Gain opposite device OAM informationor port statistics variable value *port_number* is physical interface number

Gain port 2 opposite device OAM information value:

Raisecom(debug)#**show oam peer oam-info port-list** *2*

24.4.8 OAM statistics clear function

OAM statistics sending/receiveing all OAM packets number on each OAM port link. Packets types:information, link events information, loop-back control, variable gain request, variable gain response, organise using, uncertain type and repeat event inforamtion. Users can clear port link OAM statistics information as following steps:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**clear oam statistics**	Clear OAM port link statistics information
4	**exit**	Return to global Configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam statistics**	show OAM link statistics information

Clear port 2 OAM link statistics information

Raisecom#**config**

Raisecom(config)#**interface line/client** 2

Raisecom(config-port)#**oam clear statistics**

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

Raisecom(config)#**exit**

Raisecom#**show oam statistics**

OAM record recent happening local and opposite link monitoring and fault (key) events. Users can clear port link OAM local and opposite events record as following steps:

Steps	Command	Description
1	**config**	Entry global configuration mode
2	**interface** { **line** | **client**} *port_number*	Entry Ethernet physical interface mode *port_number* is physical interface number
3	**clear oam event**	Clear OAM port link event record
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged EXEC mode
6	**show oam event**	show OAM link local event record
7	**Show oam peer event**	show OAM link opposite event record

Clear port 2 OAM link events record:

Raisecom#**config**

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)# **clear oam event**

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

Raisecom(config)#**exit**

Raisecom#**show oam event**

Raisecom#**show oam peer event**

24.4.9 Monitoring and maintenance

Command	Description
show oam	show OAM link local configuration and status
show oam peer	show OAM link information on opposite device
show oam loopback	show remote loop-back information
show oam event	show local device happening events
show oam peer event	show opposite device informing events
show oam notify	show all OAM link local events informing configuration
show oam statistics	show all OAM port link statistics information

24.4.10Configuration example

According to Figure 24-1, if response remote loop-back, device A can be configured as below:

Raisecom#**config**

Raisecom(config)#**oam passive**

Raisecom (config)#**interface client** *1*

Raisecom(config-port)#**oam** *enable*

Raisecom (config-port)# **oam loopback process**

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

Raisecom(config)#**exit**

Raisecom#**show oam loopback**

Port: client1

Loopback status: No

Loopback react: Process

Chapter 25 Extended OAM Configuration Guide

25.1 Extended OAM principle overview

Extended OAM, using IEEE802.3ah OAM to manage and monitor the remote device. It is composed by 3 parts:

1. Get the attribute of remote device;

2. Upload and down file of remote device;

3. Manage extended OAM link state and statistic.

Extended OAM includes the followings:

- Get remote attribute: the extended OAM attribute can be used to get the remote attribute form the center site.
- Set remote device: config the remote device, including host name, enable and disable port, duplex, bandwidth, fault transfer etc.
- Set remote device nettwork management parameter: can config remote device network management parameter, such as ip address, gateway, community parameter and management VLAN etc, then implement full management with SNMP protocol.
- Remote TRAP: when the port of remote device show LINK UP/DOWN, the remote device will send extended OAM notification fram to inform the center site, then the center device will send TRAP.
- Extended remote loopback: the remote optical port can be set loopback function, the function of whether to count repeatedly can be set.
- Reset remote device: send command to reset remote device.
- Other remote device function management: with the increasing of remote device, center device can manage more remote device with extended OAM function such as: SFP、Q-in-Q、Virtual Circuit diagnosis etc.
- Download remote file: the remote can get remote file from FTP/TFTP server. The file also can be send from the server to center device, then the remote device can get from the center device.
- Upload remote file: put the file to FTP/TFTP server, or from the remote device to center one, then put to server from the center device.
- Link statistic and management of extended OAM function.

Note: extended OAM link can only be established between center and remote site. The devices of two end must be set to master and passive, or the link can't be up.

25.2 Extended OAM management

25.2.1 Default extended OAM configuration

Function	Default
Powered configuration request	Enable
Extended OAM notice	Enable
Remote end trap switch	open

25.2.2 Extended OAM configuration mode

To configure remote equipments on a local end equipment, you need to enter remote configuration mode. The steps to enter remote configuration mode are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *portid*: physical port ID
3	**remote-device**	Enter remote configuration mode

To configure remote equipment ports on local equipment, you need to enter remote interface configuration mode. The steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**interface client** *client-id*	Enter remote physical port configuration mode *Clinet-id* port ID

25.2.3 Remote equipment system configuration

Configure remote equipment system configuration, including configuring remote equipments' hostname, the maximum frame length, save and delete the configuration files.

The steps to configure remote equipment hostname and remote equipment maximum frame length are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**hostname** *HOSTNAME*	Configure remote equipment hostname *HOSTNAME* remote system network name
5	**system mtu** <*1500-8000*>	Configure remote equipment maximum frame length

6	**show remote-device information**	Show current remote equipment hostname and actual effective maximum frame length

Note: configure the maximum frame length of remote equipment; the actual effective value may be different because of different remote equipment. For example, RC552-GE can configure remote maximum frame length to 1916 bytes or 1536 bytes. If the remote end is RC552-GE, and the configuration value is less than 1916, the effective value is 1536, or it is 1916.

The steps to save remote equipment configuration file is as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *portid*: physical port number
3	**remote-device**	Enter remote configuration mode
4	**write**	Save remote equipment configuration file

The steps to delete remote equipment configuration file is as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *portid*: physical port number
3	**remote-device**	Enter remote configuration mode
4	**erase**	Delete remote equipment configuration file

When executing the command to delete remote equipment configuration file, you need to confirm your operation.

Note:

- The operation to the configuration file is to save and delete the file on remote equipment, not to operate the local equipments file system.
- It takes a long time save and delete remote files, so when executing the command, there may be some unusual situations like OAM link breaking down.

25.2.4 Configure extended OAM protocol

The steps to enable/disable powered configuration request configuration are as follows:

Step	Command	Description

1	**config**	Enter global configuration
2	**extended-oam config-request** *enable* **extended-oam config-request** *disable*	Enable/disable powered configuration request *enable*: enable powered configuration request *disable*: disable powered configuration request
3	**exit**	Return to privileged EXEC mode
4	**show extended-oam status**	Show extended OAM link state

The steps to disable/enable sending extended OAM notices configuration are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**extended-oam notification** *enable* **extended-oam notification** *disable*	Enable/disable sending extended OAM notice *enable*: enable sending extended OAM notice *disable*: disable sending extended OAM notice
3	**exit**	Return to privileged EXEC mode
4	**show extended-oam notification**	Show OAM informing frame enable configuration state

25.2.5 Configure remote equipment port

- Configure remote equipment port enable/disable

The steps to disable remote equipment ports are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *portid*: port physical ID
3	**remote-device**	Enter remote configuration mode
4	**interface client** *client-id*	Enter remote physical port configuration mode *client-id:*port ID
5	**shutdown**	Shutdown remote equipment port

In remote port configuration mode, use **no shutdown** to enable remote equipment port.

- Configure remote equipment port rate/duplex

The steps to configure remote equipment ports rate/duplex are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode
3	**remote-device**	Enter remote configuration mode
4	**interface client** *client-id*	Enter remote physical port configuration mode
5	**speed** *{**auto** | 10| 100 |1000 }* **duplex** *{ **full** | **half** }*	Configure port rate and duplex mode

When the equipment has 1000M optical port, we can configure optical port auto-negotiation function, the steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**line-speed auto**	Configure remote equipment optical port auto-negotiation

In remote configuration mode, use **no line-speed auto** to shutdown optical port auto-negotiation function.

Note: when remote equipment is configured port rate/duplex, there may be some unusual situations like OAM link breaking down.

- Configure remote equipment port stream control/speed control

The steps to enable/disable remote equipment stream control are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *Portid* physcial port ID
3	**remote-device**	Enter remote configuration mode
4	**interface client** *client-id*	Enter remote physical port configuration mode
5	**flowcontrol** *{on|off}*	Enable/disable remote equipment port stream control function

The steps to configure remote equipment port in/out direction bandwidth are as follows:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**interface** {**port**|**line**|**client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**rate-limit line** *line-id* **ingress** *rate* **rate-limit client** *client-id* **ingress** *rate*	Configure remote equipment port in direction bandwidth *Line-id* line port ID *Client-id* client port ID *Rate* bandwidth
5	**rate-limit line** *line-id* **egress** *rate* **rate-limit client** *client-id* **ingress** *rate*	Configure remote equipment port out direction bandwidth

Run **no rate-limit line** *line-id* **ingress** or **no rate-limit client** *client-id* **ingress** to restore in remote configuration mode.

Run **no rate-limit line** *line-id* **engress** or **no rate-limit client** *client-id* **egress** to restore in remote configuration mode.

- Configure remote equipment port description

The steps to configure remote port information are as follows:

Step	Command	Description
1	**config**	Enter global configuration
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**description line** *line-id WORD* **description client** *client-id WORD*	Configure remote equipment port description information *Line-id WORD* remote port description information *Client-id WORD* remote port description information

In remote configuration mode, use **no description line** *line-id* or **description client** *client-id WORD* to delete the description information.

In remote configuration mode, use **show interface line/client** and **show interface line/client detail** to show remote port configuration information.

- Start/shutdown extended remote loopback

Starting loopback function may affect data transmission.

Enable remote equipment optical port inside-loopback, you can select the parameter so that the response

end could recalculate CRC. The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration ode
2	**interface** {**port**|**line**|**client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**inside-loopback** [**crc-recalculate**]	Start remote equipment optical port inside-loopback

In remote configuration mode, use **no inside-loopback** to stop remote equipment inside-loopback, use **show inside-loopback** to show remote optical port inside-loopback state and parameter.

- Run remote equipment line diagnoses function

Executing remote equipment line diagnoses function may affect the link and data transmission. The steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port**|**line**|**client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode

In remote configuration mode, use **show cable-diagnostics** to show remote equipment line diagnoses result.

25.2.6 Upload/download files from remote equipment

- Download the file from server to remote equipment

The system bootroom file, startup file, startup configration file and FPGA file of remote device can be downloaded from server to remote device (center device as the relay). This function can be started by center device or remote device, and multiple remote devices can be upgraded at the same time.

Center device starts, download from FTP/TFTP server:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port**|**line**|**client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**download** {**bootstrap** | **system-boot** | **startup-config** | **fpga**} **ftp** *A.B.C.D USRNAME PASSWORD FILENAME*	Download the file from FTP server to remote equipment *A.B.C.D:* Server IP address

download {**bootstrap** | **system-boot** | **startup-config** | **fpga**} **tftp** *A.B.C.D FILENAME*	*USRNAME:* FTP server username *PASSWORD:* FTP server password *FILENAME:* The filename on the server Download the files from TFTP server to remote equipment *A.B.C.D:* server IP address *FILENAME:* the filename on the server

Acting from the remote equipment, the steps to download files from FTP/TFTP server to remote end are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *Portid* physcial port ID
3	**download** {**bootstrap**|**system-boot**| **startup-config** | **fpga**} **ftp** *A.B.C.D USRNAME PASSWORD FILENAME* **download** {**bootstrap**|**system-boot**| **startup-config** | **fpga**} **tftp** *A.B.C.D FILENAME*	Download the file from FTP server to remote equipment *A.B.C.D:* Server IP address *USRNAME:* FTP server username *PASSWORD:* FTP server password *FILENAME:* The filename on the server Download the files from TFTP server to remote equipment *A.B.C.D:* server IP address *FILENAME:* the filename on the server

When the file downloading is over, the remote equipment can be shown with **dir** in privileged EXEC mode, and use **erase** to delete.

- Upload files to the server from remote equipment

The system bootroom file and startup configuration file on the remote equipment can be transmitted through local end to do uploading from remote equipment to the server. The function can be started by local equipment or remote equipment. When it is started from local equipment, we can no upgrade several remote equipments at the same time.

Started from local equipment, the steps to upload file from remote equipment to FTP/TFTP server are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface** {**port** | **line** | **client**} *portid*	Enter ethernet physical port mode *Portid* physical port ID

3	**remote-device**	Enter remote configuration mode
4	**upload** {**startup-config** | **system-boot** } **ftp** *A.B.C.D USRNAME PASSWORD FILENAME* **upload** {**startup-config** | **system-boot**} **tftp** *A.B.C.D FILENAME*	Upload file from remote equipment to FTP server *A.B.C.D:* Server IP address *USRNAME:* FTP server username *PASSWORD:* FTP server password *FILENAME:* The filename on the server Upload file from remote equipment to TFTP server *A.B.C.D:* server IP address *FILENAME:* the filename on the server

Started from remote equipment, the steps to upload file from remote equipment to FTP/TFTP server are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** *portid*	Enter ethernet physical interface mode *Portid* physical port ID
3	**upload {startup-config | system-boot } ftp** *A.B.C.D USRNAME PASSWORD FILENAME* **upload {startup-config | system-boot } tftp** *A.B.C.D FILENAME*	Upload file from remote equipment to FTP server *A.B.C.D:* Server IP address *USRNAME:* FTP server username *PASSWORD:* FTP server password *FILENAME:* The filename on the server Upload file from remote equipment to TFTP server *A.B.C.D:* server IP address *FILENAME:* the filename on the server

- Download remote equipment file from the server to local end

The remote equipment system bootroom file, startup file, startup configuration file and FPGA file can all be downloaded from server to local end using FTP/TFTP protocol, then be saved in local FLASH file system with a designated filename, making preparation for further upgrading.

When local end saves remote file, it will add postfix automatically according to the file type, so the local filename designated by user does not need postfix. What's else, the filename designated by remote file can not be the same with the filename of local end its own in flash. That is, the remote equipment's bootroom file can not be named as system-boot; the remote equipment's startup configure file can not be named as startup-config; the remote equipment's FPGA file can not be named as FPGA. However, the system bootroom file is not saved in FLASH, so the bootroom file of remote equipment can be named as bootstrap.

In privileged EXEC mode, the steps to download remote equipment file from the server to local end are as follows:

Step	Command	Description
1	**download {remote-bootstrap | remote-system-boot | remote-startup-config|remote-fpga} ftp** *A.B.C.D USRNAME PASSWORD FILENAME LOCAL-FILENAME* **download { remote-bootstrap | remote-system-boot | remote-startup-config|remote-fpga} tftp** *A.B.C.D FILENAME LOCAL-FILENAME*	*A.B.C.D:* server IP address *USRNAME:* FTP server username *PASSWORD:* FTP server password *FILENAME:* the filename on FTP server *LOCAL-FILENAME:* the filename saved in local end *A.B.C.D:* server IP address *FILENAME:* the filename on the server *LOCAL-FILENAME:* the filename saved on local end

When the downloading is over, you can use **dir** to show the state in privileged EXEC mode on local equipments, and use **erase** to delete.

- Upload remote equipment file from local end to the server

The remote file saved in local equipment's FLASH can be uploaded using FTP/TFTP to the server. The steps are as follows:

Step	Command	Description
1	**upload {remote-bootstrap | remote-system-boot | remote-startup-config|remote-fpga} ftp** *A.B.C.D USRNAME PASSWORD FILENAME LOCAL-FILENAME* **upload {remote-bootstrap | remote-system-boot | remote-startup-config|remote-fpga} tftp** *A.B.C.D FILENAME LOCAL-FILENAME*	*A.B.C.D:* server IP address *USRNAME:* FTP server username *PASSWORD:* FTP server password *FILENAME:* the filename on FTP server *LOCAL-FILENAME:* the filename saved in local end *A.B.C.D:* server IP address *FILENAME:* the filename on the server *LOCAL-FILENAME:* the filename saved on local end

- Download file from local end to remote equipment

The remote file saved in local equipment FLASH, can be downloaded to remote equipment using extended OAM protocol. The function can be started from local equipment or remote equipment. When started from local equipment, several remote equipments can be upgraded at the same time.

Started from local equipment, the steps to download file from local end to remote equipments are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** *portid*	Enter Ethernet physical interface mode

3	**remote-device**	Enter remote configuration mode
4	**download { bootstrap | system-boot | fpga }** *FILENAME* **download startup-config [***FILENAME***]**	Download bootroom file, startup file and FPGA file from local end to remote equipment *FILENAME:* the filename on local end Download configuration file from local end to remote equipment *FILENAME:* the filename on local end

Started from remote end, the steps to download file from local end to remote end are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** *portid*	Enter ethernet physical interface mode *Portid* physical port ID
3	**download {bootstrap | system-boot | fpga}** *FILENAME* **download startup-config [***FILENAME***]**	Download bootroom file, startup file and FPGA file from local end to remote equipment *FILENAME:* the filename on local end Download configuration file from local end to remote equipment *FILENAME:* the filename on local end

When file download is over, you can use **dir** to show the state in privileged EXEC mode on remote equipment and use **erase** to delete.

25.2.7 Configure remote equipment to network management enabled equipment

- Configure remote equipment SNMP community and IP address

The steps to configure remote equipment community name and IP address are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port|line|client}** *portid*	Enter Ethernet physical interface mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**snmp-server community** *community-name {ro|rw}*	Configure remote equipment community name and priority. *community-name* community name *ro* read only *rw* read & write

5	**ip address** *ip-address [ip-mask] vlan-list*	Configure remote equipment IP address *ip-address* *ip-mask* *vlan-list*: the managed VLAN list

In remote configuration mode, use **no snmp-server community** *community-name* to delete remote equipment community name.

When configuring IP address we need to designate and manage VLAN as well, if the VLAN does not exist, create VLAN (by default all the ports are member port); if related VLAN exists, the member port configuration will not be modified. In remote configuration mode, use **no ip address ip-address** to delete remote port IP address.

In remote configuration mode, use **show remote-device information** to show remote community name and IP address information.

- Configure remote equipment Q-in-Q

Configure remote equipment flexible Q-in-Q function, the attributions that need to be configured include: switch mode, TPID, local VLAN and access interface.

When configuring remote equipment to complete transparent mode, the other configurations, like TPID, local VLAN and access interface, are all not available. The steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**switch-mode transparent**	Configure remote equipment to complete transparent mode

When configuring remote equipment to Dot1q VLAN transparent mode, or single TAG mode, local VLAN and access port is valid, while TPID is not. When the equipment is configured to single TAG mode, the data packet coming from the access port will be marked local VLAN ID TAG if it has no TAG; if it has, it will not be handled.

The configuration steps are as follows;

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**switch-mode dot1q-vlan native-vlan** *<1-4094>* **[line]**	Configure remote equipment to Dot1q VLAN transmission mode

		native-vlan: local VLAN *<1-4094>:* VLAN ID; **line**: Line port is the access port, when the keyword line is not selected, it means that client port is the access port

Configure remote equipment to Double tagged VLAN transmission mode, that is in double TAG mode, TPID, local VLAN and access port are all valid. When the equipment is configured double TAG mode, the data packet coming from the access port will be marked specific TPID and local VLAN ID outer layer TAG, whatever it has TAG or not.

The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port|line|client}** *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**switch-mode double-tagged-vlan [tpid** *HHHH***] native-vlan** *<1-4094>* **[line]**	Configure remote equipment to Double tagged VLAN transmission mode **native-vlan:** local VLAN; *<1-4094>:* VLAN ID; **Line:** Line port is the access port **tpid:** outer-layer tagged TPID *HHHH:* outer-layer tagged TPID, hexadecimal number, 0000 to FFFF When tpid is not configured, it means the TPID that takes 0x9100 as the outer-layer TAG

In remote configuration mode, run **show remote-device information** to show remote equipment flexible Q-in-Q function related configuration.

25.2.8 Save remote equipment configuration information to local end

When remote equipment belongs to RC552 serious, the equipment itself will not save configuration file, but it is able to save remote configuration content to local end using **writ local.** When the local equipment is rebooted, it will load the saved 552 configuration file, and if there is configuration request from remote 552, the saved configuration will be sent to remote end. The saving steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port|line| lient}** *portid*	Enter ethernet physical interface mode *Portid* physical port mode

3	**remote-device**	Enter remote configuration mode
4	**write local**	Save remote configuration to local FLASH

If there is no 552 configuration file when local end is started, and local end has not sent configuration to remote 552 yet after booting, execute the command and you will be failed.

Saving FLASH file takes a long time, so when executing the command, unusual situations like OAM link breaking down may happen.

25.2.9 Reset remote equipment

The steps to reset remote equipment are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port|line|client}** *portid*	Enter ethernet physical port mode *Portid* physical port ID
3	**remote-device**	Enter remote configuration mode
4	**reboot**	Reset remote equipment

You need to confirm you operation after reset command is executed.

When remote equipment is resetting or rebooting, OAM link may break down, and local equipment may lose the connection to remote equipment.

25.2.10Extended OAM statistic clear function

Extended OAM counts the sending and receiving extended OAM messages number on each OAM link, the extended OAM message types include: variable acquirement and response, variable setting and response, file request and file data, notice and so on. User can follow the steps below to clear statistic information:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**clear extended-oam statistics [port-list** *port-list***]** **clear extended-oam statistics [line-list** *line-list***]** **clear extended-oam statistics [client-list** *client-list***]**	Clear extended OAM link static information

25.2.11Monitoring and maintenance

Command	Description

show interface line/client	Show remote equipment port information
show interface line/client detail	Show remote equipment port detailed information
show interface line/client statistics	Show remote equipment port static information
show oam capability	Show remote equipment ability of supporting OAM management
show remote-device information	Show remote equipment basic information
show sfp	Show remote equipment SFP information
show cable-diagnostics	Show link diagnoses result
show inside-loopback	Show remote loopback state and parameter
show extended-oam statistics	Show extended OAM frame static information
show extended-oam status	Show extended OAM link state
show snmp trap remote	Show remote trap enable configuration

25.2.12Typical configuration example

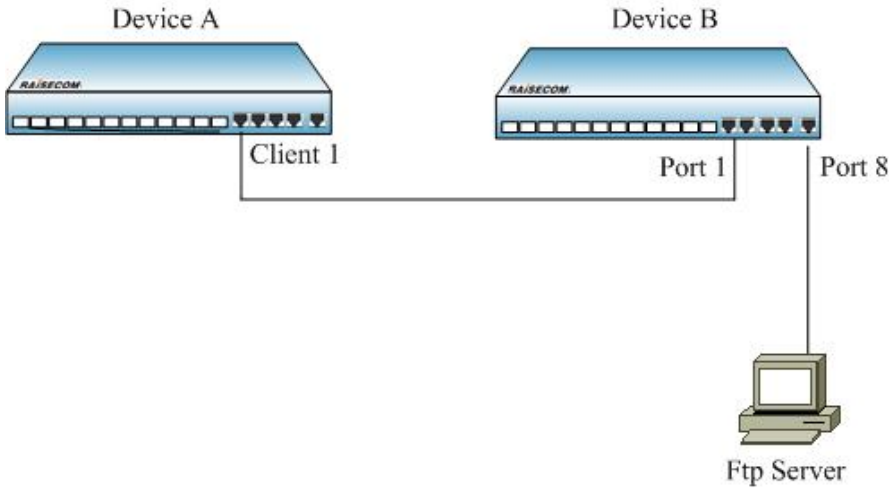


Fig 25-1 remote file upload/download function typical configuration

If you want to back-up and upgrade device A's startup configuration file on device B, configure B as the steps below:

1) upload startup configuration file to the server from remote device

Raisecom#**config**

Raisecom(config)# **interface line/client** *1*

Raisecom (config-port)# **remote-device**

Raisecom(config-remote)# **upload startup-config ftp** *12.0.0.1 raisecom raisecom configfile_version_1*

2) download startup configuration file to remote device from the server:

Raisecom(config-remote)# **download startup-config ftp** *12.0.0.1 raisecom raisecom*

configfile_version_2

Chapter 26 PING

26.1 Introduction of ping Function Principle

26.1.1 Ping function

This function can judge interoperability of the network, ping command will build a fixed format of the ICMP request packet, send request with type code 0 ICMP, the host that has received the request will reply with type 8 ICMP. Ping program calculate the time interval, and calculate how many packets have been delivered. Users can determine the network situation in general.

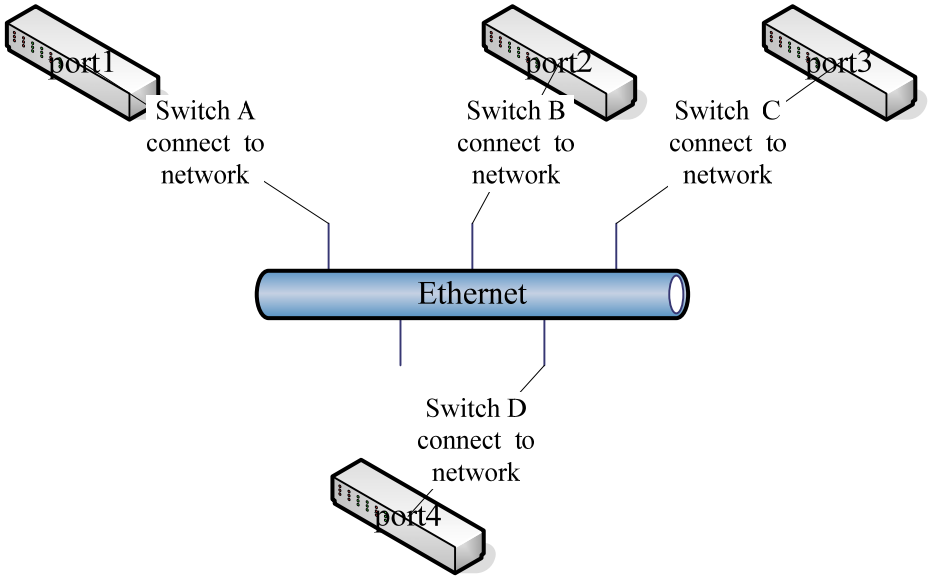


Figure 26-1 topology diagram of ping practical application

As shown in Figure 1, if the switch D want to ping certain ip address, then this switch not only can directly ping tests through the command line, switches A, B, or C can also telnet to the switch D on the implementation of the ping tests, so that the same device may have multiple users on the implementation of a ping test (including the network management users), the network can achieve to determine the purpose of interoperability. However, in D, the implementation of the ping tests can only have up to 10 users simultaneously.

26.1.2 Ping configuration

Packet size, number and time-out of ping test, is optional, the default values are: 0 (does not contain icmp header), 1 and 3 (unit: s), ip address is a necessary option, and can only be A, B or C class address.

26.1.3 Cli user configuration ping

Step	Command	Description
1	**Raisecom#**	Enter privileged user mode

2	**Raisecom#ping A.B.C.D [count** *<1-165535>***] [size** *<0-4096>***] [waittime** *<1-60>***]**	Configure ping test A.B.C.D: is the IP address to PING; Count: packets sent number, the default is 1, range in 1-65535; Size: bytes of packets sent,(does not include icmp header) default 0, range in 0-4096; Waittime: timeout for the ping packet, the default is 3s, range in 1-60s

26.1.4 Telnet user configuration ping

Step	Command	Description
1	**Raisecom#**	Enter privileged user mode
2	**Raisecom#telnet X.X.X.X**	Telnet to certain switch, ip address of the switch is X.X.X.X
3	**Raisecom#ping A.B.C.D [count** *<1-165535>***] [size** *<0-4096>***] [waittime** *<1-60>***]**	Configure ping test A.B.C.D: is the IP address to PING; Count: packets sent number, the default is 1, range in 1-65535; Size: bytes of packets sent,(does not include icmp header) default 0, range in 0-4096; Waittime: timeout for the ping packet, the default is 3s, range in 1-60s

26.1.5 Examples of typical configuration

Purpose:

Start ping test, size of a ping is 20 bytes, time-out time is 5s, packets numbers is 13, destinated ip is 20.0.0.2.

Configuration steps:

Raisecom#**ping** *20.0.0.2* **count** *13* **size** *20* **waittime** *5*

Showing results 1 are as follows:

Type CTRL+C to abort.

Sending 13, 28-byte ICMP Echos to 20.0.0.2 , timeout is 5 seconds:

!!!!!!!!!!!!

---- PING Statistics----

13 packets transmitted,

13 packets received, Success rate is 100 percent(13/13)

round-trip (ms) min/avg/max = 0/16/16

Showing results 2 are as follows:

Type CTRL+C to abort.

Sending 13, 28-byte ICMP Echos to 20.0.0.2 , timeout is 5 seconds:

UUUUUUUUUUUU

no answer from 20.0.0.2

Attention: The when 20.0.0.2 above is able to pass ping, it will print according to showing results 1;

when 20.0.0.2 ping in invalid, it will print according to showing results 2.

Note:

- In execution of the ping command, user can no longer have any other input to the command line until the end of the command line or through the ctl + c keys.
- Ping remote switch from local switch, six telnet user at most are allowed to log on to local switch and can execute ping without interfere with each other simultaneously
- Implementation number of the ping by Snmp, cli, and telnet user is at most 10, more than 10 users will be not available in implementation of the ping, prompts an error.

Chapter 27 Auto-configuration and Load

27.1 Auto-configuration and load principle

Auto-configuration and load use TFTP protocol to acquire the configuration file stored on TFTP server, it is a way to configure the equipment. Viewing from application, it can be sorted to auto-run when the systems starts and running when the system is running.

Updated auto-configuration and load function allows the configuration files on TFTP server contain the commands related with auto-configuration and load function, so that there can be multi-configuration and load, to supply with the need of auto-configuration and load in complex network environment.

The switch supports several ways to make sure the configuration name on TFTP server correct, like manual input, using DHCP-Client for acquisition, using default configuration file name. Except this, user can specify one configuration file naming convention, using the attribute of the equipment to make sure the corresponding configuration file name by rules.

By combining multi-configuration and load technology and several accesses of acquiring configuration file name, the equipment can do auto-loading without configuration.

27.2 Default auto-configuration and load configuration

Function	Default
TFTP server address	0.0.0.0 (not available)
The configuration files name on the server	Startup_config.conf
The naming rules of configuration files on the server	No rule number
Cover local configuration file switch state	Disable
On-power auto-configuration and load switch state	Disable
Send completing Trap switch state	Disable
Auto configuration and load running state	DONE
Auto configuration and load running result	NONE

27.3 Auto configuration and load function configuration

27.3.1 Configure TFTP server address

By default, TFTP server address is 0.0.0.0, 0.0.0.0 can not be configured by the command. Run the opposite command **no service config tftp-server** and TFTP server address will be 0.0.0.0, but 0.0.0.0 can not be take as a available address to download configuration files and load it, and it shows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service config tftp-server** *A.B.C.D*	Configure TFTP server address
3	**exit**	Quit global configuration mode and enter privileged EXEC mode
4	**show service config**	Show auto-configuration and load information, **Config server IP address** shows the configuration information of TFTP server address

To restore default address, use **no service config tftp-server**.

Notice:

- The configure IP address must accord with RFC1166, or it may cause configuration failure.
- After using the command to configure TFTP server address, when you run auto-configuration and load, the address that is configured by the command will be used, not the address acquired from DHCP Client. So, if you don't want to use local configured address, you don't have to configure it; if it has been configured, use **no service config tftp-server** to restore and run auto-configuration and load function.

27.3.2 Configure file name rule

By default, there is no filename naming rule, use **show service config** and it will show: --. When naming rule and filename are not configured, while no configuration filename is acquired successfully from DHCP Client function, the system will use default filename: **startup_config.conf**.

The configured file naming rule has the highest priority. When configured naming rule, you should use the naming rule to make sure the filename according to the equipment attribute.

Step	Command	Description
1	config	Enter global configuration mode
2	**service config filename rule** *[<80001-89999>]*	Configure file naming rules
3	**exit**	Quit from global configuration mode and enter privileged EXEC mode
4	**show service config**	Show auto-configuration and load information, among them, **Config filename rule** shows the filename configuration information

Use command **no service config filename rule** to delete the configured filename naming rules.

If there be no input rule number, then the system will create rule number in the way of question according to the answer user offers.

Raisecom(config)#**service config filename rule**

Enter the first question

Please check device type rule, configuration filename

0 - includes no device type information

1 - includes device type information

Please select:

0 means that the configuration files do not contain equipment type;

1 means that the configuration files do not contain switch type.

Input 0 or 1, press Enter, and enter the second question:

Notice: If the input number is not 0/1, it will be returned fault and failure in rule creation.

Please check MAC address rule, configuration filename

0 - includes no MAC address information

1 - includes the first 2 characters in MAC address

2 - includes the first 4 characters in MAC address

3 - includes the first 6 characters in MAC address

4 - includes the first 8 characters in MAC address

5 - includes the first 10 characters in MAC address

6 - includes all characters in MAC address

Please select:

0 means that ROS software version information is not contained in the configuration filename;

1 means that complete ROS software version information is contained in the configuration filename;

2 means that the software version information except the equipment type is contained in the configuration filename;

3 means that the software version information except the equipment type and date is contained in the configuration filename;

4 means that the software version high 3 figures are contained in the configuration filename;

5 means that the software version high 2 figures are contained in the configuration filename;

6 means that the software version the highest figure is contained in the configuration filename.

Input a random number among 0 and 6, press Enter, and end up rule number configuration.

Notice: If you input any number that is not among 0 and 6, it will return fault and failure in rule creation.

Please check MAC address rule, configuration filename

0 - includes no MAC address information

1 - includes the first 2 characters in MAC address

2 - includes the first 4 characters in MAC address

3 - includes the first 6 characters in MAC address

4 - includes the first 8 characters in MAC address

5 - includes the first 10 characters in MAC address

6 - includes all characters in MAC address

Please select:

Notice: If the input number belongs not to 0-6, it will be returned fault and failure in rule creation.

Please check ROS version rule, configuration filename

0 - includes no ROS version information

1 - includes entire ROS version information

2 - includes all except device type

3 - includes all except device type and date

4 - includes the highest 3 version number

5 - includes the highest 2 version number

6 - includes the highest version number

Please select:

Notice: If the input number belongs not to 0-6, it will be returned fault and failure in rule creation.

The configuration file naming rules are as follows:

The rule number is made up of 5 numbers, myriabit is 8, which has no actual meaning.

1) Kilobit shows the equipment type rules:

0 – equipment type is not included in the configuration file name;

1 – equipment type is included in the configuration file name;

2 – 9, reserved number, for rules extension.

2) Hundred shows MAC address rules: (take 000E08.5118 for example)

0 – the equipment MAC address information is not included in the configuration file name

1 – the first 2 characters of the equipment MAC address is included in the configuration file name (that is 00)

2 - the first 4 characters of the equipment MAC address is included in the configuration file name (000E)

3 - the first 6 characters of the equipment MAC address is included in the configuration file name (000E.5E)

4 - the first 8 characters of the equipment MAC address is included in the configuration file name (000E.5E08)

5 - the first 10 characters of the equipment MAC address is included in the configuration file name (000E.5E08.51)

6 - the first 6 characters of the equipment MAC address is included in the configuration file name (000E.5E.5E08.5118)

7 – 9 reserved number, for extension.

3) Tens show the software version number rule: (take ROS_4.3.2 ISCOM

2926.1.20080602)

0 – no software version information is contained;

1 – complete version information is contained (ROS_4.3.2 ISCOM 2926.1.20080602)

2 – the software version information without equipment type is contained (ROS_4.3.2.1.20080602)

3 – the software version information without equipment type and data is contained in the software version information (ROS_4.3.2.1)

4 – the software version information contains the higher three-figure (ROS_4.3.2)

5 – the software version information contains the higher two-figure (ROS_4.3)

6 – the software version information contains the higher one-figure (ROS_4)

7 – 9 restored, for extension.

4) Units digit shows the extension rules:

0 – extension rule is not supported;

1 – 9 restored, for extension.

The configuration file name is of the following style:

(equipment type)_M(MSC address)_(software version number)

For example: rule number 81650 stands for the configuration file name:

ISCOM2926_M000E.5E08.5118_ROS_4

Notice: After using the command to configure the naming rules, when auto-configuration is loaded, the naming rule will be used to configure the filename, while manual configuration filename and the one acquired from DHCP Client will no be used. So, if you do not want to use the naming rules, you don't have to configure the naming rules, and if it had been configured, use **no service config filename rule** to restore to default cases.

27.3.3 Configure the filename

By default, the filename is empty, use **show service config** and you will see: --. Follow the steps below to configure the filename, the length can not be longer than 80 bytes.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service config filename** *FILENAME*	Configure the filename. FILENAME: the filename, shorter than 80 bytes
3	**exit**	Quit from global configuration mode and enter privileged EXEC mode
4	**show service config**	Show auto-configuration loading information; **config file name** shows the configuration information of the filename.

Use **no service config filename** to delete the configured configuration filename.

Notice:

- If the configuration filename rule had been configured, then the configuration filename using this command will not be used.
- Under the promise that no naming rule is configured, if the command is used to configure the filename, then when auto-configuration is loaded, the filename configured by this command will be used, while the filename acquired from DHCP Client will not be used.
- If you want to use the filename acquired from DHCP Client or default filename, there is no need to configure the filename. And if it had been configured, use **no service config filename** to resume and run auto-configuration loading function.

27.3.4 Configure the switch of covering local configuration

Enable/disable covering local configuration file switch function. If it is enabled, use the file on the server to cover local configuration file in the process of auto-configuration loading.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service config overwrite** {*enable* | *disable*}	Configure the switch of overwriting local configuration file
3	**exit**	Return to global configuration mode and enter privileged EXEC mode
4	**show service config**	Show auto-configuration loading information, **config file name** show the configuration information of the filename

27.3.5 Run auto-configuration loading when the equipment is working

Use manual configuration to run auto-configuration loading, the configuration access is shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service config**	Run auto-configuration loading function
3	**show service config**	Show the running state and result of auto-configuration loading, **operation states** shows the state of auto-configuration loading, **result** shows the result of auto-configuration loading

Notice: When the command is running, the switch of sending Trap when configuration is loaded successfully will be closed automatically.

27.3.6 Running auto-configuration loading automatically when the equipment is started

There are two situations when running auto-configuration loading automatically when the equipment is started:

1) The local configuration file of the equipment does not exist, then auto-configuration loading will be

carried out automatically when the equipment is started

2) The local configuration file of the equipment exists, and **service config** exists in local configuration file, then auto-configuration loading will be started when local configuration file is loaded

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service config startup enable**	Enable auto-configuration loading when powered
3	**write**	Write the configuration into local configuration file
4	**exit**	Quit from global configuration mode and enter privileged EXEC moe
5	**reboot now**	Restart the switch

27.3.7 Stop auto-configuration loading try

If auto-configuration loading failed the switch will run auto-configuration loading once in a certain interval. The first failure interval is 2 seconds, the second time it is 10 seconds, the third time it is 100 seconds, the fourth time it is 300 seconds.

Use **no service config** to stop auto-configuration loading try caused by auto-configuration loading failure.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**no service config**	Stop auto-configuration loading try caused by loading failure
3	**exit**	Quit from global configuration mode and enter privileged EXEC mode

27.4 Monitoring and maintenance

Use **show service config** to show auto-configuration loading information and the running situation.

The information shown is as follows:

Perform on startup: disable

Config server IP address: --

Config file name rule: 81000

Config file name: --

Overwrite local configuration file: disable

Send Completion trap: disable

Operation states: done

Result: none

Use the command below to show the meaning of the configuration filename rule:

Command	Description
show service config filename rule [*ruleNum*]	Describe the meaning of filename rule, and provide the optical auto-configuration loading command rule number.

27.5 Typical configuration example

27.5.1 Destination

When the switch is started, by running auto-configuration loading twice, the switch can go through VLAN and get the specific configuration file.

27.5.2 The topology structure

The topology structure is shown below:

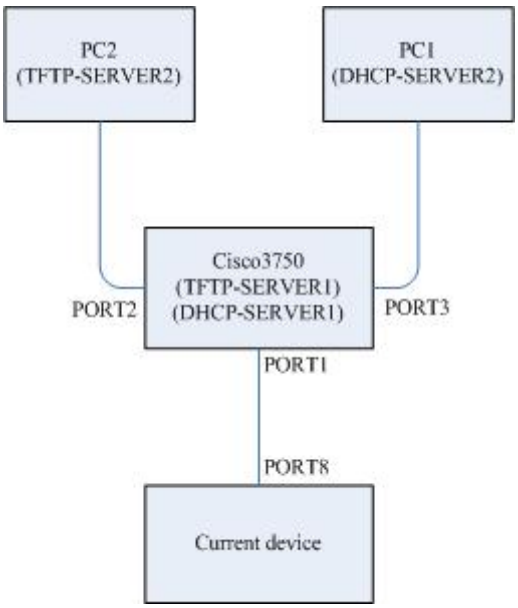


Fig 27-1 topology structure

27.5.3 The configuration steps on Cisco 3750

Step 1: configure IP address on VLAN port 100:

Switch#**config**

Switch(config)#**interface vlan** *100*

Switch(config-if)#**ip address** *20.100.0.100 255.255.255.0*

Switch(config-if)#**no shutdown**

Switch(config-vlan)#**exit**

Step 2: configure TFTP-SERVER1

Switch(config)#**tftp-server** *flash*:*startup_config.conf*

Step 3: configure DHCP-SERVER1 on VLAN 100:

Switch(config)#**ip dhcp pool** *newpool*

Switch(dhcp-config)#**network** *20.100.0.100 255.255.255.0*

Switch(dhcp-config)#**option** *150* **ip** *20.100.0.100*

Switch(dhcp-config)#**exit**

Step 4: configure port 2 to access mode and enter VLAN 200

Switch(config)#interface *G 1/0/2*

Switch(config-if)#**switch mode access**

Switch(config-if)#**switch access vlan** *200*

Switch(config-if)#**exit**

Step 5: configure port 3 to access mode and enter VLAN 200

Switch(config)#interface *G 1/0/3*

Switch(config-if)#**switch mode access**

Switch(config-if)#**switch access vlan** *200*

Switch(config-if)#**exit**

Step 6: configure port 1 to Trunk mode and native VLAN to 100

Switch(config)#interface *G 1/0/1*

Switch(config-if)#switch trunk encapsulation *dot1q*

Switch(config-if)#switch mode trunk

Switch(config-if)#switch trunk native vlan *100*

The content of the configuration file **startup_config.conf** that is added to TFTP-SERVER1:

!ROS Version 3.7.1043.ISCOM2009.84.20080602

!command in view_mode

!

!command in config_mode first-step

create vlan 200 active

!

!command in enable_mode

!

!command in ip igmp profile mode

!

!command in port_mode

Interface port 8

Switch mode trunk

!

!command in vlan configuration mode

!

!command in ip interface mode

interface ip 0

ip address dhcp 200

!

!command in cluster_mode

!

Chapter 28 CFM Configuration

This chapter describes switch CFM configuration and the contents are shown as below:

- ✧ CFM introduction
- ✧ CFM default configuration list
- ✧ CFM configuration guide and limitation
- ✧ CFM configuration list and specifications
- ✧ CFM monitoring and maintenance
- ✧ CFM basic configuration examples

28.1 CFM Introduction

Since it grows rapidly, Ethernet technology has been used widely in MAN (metropolitan area network) and WAN (wide area network). Because of the complex network structure and a huge number of various users in WAN and MAN, many operators co-operate their network together to provide end-to-end service. Thus, there will be more strict requirements for the Ethernet's management, maintenance and its reliability. To provide as same quality service as traditional telecommunication transmission network does, many organizations and research groups are working on the technology development and standard modification.

IEEE and ITU-T have established CFM (Connectivity Fault Management) protocol (802.1ag), which can provide end-to-end OAM service ability. CFM is able to detect the end-to-end continuous fault in a very short time; it also can provide the fault confirmation and fault isolation function if needed. All those can provide a more complete OAM function for the Ethernet network.

CFM (Connectivity Fault Management) protocol is a layer 2 Ethernet OAM protocol. CFM works as the active fault diagnoses for point-to-point or multi-points to multi-points EVC(Ethernet Virtual Connection); it is based on end-to-end OAM protocol(service level); we can use CFM protocol to cut down the network maintenance cost effectively; it is used in Ethernet access network, convergence network and core network; it can be used in all Ethernet devices.

28.1.1 CFM Modules

1. MD

MD (Maintenance Domain) is a network which is used to manage CFM; it states range of CFM check. MD has level attribute which has 8 levels in total (0-7). The bigger level number, the higher MD level and the bigger the MD range. In one VLAN, different MDs can be nearby or nesting but not cross.

2. MA

One MA is corresponding one service instance and S-VLAN. One MA can configure many MEPs. MEPs from same MA have same VLAN TAG in their sending messages. Also, a MEP can receive sending CFM messages from other MEPs in the same MA.

3. MIP

MIP is a managing activity entity which is formed by two MHF (MIP Half Function). MIP can not send CFM messages actively, but can process and reply CFM messages.

4. MEP

MEP is configured at MD edge and a managing activity entity related to service instance. One MEP is related to one service instance. MEP can send and process CFM messages, MD and MA (MEP belonged) confirm MEP sending messages level and VLAN. MEPs stop and process the receiving messages which are same or lower level than their MEP level; MEPs relay directly those levels higher than them. MEP and MIP are called MP.

28.1.2 CFM Basic Function

CFM function is based on right configurations of MD, MA, MEP and MIP. CFM mainly have three functions:

Continuity Check, CC

Loop back, LB

Link trace, LT

28.1.2.1 Fault Continuity Check

Fault check function is using CC (Continuity Check) protocol to check a Ethernet Virtual Connection (EVC)'s connectivity and also confirm connections between MPs. The Function is achieved by MEP periodically sending CCM (Continuity Check Message) multi-cast message. Other MEPs from same MA receive that message thus to check the remote MEP status. If device fault or link configured error, then MEP can not send CCM messages to remote MEP and can not receive remote CCM message as well. If MEP does not receive remote CCM message in 3.5 times of CCM interval period, then it will state the link fault occurring and send fault alarm information to the administrator according to the alarm and priority configuration. When multiple MEPs of multiple MAs from the same MD send CCM messages that can be multi-points to multi-points link check.

28.1.2.2 Fault Confirm

Faults confirm function is used to check the connectivity between local devices and remote devices. The function can send LBM (Loop back Message) through MEP to the MPs which needs fault confirm. When that MP receives LBM message, it sends a LBR reply message to source MEP, shows route is connected. If source MEP does not receive LBR message, then the link has fault. Faults confirm function is similar to layer 2 ping functions. Both sending LBM and receiving LTR are uni-cast message. LBM and LTR receiving are used to confirm the link status between to MPs.

28.1.2.3 Fault Isolation

Fault isolation function is used to confirm the route between source MEP and destination MP. The function is achieved by source MEP sending LTM (Linktrace Message) to MP which can confirm route; bridge device from each configured MP on that route sends LTR reply message to source MEP. Information can

be reformed by recording effective LTR and LTM. Lastly the route between MP is confirmed. LTM is multi-cast message and LTR is uni-cast message.

By the three functions above, CFM protocol can achieve end to end OAM technology, reduces service providers' operation and maintenance cost. So in a certain way, it increases the service providers' competitive advantage

28.2 CFM Default Configuration List

Number	Attribute	Default Value
1	CFM protocol enable and disable in CONFIG mode	CFM protocol disable
2	Port CFM protocol status	All ports CFM enable
3	CCM messages send status	Not sending CCM messages
4	CCM messages sending time intervals	10 seconds
5	The time which CC data base save wrong CCM	100 minutes
6	Linktrace Database enable/ disable	Disable
7	Linktrace Database saving data time	100 minutes
8	Linktrace Database saved data Enter number	When Linktrace Database is enable, data entries can be saved as 100; as it is disable, data entries can be saved as 0.
9	Network bug alarm	When it is set as macRemErrXcon is set, it supports four bug alarms: Macstatus,RemoteCCM,ErrorCCM and XconCCM.

28.3 CFM Configuration Guide and Limitation

1. MEP is based on MD and MA. MD has 8 levels (0-7). MA has 4094 VLANs to be configured. for the switch function, each switch can be set in 128 service instances and 128 MEP. MEPID is in the range of 1-8191.

2. Configure CCM messages sending interval, protocol can be configured as 10/3 ms, 10ms, 100ms, 1s, 10s, 1m and 10m. For the switch stable performance, our support range is among 1s, 10s, 1m and 10m. Once each MEP receives CCM messages, it will record the efficient CCM in MEP CCM Database. Each MEP maintaining CCM Database can save 32 information bars.

3. To state maintenance domain (MD), the domain name's character string length is 1-16 byte, maintaining level are level 0-7.

4. As configure customer service instance s, service instance ID's character string lengthis1-16 bytes. Vlan ID is in the range of 1-4094 and Vlan list is also in the range of 1-4094.

5. MEP CCM Database's wrong CCM messages archive time is in the range of 1-65535.

6. Configure Linktrace Database data archive time is in the range of 1-65535, saved data entries could be in 1-4095.

28.4 CFM Configuration List and Specification

A. Configure CFM domain

a) Configure CFM maintain MD

b) Configure CFM service illustration MA

c) Configure MIP

d) Configure MEP

B. Fault Check

a) Configure CC protocol enable/disable

b) Configure CCM messages sending interval

c) Configure Error CCM messages saving time

C. Launch Loopback protocol

D. Route trace

a) Launch Linktrace protocol

b) Configure Linktrace data enable/disable status

c) Configure Linktrace data saving time

d) Configure Linktrace Database saved data entries' number

E. Fault indication

F. Protocol enable/disable

28.4.1 Configure CFM Maintenance Domain -- MD

Before configure MD name, MD name must be the only name in the whole CFM managing network range; Different named MD can be configured in the same level, but two

MDs with same name could not be related to different levels.

Delete MD: **no ethernet cfm domain** *domain-name* **level** *level-id*

Steps	Command	Description
1	**config**	Enter configure mode
2	**ethernet cfm domain** *domain-name* **level** *level-id*	Configure CFM maintain domain, state MD name and level. *domain-name*: domain name character string in 1-16 bytes; *level-id*: maintain level 0-7
3	**Exit**	Return to Privileged EXEC mode.
4	**show ethernet cfm domain**	Display indicated maintain domain configure information

Example: Configure MD, name as md3-1, level as 3

Raisecom#**config**

raiecom(config)#**ethernet cfm domain md3-1 level 3**

raiecom(config-ether-cfm)#**exit**

raiecom(config)#**exit**

28.4.2 Configure Service Instance MA

To configure service illustration, we need to configure MD first and make sure this service illustration is the only one inside that MD; but in two different MD, we can configure the same name service illustration; in one MD, a VLAN can only be related to one service illustration. If configured MA name is same as the existed MA name, but the related VLAN is different, then that MA should be given a new related VLAN.

Delete service illustration: **no service** *csi-id* **vlan** *vlan-id.* Before delete service illustration, we need to delete its all MEP first.

Steps	Commands	Description
1	**config**	Enter GLOBAL configure mode
2	**ethernet cfm domain** *domain-name* **level** *level-id*	Configure CFM MD, states MD name and MD level. *domain-name*: domain name character string length 1-16 bytes; *level-id*: MD level 0-7
3	**service** *csi-id* **vlan** *vlan-id*	Configure service illustration name and related VLAN. *csi-id*: service illustration ID character string, length 1-16 bytes; *vlan-id*: VLAN ID 1-4094
4	**Exit**	Return to Privileged EXEC mode.
5	**show ethernet cfm domain**	Show indicated CFM domain configuration information

Example: In MD named md3-1, configure service illustration as ma3-1-4 and its related VLAN as 4.

Raisecom#**config**

raiecom(config)#**ethernet cfm domain md3-1 level 3**

Raisecom(config-ether-cfm)#**service ma3-1-4 vlan 4**

Raisecom(config-ether-cfm)#**exit**

Raisecom(config)#**exit**

28.4.3 Configure MIP

Before configure MIP, we must make sure that configure the switch with the same level MD, and there should not be any same or higher level MEP in the port. Same port can only be configured one MIP. If we configure two MIP, the new one will replace the old one. Before delete MIP, we should make there is no lower level MEP in the port.

Delete MIP: **no ethernet cfm mip level** *level-id*

Steps	Commands	Description

1	**config**	Enter GLOBAL configure mode
2	**interface port** *port-num*	Enter related port. *port-num*: port number
3	**ethernet cfm mip level** *level-id*	In indicated MD, configure MIP, same level as MD. *level-id*: *MD level*: 0-7
4	**Exit**	Return to GLOBAL configure mode
5	**Exit**	Return to Privileged EXEC mode.
6	**show cfm mp local**	Display local MP configuration information includes MEP and MIP.

Example: in port 3, configure MIP as level 5(we have configured MEP as level 5, MD configuration can be found in 1.4.1)

Raisecom#**config**

Raisecom(config)#**interface port** *5*

Raisecom(config-port)#**ethernet cfm mip level** *5*

28.4.4 Configure MEP

Before configuring MEP, we configure MEP located MD, MD's service illustration and a high level MIP. If MEP level is 7, we don't need to configure high level MIP. If there is an MIP configured in the port, then we can configure any same or higher level MEP on that port. So far, all supported configured MEP directions are UP, so if commands are not indicated, the default is UP.

Delete indicated MEP: **no ethernet cfm mep level** *level-id* **[up] mpid** *mep-id* **vlan** {*all*|*vlanlist*}

Steps	Commands	Description
1	**Config**	Enter GLOBAL configure mode
2	**interface port** *port-num*	Enter related port *port-num*: port number
3	**ethernet cfm mep level** *level-id* [**up**] **mpid** *mep-id* **vlan** {**all**|*vlanlist}*	In related MD, configure MEP. *level-id*: MD level: 0-7 *mep-id*: 1-8191; *vlanlist*: Vlan list 1-4094
4	**Exit**	Return to Privileged EXEC mode.
5	**show ethernet cfm domain**	Display indicated MD configuration information

Example:

√ **Configure the MEP which is not level 7:** First configure high level (level is 5) MD; in that MD we configure a level 3 MD and related service illustration; finally, we configure its related MEP.

Raisecom#**config**

Configure high level MD: Raisecom(config)#**ethernet cfm domain md5 level** *5*

Raisecom(config-ether-cfm)#**exit**

Configure indicated level MD: Raisecom(config)#**ethernet cfm domain md3 level** *3*

Configure related service illustration: Raisecom(config-ether-cfm)#**service ma4 vlan** *4*

Raisecom(config-ether-cfm)#**exit**

Enter port mode: Raisecom(config)#**interface port** *1*

Under high level, configure MIP: Raisecom(config-port)#**ethernet cfm mip level** *5*

Configure MEP: Raisecom(config-port)#**ethernet cfm mep level** *3* **up mpid** *1* **vlan** *4*

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

Raisecom(config)#**exit**

√ Configure MEP which is level7: Firstly, configure a level 7 MD and its related service instance; then configure MEP.

Raisecom#**config**

Configure level 7 MD: Raisecom(config)#**ethernet cfm domain** *md7* **level** *7*

Configure related service instance: Raisecom(config-ether-cfm)#**service** *ma7-1-4* **vlan** *4*

Raisecom(config-ether-cfm)#**exit**

Enter port mode: Raisecom(config)#**interface port** *1*

Configure MEP: Raisecom(config-port)#**ethernet cfm mep level** *7* **up mpid** *1* **vlan** *4*

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

Raisecom(config)#**exit**

28.4.5 Configure CC Protocol Enable/Disable

Launch the indicate service instance CC protocol, thus MEP from the instances can send CCM messages. When CC protocol is disable, MEP stops sending CCM messages.

As configure that command, we should make sure that the switch is configured same level MD and each VLAN from VLAN list is found a related MA from the same level MD. In default, the CC protocol is set as disable.

Steps	Commands	Description
1	**config**	Enter to configure mode
2	**ethernet cfm cc {enable|disable} level {all|***levellist***} vlan {all|***vlanlist***}**	Enable/disable cc protocol. *All:* all configure levels; *Levellist:* maintenance domain level list; *all:* all configured VLAN; *vlanlist:* VLAN range 1-4094
3	**Exit**	Return to Privileged EXEC mode.
4	**show ethernet cfm domain**	Display indicated maintenance domain configure information

Example: configure the named as md3-1, level-3 MD; inside the MD configure the named ma3-1-4 MA and its related VLAN 4, enable cc protocol.

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain** *md3-1* **level** *3*

Raisecom(config-ether-cfm)#**service** *ma3-1-4* **vlan** *4*

Raisecom(config-ether-cfm)#**exit**

Raisecom(config)#**ethernet cfm cc enable level** *3* **vlan** *4*

Raisecom(config)#**exit**

28.4.6 Configure CCM Message Sending Interval

Before configure this command, we should make sure the switch is configured same MD level and each VLAN in the VLAN list has a related MA within the same MD level.

In default situation, MEP CCM messages sending interval is 10 seconds.

In recover indicated service example, we configure the CCM messages sending interval as default value: **no ethernet cfm cc level** *levelid* **vlan** ***{****all* **|** *vlanlist****}*** **interval**

Steps	Commands	Description
1	**config**	Enter GLOBAL configure mode
2	**ethernet cfm cc level** ***{all*** **|** *levellist****}*** **vlan** ***{ all*** **|** *vlanlist****}*** **interval** *{1| 10	60	600}*	Set CCM messages sending interval, can configure ALL/some indicated level from all service level list/some indicated service instance or indicated level in indicated service with instance CCM messages sending interval. *Levellist*: maintenance domain level list 0-7
3	**Exit**	Return to Privileged EXEC mode.
4	**show ethernet cfm domain**	Display local configuration MD related information

Example: Set sending interval as 60 seconds, configure related MD and service example, and see reference as **1.4.2** service instance configuration.

Raisecom#**config**

Raisecom(config)#**ethernet cfm cc level** *3* **vlan** *4* **interval** *60*

Raisecom(config)#**exit**

28.4.7 Configure CCM Message Error Archive Time in MEP CCM Database

Each CCM error has its created time and we use the commands to save the CCM information created time. Unless error data archive time is reset, the error list archive time does not change. Only if it is reset, then the new error list will use the new archive time. Before configure the CCM messages archive time, we should configure the related MEP. In default situation, CC database can archives CCM error for 100 minutes.

Recover data error archive time in MEP CCM Database: **no ethernet cfm mep archive-hold-time**

Steps	Commands	Description
1	**config**	Enter GLOBAL configure mode
2	**ethernet cfm mep archive-hold-time** *minutes*	Configure CCM messages error archive time. *Minutes*: archive time (minutes) range 1-65535
3	**Exit**	Return to Privileged EXEC mode.

4	**show ethernet cfm**	Display CFM related information

Examples: set CCM messages error archive time as 50, firstly configure related MEP, see reference as 1.4.4 MEP configure Commands!

Raisecom#**config**

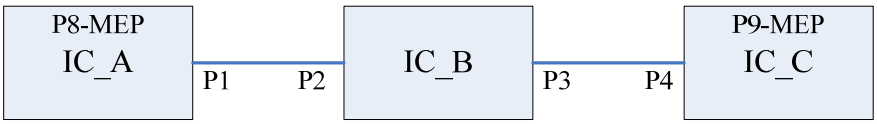
Raisecom(config)#**ethernet cfm mep archive-hold-time** *50*

Raisecom(config)#**exit**

28.4.8 Launch Loopback Protocol

Before uses the commands, the switch must be configured same level, same VLAN MEP. When there is only one related MEP, we don't need to add the key word ***source*** *mpid* in commands; if switch has more than one same level same VLAN MEPs, we must indicate the MEPIP of the source MEP – as add the key word ***source*** *mpid* in the commands.

Steps	Commands	Description
1	**config**	Enter GLOBAL configure mode
2	**ping ethernet** *{mac-address* | **mep** *mep-id}{***domain** *domain-name* | **level** *level-id}* **vlan** *vlan-id* [**source** *mpid]*	Launch Loopback protocol, achieve fault confirm function. *mac-address*: remote MP MAC address, format is HHHH.HHHH.HHH, *mep-id*: remote MEP ID number(1-8191) . *level-id*: maintenance *domain level*: 0-7 *vlan-id*: VLAN ID1-4094 *domain-name*: domain name string length 1-16 bytes; *Mpid*: MEPID
3	**Exit**	Return GLOBAL configure mode



Examples: as topology graph shows above, configure IC_A port 8 and IC_C port 9 with MEPs that have same MD, same MA, and then launch Loopback Commands on IC_A, ping IC_C success. NOTE: set IC_A MAC address as AAAA, IC_B MAC address as BBBB, IC_C MAC address as CCCC. Details showed as below:

1. on IC_A, enable CFM protocol: IC_A(config)#**ethernet cfm enable**

2. on IC_A port 8, configure MEP, MEP ID as 1:

IC_A(config)#**ethernet cfm domain md5-1 level 5**

IC_A(config-ether-cfm)#**exit**

IC_A(config)#**ethernet cfm domain md3-1 level 3**

IC_A(config-ether-cfm)#**service ma3-1-4 vlan 4**

IC_A(config-ether-cfm)#**exit**

IC_A(config)#**interface port 8**

IC_A(config)#**switchport mode trunk**

IC_A(config-port)#**ethernet cfm mip level 5**

IC_A(config-port)#**ethernet cfm mep level 3 up mpid 1 vlan 4**

3. on IC_A, enable CC protocol: IC_A(config)#**ethernet cfm cc enable level 3 vlan 4**

4. on IC_A port1, configure mode: IC_A(config-port)#**switchport access vlan 4**

5. on IC_B, enable CFM protocol: IC_B(config)#**ethernet cfm enable**

6. on IC_B port 2 and 3, configure MIP:

IC_B(config)#**ethernet cfm domain md3-1 level 3**

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

IC_B (config-port)#**ethernet cfm mip level 3**

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

IC_B (config)#**interface port 3**

IC_B (config-port)#**ethernet cfm mip level 3**

7. on IC_B port 2, 3 configure mode: IC_B(config-port)#**switchport access vlan 4**

8. on IC_C, enable CFM protocol: IC_C(config)#**ethernet cfm enable**

9. on IC_C enable CC protocol: IC_C(config)#**ethernet cfm cc enable**

10. on IC_C port 9, configure MEP, MEP ID as 2:

IC_C(config)#**ethernet cfm domain md5-1 level 5**

IC_C(config-ether-cfm)#**exit**

IC_C(config)#**ethernet cfm domain md3-1 level 3**

IC_C(config-ether-cfm)#**service ma3-1-4 vlan 4**

IC_C(config-ether-cfm)#**exit**

IC_C(config)#**interface port 9**

IC_C(config-port)#**ethernet cfm mip level 5**

IC_C(config-port)#**ethernet cfm mep level 3 up mpid 2 vlan 4**

IC_C(config-port)#**switchport mode trunk**

11. on IC_C port10, configure MEP, MEP ID as 3:

IC_C(config)#**interface port 10**

IC_C(config-port)#**ethernet cfm mip level 5**

IC_C(config-port)#**ethernet cfm mep level 3 up mpid 3 vlan 4**

12. on C_C port4, configure mode: IC_C(config-port)#**switchport access vlan 4**

13. On IC_A, launch to ping IC_C: IC_A#**ping ethernet CCCC level 3 vlan 4**

Display results:

Sending 5 Ethernet CFM loopback messages to CCCC, timeout is 5 seconds:

!!!!!

Success rate is 100 percent (5/5).

Ping statistics from AAAA:

Received loopback replys: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

28.4.9 Launch Linktrace Protocol

Before uses the commands, the switch must be configured same level, same vlan MEP. When there is only one related MEP, we don't need to add the key word ***source*** *mpid* in commands; If switch has more than one same level same vlan MEPs, we must indicate the MEPIP of the source MEP – as add the key word ***source*** *mpid* in the commands.

Steps	Commands	Description
1	**config**	Enter GLOBAL configure mode
2	**traceroute ethernet** *mac-address* {**domain** *domain-name* | **level** *level-id*} **vlan** *vlan-id* [**source** *mpid*]	Launch Linktrace protocols configure. *mac-address*: Remote MP's MAC address, format as HHHH.HHHH.HHH; *domain-name* : domain name character string 1-16 bytes; *level-id*: maintenance domain *level*: 0-7 *vlan-id*: VLAN ID 1-4094 MEP ; *Mpid*: MEPID

Examples: Topology structure and configurations are same as last section; launch Traceroute Commands in two MEPs which have same MD and MA.

1. On IC_A, launch traceroute Commands: IC_A#**traceroute ethernet CCCC level 3 vlan 4**

Display Results:

Before get to final end node, same level MIP on egress port transmits LTM messages and replies LTR:

TTL: <64>

Tracing the route to CCCC on domain <md3-1>, level <3>, VLAN <4>.

Traceroute send via port <port-id>.

Hops HostMAC Ingress/EgressPort IsForwarded RelayAction NextHop

---

<1> <AAAA> <8/1> <yes> <RlyFDB> <AAAA>

<2> <AAAA> <2/3> <yes> <RlyFDB> <BBBB>

!<3> <BBBB> <-/9> <no> <RlyHit> <CCCC>

28.4.10 Configure Linktrace Database Enable/Disable Status

When LinkTrace database is enable status, LinkTrace data protocol link trace information is saved in

LinkTrace database and can use command: **show ethernet cfm traceroute-cache** to view them; when LinkTrace database is disable status, then we can not use that command: **Show ethernet cfm traceroute-cache** to check the route trace information. The default configuration is disable status.

Steps	Commands	Description
1	**config**	Enter GLOBAL configure mode
2	**ethernet cfm traceroute cache** *{ enable | disable }*	Configure database Enable/Disable status. *traceroute*: trace LTM messages sending route;
3	**exit**	Return to GLOBAL configure mode
4	**show ethernet cfm traceroute-cache**	Display trace route information

Example: Enable database and check the data information

Raisecom#**config**

Raisecom(config)#**ethernet cfm traceroute cache** *enable*

Raisecom(config)#**exit**

Raisecom#**show ethernet cfm traceroute-cache**

28.4.11 Configure Linktrace Database Archive Time

Only if LinkTrace database is enable, we can configure the data archive time. Default archive time is 100 minutes. To recovers database default data archive time, we use command: **no ethernet cfm traceroute cache hold-time**

Steps	Commands	Description
1	**config**	Enter GLOBAL configure mode
2	**ethernet cfm traceroute cache enable**	Enable LinkTrace database
3	**ethernet cfm traceroute cache hold-time** *minutes*	Configure Linktrace database data archive time *Minutes*: database archive time, unit is minute, value *range* of 1-65535
4	**Exit**	Return GLOBAL configure mode
5	**show ethernet cfm traceroute-cache**	Check data information

Examples: Enable database and set configure archive time 1000

Raisecom#**config**

Raisecom(config)#**ethernet cfm traceroute cache** *enable*

Raisecom(config)#**ethernet cfm traceroute cache hold-time** *1000*

Raisecom(config)#**exit**

Raisecom(config)#**show ethernet cfm traceroute-cache**

28.4.12 Configure Linktrace Database Data Entries

Only if LinkTrace database is enable, we can configure the size of data entries. When LinkTrace database is

enable, default entries number is 100; when LinkTrace database is disable, default data entries number is 0. To recover Linktrace database entries number default value, we use command: **no ethernet cfm traceroute cache size**

Steps	Commands	Description
1	**config**	Enter GLOBAL configure mode
2	**ethernet cfm traceroute cache enable**	Enable LinkTrace database
3	**ethernet cfm traceroute cache size** *entries*	Configure data entries number. *Entries*: Database data entry number *range* of 1-4095
4	**Exit**	Return to GLOBAL configure mode
5	**show ethernet cfm traceroute-cache**	Check data information

Example: Enable database; configure data entries number as 150.

Raisecom#**config**

Raisecom(config)#**ethernet cfm traceroute cache** *enable*

Raisecom(config)#**ethernet cfm traceroute cache size** *150*

Raisecom(config)#**exit**

28.4.13 Fault Indication

To configure the five network trouble alarms, we need to configure them by their priorities. After configure some priority alarm, the network trouble alarms which are equal or higher than this alarm are enable. Different alarm switches are configured to send all types of alarms (5 alarms): macRemErrXcon sends Macstatus, RemoteCCM,ErrorCCM and XconCCM alarms, which are also called sending alarm type 1-4; remErrXcon sends RemoteCCM,ErrorCCM and XconCCM alarms, which can be called alarm type 1-3; errXcon sends ErrorCCM and XconCCM alarms, which also can be called alarm type 1-2; Xcon sends XconCCM alarm – alarm type 1; None, do not send any alarm. Default status is macRemErrXcon, which are sendMacstatus, RemoteCCM,ErrorCCM and XconCCM four alarms. To recover sending alarm types, we use command: **no snmp-server cfm-trap**

Steps	Commands	Description
1	**config**	Enter GLOBAL configure mode
2	**snmp-server cfm-trap** *{all| macRemErrXcon | remErrXcon | errXcon | xcon | none}*	Configure four network trouble alarms
3	**Exit**	Return to GLOBAL configure mode
4	**show ethernet cfm**	Display CFM basic information

Examples: set alarm as remerrxcon:

Raisecom(config)#**snmp-server cfm-trap remerrxcon**

Raisecom(config)#**exit**

Sent none as alarm:

Raisecom(config)#**snmp-server cfm-trap none**

28.4.14 Configure Enable/Disable CFM Protocol in GLOBAL Mode

It is used to command CFM protocol in GLOBAL mode. In default situation, CFM protocol is disable.

Steps	Commands	Description
1	**Config**	Enter GLOBAL configure mode
2	**ethernet cfm {***enable* |*disable***}**	Enable/disable CFM protocol. *enable*: enable CFM protocol in GLOBAL mode; *Disable*: Disable CFM protocol in GLOBAL mode.
3	**Exit**	Return to Privileged EXEC mode.
4	**show ethernet cfm**	Check all configuration information of CFM protocol on switches.

Example: in GLOBAL mode, enable CFM protocol

raiecom#**config**

raiecom(config)#**ethernet cfm** *enable*

raiecom(config)#**exit**

28.4.15 Configure Enable/Disable CFM Protocol in Port Mode

We use the command to allow switch port runs CFM protocol. If some port is needed to stop running CFM protocol, then use those commands to configure. The default all ports CFM protocols are enable.

Steps	Commands	Description
1	**Config**	Enter GLOBAL configure mode
2	**interface port port-num**	Enter indicated port's port number
3	**ethernet cfm {***enable*|*disable***}**	Enable/disable CFM protocol. *enable*: in GLOBAL mode, enable CFM protocol; *disable*: in GLOBAL mode, disable CFM protocol
4	**Exit**	Return to Privileged EXEC mode.
5	**Exit**	Return to GLOBAL configure mode
6	**show ethernet cfm**	Check the switch about the CFM protocol's whole configuring information.

Example: In port 3, enable CFM protocol

raiecom#**config**

Raisecom(config)#**interface port** *3*

Raisecom(config-port)#**ethernet cfm** *enable*

28.5 Monitoring and Maintenance

Commands	Description

show ethernet cfm traceroute-cache	displays LinkTrace database studied route trace information
show ethernet cfm mp local	displays local MP configure information, include MEP and MIP
show ethernet cfm errors	displays error CCM database information
show ethernet cfm domain	displays indicated maintenance domain configuration information
show ethernet cfm mp remote	displays remote MEP information
show ethernet cfm mp remote detail	displays remote MEP detail information
show ethernet cfm	displays CFM protocol configuration information
clear ethernet cfm errors	clear error CCM database indicated information
clear ethernet cfm mp remote	clear indicated remote MEP information
clear ethernet cfm traceroute-cache	clear Linktrace database archived route trace information

28.5.1 Display LinkTrace Database Studied Route Trace Information

Commands format: show ethernet cfm traceroute-cache

Function: shows LinkTrace database archived entry number and time, related MD names, levels and service instance related VLANs. Also, it also can display each Linktrace hop number; reply LTR messages MP's MAC address, LTM messages receiving and sending port, LTM messages transmitting status, LTM messages transmitting type and next-hop devices' mac address. When LinkTrace database is in disable status, there is no any route trace information is displayed.

Display results: details can be found in **1.4.9**. Default archive data entry number is 100, archive time is 100(database is enable). Trace one MEP route with MD of md1, level of 3, VLAN of 4 and MAC address is CCCC.

IC_A#**show ethernet cfm traceroute-cache**

The size of the linktrace database: 100 hold-time: 100

Tracing the route toCCCC on domain md1, level 3, VLAN 4.

Hops	*HostMAC*	*Ingress/EgressPort*	*IsForwarded*	*RelayAction*	*NextHop*
1	*AAAA*	*8/1*	*Yes*	*RlyFdb*	*BBBB*
2	*BBBB*	*2/3*	*Yes*	*RlyFdb*	*CCCC*
3	*CCCC*	*-/9*	*No*	*RlyHit*	*CCCC*

28.5.2 Display local MP Configuration Information, include MEP and MIP

Command Format: show ethernet cfm mp local *[mep | mip] [interface port portid | domain domain-name | level level-id]*

Function: It is used to check the local MP configuration information and also can check the MIP related MD levels, related port number and MAC address information. Also, it can check MEP name, related MD level, port number, MEP send direction, MAC address information, CCM messages enable/disable status, sent entries number, etc. We can choose whether display MEP, MIP or both; we also can choose display indicated port MP or all port MP, or choose to display MP of indicated MD.

Display results: details can be found in **1.4.4,** display the level 5 MIP which is configured in port 2 and related MAC address as BBBB; when a MEP is configured as level 3, sending direction is up, CCM messages is disable, sent messages entries number is 0.

IC_B#**show ethernet cfm mp local**

Level Type Port Mac Address

---

5 MIP 2 BBBB

Mpid MdName Level Vlan Type Port Mac Address CC-Status SendCCMs

---

1 md3-1 3 4 UP 2 BBBB Disable 0

28.5.3 Display Error CCM Database Information

Command Format: show ethernet cfm errors [*domain domain-name* | *level level-id*]

Function: it is used to check levels of MD which has fault occurred, fault occurred MA's VLAN, fault occurred local MEP's MEPID, fault related remote MEP's MAC address, the fault types which can be checked at the same time, , can choose to show the CCM fault information in indicated MD, also can choose to show indicated MD level's CCM fault information.

Display results: details can be found in **1.4.8**. Display level 1 fault CCM information, fault MA's VLAN 4, fault found local MEP's MPID as 2, fault found remote MAC address as CCCC, fault type as ErrorCCM.

IC_A#**show ethernet cfm errors level** *1*

Level VLAN MPID RemoteMEP MAC ErrorType AffectedService

---

1 4 2 CCCC ErrorCCM md1-ma4

28.5.4 Display Indicated Maintenance Domain Configuration Information

Commands format: show ethernet cfm domain [*domain-name*]

Function: It is used to check the created MD level and MA related VLAN. Also CCM messages' sending interval can be displayed.

Display results: details can be found in **1.4.2**, displays MD which is configured as name of md3-1, level 3, service instance named ma3-1-4 and related VLAN 4. Also it shows MD named md5-1, level 5.

Raisecom#**show ethernet cfm domain**

In maintenance domain md3-1:

Level: 3

Total services: 1

Service Vlan CCMInterval

---

ma3-1-4 4 10

In maintenance domain md5-1:

Level: 5

Total services: 0

Service Vlan CCMInterval

28.5.5 Display Remote MEP Information

Commands format: show ethernet cfm mp remote [*domain domain-name* | *level level-id*]

Function: it is used to check the remote MEP's MEP ID, the remote MEP located MD name, and that MD's level, the remote MEP located MD level, the remote MEP located MA's related VLAN, the remote MEP name located port status, the remote MEP MAC address, the local switch port which receive CCM messages sent by the remote MEP, and the CCM messages receiving interval from the same remote MEP last time.

Display results: see details in **1.4.8**. Display the remote MEP MPID as 1, its MD is md3; Level is 3; remote MEP located MA VLAN 4; port status is up; remote MEP MAC address is CCCC; local switch port number which receives messages is 1; the interval is 9 seconds.

IC_A#**show ethernet cfm remote level** *3*

MPID MD name Level VLAN PortState MAC IngressPort Age

---

1 md3 3 4 UP CCCC 1 9

28.5.6 Display Remote MEP Particular Information

Commands format: show ethernet cfm mp remote detail {*mpid mep-id* | *mac mac-address*}[*domain domain-name* | *level level-id [vlan vlan-id]]*

Function: can display remote MEP MAC address, remote MEP located MD name, remote MEP located MD level, remote MEP located MA VLAN, remote MEP's MEP ID, the local switch port which receives CCM messages sent by that remote MEP, CCM messages receiving time interval since last time from that remote MEP port, CCM receiving amount statistics sent by that remote MEP and error CCM receiving amount statistics.

By commands parameter, filter remote MEP and display:

1. [Compulsory] choose to indicate remote MEP's MEP ID or MAC address.

2. [Optional] do not indicate MD, MD name or MD level; If choose to indicated MD level, we also can choose to indicate VLAN ID or not.

We can form the filter remote MEP by those two parameters above.

Display Results: configuration details can be found in **1.4.8**. We can find the remote MEP MAC address is CCCC, located MD's name is Md1,level is 3, located MA VLAN is 4, remote MEP's MEPID us 1, local switch port number which receives messages is 8,time interval is 9 seconds, CCM messages received are 120 and error packet is 0.

IC_A#**show ethernet cfm remote detail mpid** *1* **domain** *md1*

MAC address: CCCC

MD/Level: Md1/3

VLAN: 4

MPID: 1

Ingress Port: 8

Age: 9

CCM statistics: 122/0 (Received/Error)

28.5.7 Display CFM Protocol Configuration

Commands format: show ethernet cfm

Function: It is used to display CFM configuration information such as CFM protocol status in GLOBAL mode, CFM status in the port, error CCM messages archived time and error indication level.

Display results: enable GLOBAL CFM protocol, default port CFM protocol is enable, error archive time is 100, error sending level macRemErrXcon.

Raisecom#**show ethernet cfm**

Global CFM Admin Status: enable

Port CFM Enabled Portlist: 1-26

Archive hold time of error CCMs: 100

The trap status: macRemErrXcon

28.5.8 Clear Error CCM Database Indicated Information

Commands format: Clear Ethernet cfm errors [*domain domain-name* | *level level-id*]

Function: By enter MD name, we can clear indicated MD error information; by enter MD level parameters, we can clear the indicated level error information; if do not enter any parameter, it will delete all the error information.

Example: Clear all level 3 error information in CCM error database

Raisecom(config)#**clear ethernet cfm errors level** *3*

28.5.9 Clear Linktrace Database Archive Route Trace Information

Commands format: Clear Ethernet cfm traceroute-cache

Function: Clear data information in LinkTrace database

Example: Raisecom(config)#**clear ethernet cfm traceroute-cache**

28.5.10Clear Indicated Remote MEP Information

Command Format: Clear Ethernet CFM mp remote [domain domain-name | level level-id]

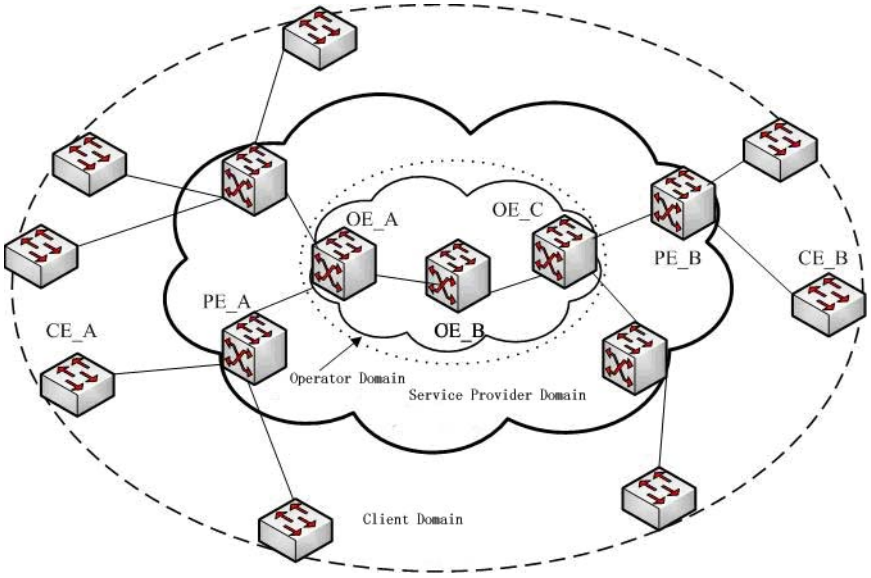
Function: It is used to clear CC database indicated remote MEP information and it also can indicate the MD which needs to be cleared.

Example: Clear remote MEP information in MD named md3-1

Raisecom(config)#**clear ethernet cfm mp remote domain md3-1**

28.6 Basic Configuration Example

Topology as shown below:



We divide metropolitan access network (MAN) into three maintenance domains: client domain with level 5, service provider domain with level 3 and operator domain with level 1. As the figure above, CE_A is connected to PE_A, PE_A is connected to OE_A, OE_A is linked to device OE_C through device OE_B, CE_B is connected to PE_B, PE_B is connected to OE_C. We configure CE_A and CE_B with level 5 MEP; PE_A and PE_B are configured as level 5 MIP, level 3 MEP and level 3 MIP; OE_A and OE_C are configured level 3 MIP, level 1 MEP and level 1 MIP; OE_B is configured with two level 1 MIPs. Details

are:

CE_A configuration steps:

Raisecom(config)#**ethernet cfm domain md7-1 level** *7*

Raisecom(config-ether-cfm)#**exit**

Raisecom(config)#**ethernet cfm domain** *md5-1* **level** *5*

Raisecom(config-ether-cfm)#**service** *ma5-1-100* **vlan** *100*

Raisecom(config-ether-cfm)#**exit**

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

Raisecom(config-port)#**ethernet cfm mip level** *7*

Raisecom(config-port)#**ethernet cfm mep level** *5* **up mpid** *501* **vlan** *100*

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

Raisecom(config)#**ethernet cfm** *enable*

Raisecom(config)#**ethernet cfm cc** *enable* **level** *5* **vlan** *100*

PE_A configuration steps:

Raisecom(config)#**ethernet cfm domain md5-1 level** *5*

Raisecom(config-ether-cfm)#**exit**

Raisecom(config)#**ethernet cfm domain md3-1 level** *3*

Raisecom(config-ether-cfm)#**service ma3-1-100 vlan** *100*

Raisecom(config-ether-cfm)#**exit**

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

Raisecom(config-port)#**ethernet cfm mip level** *5*

Raisecom(config-port)#**ethernet cfm mep level** *3* **up mpid** *301* **vlan** *100*

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

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

Raisecom(config-port)#**ethernet cfm mip level** *3*

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

Raisecom(config)#**ethernet cfm enable**

Raisecom(config)#**ethernet cfm cc enable level** *3* **vlan** *100*

OE_A configuration steps:

Raisecom(config)#**ethernet cfm domain md3-1 level** *3*

Raisecom(config-ether-cfm)#**exit**

Raisecom(config)#**ethernet cfm domain md1-1 level** *1*

Raisecom(config-ether-cfm)#**service ma1-1-100 vlan** *100*

Raisecom(config-ether-cfm)#**exit**

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

Raisecom(config-port)#**ethernet cfm mip level** *3*

Raisecom(config-port)#**ethernet cfm mep level** *1* **up mpid** *101* **vlan** *100*

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

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

Raisecom(config-port)#**ethernet cfm mip level** *1*

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

Raisecom(config)#**ethernet cfm** *enable*

Raisecom(config)#**ethernet cfm cc** *enable* **level** *1* **vlan** *100*

OE_B configuration steps:

Raisecom(config)#**ethernet cfm domain md1-1 level** *1*

Raisecom(config-ether-cfm)#**exit**

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

Raisecom(config-port)#**ethernet cfm mip level** *1*

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

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

Raisecom(config-port)#**ethernet cfm mip level** *1*

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

Raisecom(config)#**ethernet cfm** *enable*

OE_C configuration steps:

Raisecom(config)#**ethernet cfm domain md3-1 level** *3*

Raisecom(config-ether-cfm)#**exit**

Raisecom(config)#**ethernet cfm domain md1-1 level** *1*

Raisecom(config-ether-cfm)#**service ma1-1-100 vlan** *100*

Raisecom(config-ether-cfm)#**exit**

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

Raisecom(config-port)#**ethernet cfm mip level** *3*

Raisecom(config-port)#**ethernet cfm mep level 1 up mpid** *102* **vlan** *100*

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

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

Raisecom(config-port)#**ethernet cfm mip level** *1*

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

Raisecom(config)#**ethernet cfm** *enable*

Raisecom(config)#**ethernet cfm cc** *enable* **level** *1* **vlan** *100*

PE_B configuration steps:

Raisecom(config)#**ethernet cfm domain md5-1 level** *5*

Raisecom(config-ether-cfm)#**exit**

Raisecom(config)#**ethernet cfm domain md3-1 level** *3*

Raisecom(config-ether-cfm)#**service ma3-1-100 vlan** *100*

Raisecom(config-ether-cfm)#**exit**

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

Raisecom(config-port)#**ethernet cfm mip level** *5*

Raisecom(config-port)#**ethernet cfm mep level** *3* **up mpid** *302* **vlan** *100*

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

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

Raisecom(config-port)#**ethernet cfm mip level** *3*

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

Raisecom(config)#**ethernet cfm** *enable*

Raisecom(config)#**ethernet cfm cc** *enable* **level** *3* **vlan** *100*

CE_B configuration steps:

Raisecom(config)#**ethernet cfm domain md7-1 level** *7*

Raisecom(config-ether-cfm)#**exit**

Raisecom(config)#**ethernet cfm domain md5-1 level** *5*

Raisecom(config-ether-cfm)#**service ma5-1-100 vlan** *100*

Raisecom(config-ether-cfm)#**exit**

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

Raisecom(config-port)#**ethernet cfm mip level** *7*

Raisecom(config-port)#**ethernet cfm mep level** *5* **up mpid** *502* **vlan** *100*

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

Raisecom(config)#**ethernet cfm** *enable*

Raisecom(config)#**ethernet cfm cc** *enable* **level** *5* **vlan** *100*

After configuring CE_A, PE_A, OE_A, OE_B, OE_C, PE_B and CE_B, the MEP configured device should be able to ping MAC address and trace route success with other devices which are configured MEP with same level MP.

On CE_A, ping and trace route CE_B as below, use "CE_B" represents CE_B device's MAC address:

Raisecom#**ping ethernet CE_B level** *5* **vlan** *100*

Raisecom#**traceroute ethernet CE_B level** *5* **vlan** *100*

On PE_A, ping and trace route PE_B are described as below, use "PE_B" represents PE_B device's MAC address:

Raisecom#**ping ethernet PE_B level** *3* **vlan** *100*

Raisecom#**traceroute ethernet PE_B level** *3* **vlan** *100*

On OE_A, ping and trace route OE_B are OE_C as described as below, use "OE_B"and "OE_C" represent OE_B and OE_C device MAC address:

Raisecom#**ping ethernet OE_B level** *1* **vlan** *100*

Raisecom#**traceroute ethernet OE_B level** *1* **vlan** *100*

Raisecom#**ping ethernet OE_C level** *1* **vlan** *100*

Raisecom#**traceroute ethernet OE_C level** *1* **vlan** *100*

Chapter 29 Trace Route

29.1 Overview

Traceroute, like ping, is a useful application in network management, which is used to discover the routing path that the message actually passed before it get its destination.

L3 Traceroute is realized by sending a serious of incremental TTL probe packets. Probe message is in the form of UDP message, while some uses ICMP Echo requesting message. Unless TTL value is larger than 0, each hop to the destination will bring back a ICMP message, with which we can calculate each hop's RRT on the path to destination.

29.2 Configure traceroute

Before using L3 Traceroute, we need to configure the switch IP address and default gateway, the related commands are as follows:

Command	Description
config	Enter global configuration mode
int ip *0*	Enter IP interface 0
ip address *A.B.C.D* **vlanID**	Configure the switch IP addrss
exit	Quit from global configuration mode and enter privileged EXEC mode
ip default-gateway A.B.C.D	Configure the switch default gateway
show int ip	Show IP configuration
show running	Show default gateway configuration
traceroute A.B.C.D [**firstTTL** <*1-255*>] [**maxTTL** <*1-255*>] [**port** <*1-65535*>] [**waittime** <*1-60*>] [**count** <*1-10*>]	Traceroute show the actual path to the destination

The commands execution echo is shown below:

Router1#**traceroute** *34.0.0.4*

Type ctrl+c to abort.

Tracing the route to 34.0.0.4

1 12.0.0.2 4 ms 4 m 4 m

2 23.0.0.3 20 ms 16 ms 16 ms

*3 34.0.0.4 16 ms * 16 ms*

Trace complete.

29.3 Typical configuration example

For example: to trace the route to 58.63.236.42(www.sina.com.cn)

Raisecom#**config**

Raisecom(config)# **int ip** *0*

Raisecom(config-ip)#**ip address** *10.0.0.8 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**ip default-gateway** *10.100.0.1*

Raisecom(config)#**exit**

Raisecom#Tracing the route to *58.63.236.42*

Type ctrl+c to abort.

1	*10.0.0.1*	*10 ms*	*10 ms*	*10 ms*
2	*192.168.101.5*	*3 ms*	*3 ms*	*73 ms*
3	*192.168.101.5*	*10 ms*	*10 ms*	*10 ms*
4	*202.96.4.81*	*18 ms*	*16 ms*	*19 ms*
5	*202.106.228.177*	*9 ms*	*5 ms*	*12 ms*
6	*202.106.228.5*	*10 ms*	*8 ms*	*9 ms*
7	*202.96.12.25*	*7 ms*	*8 ms*	*5 ms*
8	*219.158.11.66*	*24 ms*	*20 ms*	*10 ms*
9	*202.97.15.57*	*101 ms*	*101 ms*	*126 ms*
10	*202.97.60.185*	*218 ms*	*222 ms*	*205 ms*
11	*202.97.40.58*	*119 ms*	*112 ms*	*113 ms*
12	*219.136.246.134*	*118 ms*	*142 ms*	*131 ms*
13	*219.136.246.6*	*138 ms*	*135 ms*	*110 ms*
14	*58.63.232.46*	*103 ms*	*115 ms*	*105 ms*
15	*58.63.236.42*	*199 ms*	*205 ms*	*197 ms*

Trace complete.

Chapter 30 Failover

30.1 Failover overview

Failover function is used to provide specific port linkage project for special usage, which is able to expand the range of link backup. By monitoring uplink to configure down link, so that uplink fault is able to be sent to downriver equipments, which raises backuplink switch and prevent stream lose because of long time uplink fault.

Failover group is made up of uplink ports and downriver ports, a failover group may contain several uplink ports and downriver ports. When failover group is configured, the uplink ports will be monitored. Once all the uplink ports in failover group are in trouble, all the downriver ports will be turned to DOWN compulsively. When one or more uplink ports restore to normal, the downriver ports will be restored to UP. A downriver port fault will not affect the state of uplink port or other downriver ports.

Failover is used in the topology of double uplink or multi-uplink usually. When the main link gets into trouble, by switching the fault from uplink port to downriver port, the main link can be made sure to switch backup link quickly. In double uplink network, when one uplink route is blocked by redundance, the other link will be used for up sending. When link fault happens, the switch in the middle will switch the fault to downriver switch immediately, informing downriver switch for link switch, to decrease traffic lose.

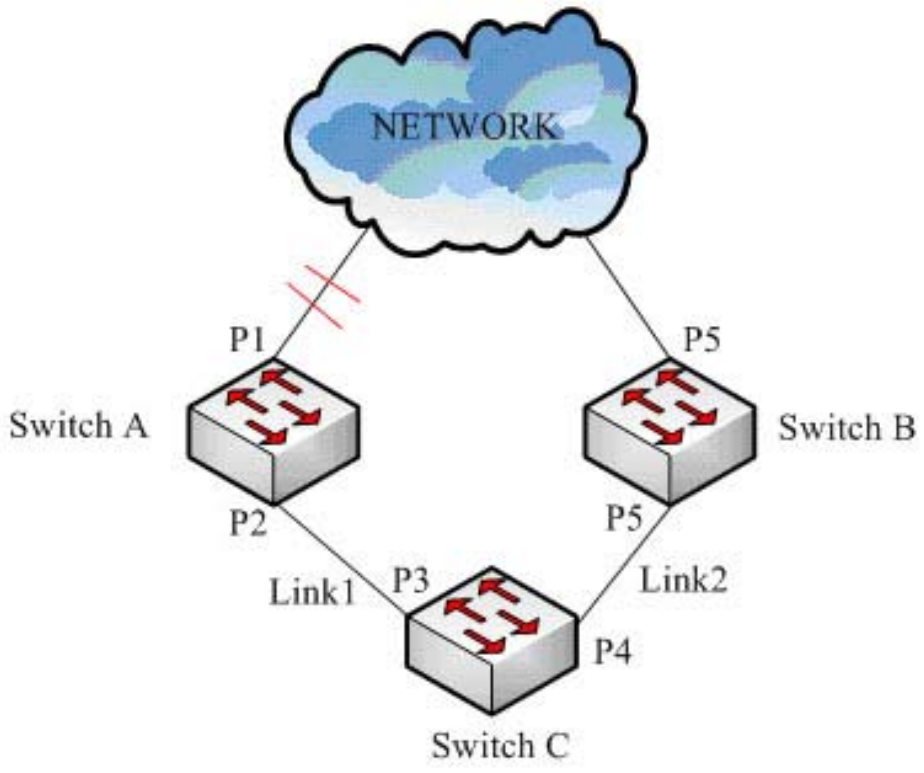


Fig 30-1 Failover

As is shown in figure 1-1, SwitchC uses main link Linke1 and backup link Link2 to connect to NETWORK,

when the link that SwitchA connects to NETWORK has fault, SwitchA will switch the fault to downriver port immediately, so that when Link1 breaks down, SwitchC will find out Link1 fault of SwitchA and its own and switch to Link2 that is connected with SwitchB, which realizes the rapid switch from the main link to backup link.

30.2 Configure failover

Failover configuration includes failover group and failover port configuration. The switch supports 1-10 failover groups. If failover group has not been created before configuring failover port, then a failover group will be created first and the ports will be added to the group. A port can belong to one failover group for only, and it can be only uplink or downriver port. The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**link-state-tracking group** *groupNumber*	Create and enable failover group. If the failover group has not been created, the failover group will be created and enabled first. *groupNumber:* failover group number, range is 1-10;
3	**interface line/client** <1-MAX_PORT_NUM>	Enter physical port mode
4	**link-state-tracking group** *groupNumber* **{upstream |downstream}**	Configure which failover group the port belongs to and the port type *groupNumber*; failover group number, range is 1-10; **Upstream**: uplink port **Downstream**: downriver port
5	**exit**	Return to global configuration mode
6	**exit**	Return to privileged EXEC mode
7	**show link-state-tracking group** [*groupNumber*]	Show failover group configuration and state

Use **no link-state-tracking group** *groupNumber* to disable failover function, if there is no port in the group and the group is not enabled, the group will be deleted as well.

Use **no link-state-tracking group** to delete a port from a failover group, if there is no port in the failover group, the group will be deleted as well.

Attention: There can be several uplink ports in a failover group, if only there is one uplink port in UP state failover function will not happen; only when all the uplink ports are in DOWN state can failover function takes effect.

30.3 Monitoring and maintenance

Command	Description

show link-state-tracking group [*groupNumber***]**	Show failover group configuration and state
show link-admin-status port *portlist*	Show port UP/DOWN management state

Attention: The command **show link-state-tracking group [***groupNumber***]** can not show the information of the failover group that has been created but not enabled, and there is not port in it.

30.4 Typical configuration example

The topology structure of failover function is shown in the figure below:

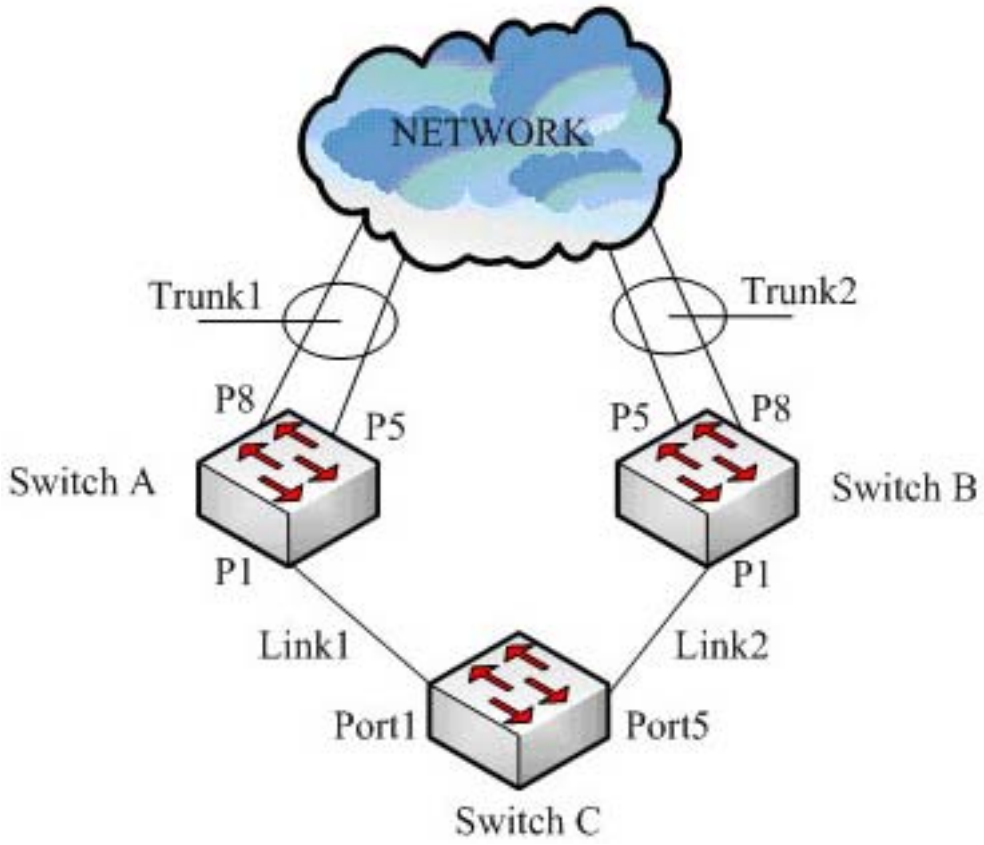


Fig 30-2 Typical topology structure of failover function

As is shown in figure 1-2, to make sure the network connection SwitchC uses Link1 and Link2 for uplink. SwitchA and SwtichB use Trunk1 and Trunk2 to connect to the network. Enable spanning tree protocol on SwitchC, Link2 is in discarding state. When Link1 is breaking down, the spanning tree will switch to Link2 immediately. But if SwtichA uplink Trunk1 breaks down, SwitchC may not being able to rapidly inspect the disconnection of its uplink channel, which may cause message lose. If when Trunk1 is breaking down, SwitchA breaks down it downriver port at the time, then SwitchC will switch the uplink route to Link2 to make sure the connection of the uplink. So we should configure failover group on SwitchA and SwitchB, and the configuration of the two should be the same completely. The configuration of SwitchA is shown below:

Raisecom#**config**

Raisecom(config)#**link-state-tracking group** *1*

Raisecom(config)#**intface port** *1*

Raisecom(config-port)#**link-state-tracking group** *1* **downstream**

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

Raisecom(config)#**intface range** *5,8*

Raisecom(config-range)#**link-state-tracking group** *1* **upstream**

Raisecom(config-range)#**exit**

Raisecom(config)#**exit**

Raisecom#**show link-state-tracking group** *1*

Raisecom#**show link-admin-status port** *1,5,8*

Link State Tracking Group: 1 (Enable)

Status: Normal

Upstream Interfaces:

Port5(Down) Port8(Up)

Downstream Interfaces:

Port1(Down)

Port	*module*	*admin*
1	*shutdown*	*Up*
	LoopbackDetect	*Up*
	linkStateTrack	*Up*
5	*shutdown*	*Up*
	LoopbackDetect	*Up*
	linkStateTrack	*Up*
8	*shutdown*	*Up*
	LoopbackDetect	*Up*
	linkStateTrack	*Up*

If SwitchA uplink Trunk1 is breaking down, the configuration result will be shown below:

Link State Tracking Group: 1 (Enable)

Status: Failover

Upstream Interfaces:

Port5(Down) Port8(Down)

Downstream Interfaces:

Port1(Disable)

Port	*module*	*admin*

```
-------------------------------------------------
1       shutdown            Up
        LoopbackDetect      Up
        linkStateTrack      Down
5       shutdown            Up
        LoopbackDetect      Up
        linkStateTrack      Up
8       shutdown            Up
        LoopbackDetect      Up
        linkStateTrack      Up
```

Chapter 31 Schedule Commands

31.1 cmd-str schedule-list

[Function]

Operating the command according to schedule mode or say, add the command into schedule list.

[Command Format]

cmd-str **schedule-list** *list-no*

no schedule-list *list-no* **command** *cmd-no*

[Parameter]

cmd-no: command in the schedule list, this is a dynamic variational command no.;

schedule-list: set start time, finish time and interval of perodic executiong of schedule task;

list-no: the range of schedule list is <0-99>.

[Command Modes]

Global configuration mode, Privileged user

[Explanation of command execution echo]

Set successfully.

Current schedule list not existed.

[Example]

Raisecom(config)#**storm-control dlf schedule-list** *1*

Raisecom#**no schedule-list** *1* **command** *0*

[Related commands]

Commands	Description
schedule-list *list-no*	Add or modify schedule list.
show schedule-list	Show information of schedule-list.

Commands list in support of schedule:

[no] filter *{ip-access-list|mac-access-list| access-list-map} (all|<0-399>)* **port-list** *(all|{1-26}) {ingress|egress|both}*

filter *{enable|disable}*

[no] filter *{ip-access-list|mac-access-list| access-list-map}{all|<0-399>}* **vlan-list** *{all|{1-4094}}*

clear arp

flowcontrol *{on | off }*

ip igmp-snooping

no ip igmp-snooping

ip igmp-snooping

no ip igmp-snooping

no shutdown

shutdown

duplex *{full-duplex | half-duplex }*

speed *{ auto | 10 | 100 |1000}*

clear interface port statistics

clear interface port *<1-"MAX_PORT_STR">* **statistics**

switchport protect

no switchport protect

rate-limit port-list *(all | {1-"MAX_PORT_STR"})* **ingress**

rate-limit port-list *(all | {1-"MAX_PORT_STR"})* **egress**

no rate-limit port-list *(all | {1-"MAX_PORT_STR"}) (ingress | egress | both)*

sntp server *A.B.C.D*

no sntp server

spanning-tree *(enable|disable)*

mac-address-table aging-time

no mac-address-table aging-time

mac-address-table learning *(enable | disable)* **port-list** *(all | {1-"MAX_PORT_STR"})*

mac-address-table static *HHHH.HHHH.HHHH* **vlan** *<1-4094>* **port** *<1-"MAX_PORT_STR">*

clear mac-address-table *(all | dynamic | static)*

mirror *(enable | disable)*

svl *(enable|disable)*

dlf-forwarding *(enable | disable)*

no relay *(bpdu | dot1x | lacp | garp | gmrp | gvrp | all)* **port-list** *[{1-"MAX_PORT_STR"}]*

relay *(bpdu | dot1x | lacp | garp | gmrp | gvrp | all*) **port-list** *{1-"MAX_PORT_STR"}*

storm-control ratio *<1-100> <0-512>*

storm-control ratio *<1-100>*

storm-control bps *<0-1000> <0-512>*

storm-control pps *<0-262143>*

storm-control all *(enable | disable)*

storm-control dlf *(enable | disable)*

storm-control multicast *(enable | disable)*

storm-control broadcast *(enable | disable)*

[no] ip dhcp relay(global configuration mode)

[no] ip dhcp relay(IP interface configuration mode)

[no] ip dhcp relay ip-list *{ all | ip-list }* **target-ip** *A.B.C.D*

[no] ip dhcp relay target-ip *A.B.C.D*

[no] ip dhcp relay information option

ip dhcp relay information policy *{ drop | keep | replace }*

[no] ip dhcp relay information trusted port-list *{ all | port-list }*

[no] ip dhcp relay information trusted

[no] ip dhcp server (global configuration mode)

[no] ip dhcp server (IP interface configuration mode)

ip dhcp server ip-pool pool-name start-ip end-ip mask-ip ip *<0-MAXIP> [gateway gtw-address] [dns dns-address] [secondary-dns dns-address]*

no ip dhcp server ip-pool pool-name

ip dhcp server relay-ip *A.B.C.D A.B.C.D*

no ip dhcp server relay-ip *A.B.C.D*

ip dhcp snooping

no ip dhcp snooping

ip dhcp snooping port-list *{ all | port-list }*

no ip dhcp snooping port-list *{ all | port-list }*

ip dhcp snooping trust

no ip dhcp snooping trust

ip dhcp snooping information option

no ip dhcp snooping information option

31.2 schedule-list

[Function]

Add or modify schedule-list, this command used to set the starting time, ending time and periodical execution interval.

[Command Format]

no command to delete a queue.

schedule-list *list-no* **start** {**up-time** *days time* [**every days time** [**stop** *days time*]] | **date-time** *date time* [**every** {*day* | *week* | *days time*} [**stop** *date time*]]}

no schedule-list *list-no*

[Parameter]

list-no: dispatching list range is <0-99>;

up-time: Relative time after startup;

date-time: Absolute time after startup;

days time: a time period, the format is: days: <0-65535>, time: HH:MM:SS. Example: 3 3:2:1;

date time: a time point, input format is: MMM-DD-YYYY HH:MM:SS. Example: jan-1-2003 or 1-1-2003, the range of YYYY is 1970 to 2199.

[Command Modes]

Global configuration mode; privileged user.

[Explanation of command execution echo]

Set successfully.

input Date & Time should be MMM-DD-YYYY(1900-2199), HH:MM:SS format

[Example]

Raisecom# **schedule-list** *1* **start date-time** *Feb-2-2004 0:0:0* **every** *6 0:0:0* **stop** *Feb-2-2005 0:0:0*

[Related commands]

Commands	Description
Show schedule-list	Show schedule-list information.
comd-str schedule-list *list-no*	Execute the command based on the way of dispatching.

31.3 show schedule-list

[Function]

Show schedule list information.

[Command Format]

show schedule-list [*list-no*]

[Parameter]

list-no: dispatching list range is <0-99>.

[Command Modes]

Privileged EXEC, privileged user

[Example]

Raisecom# **show schedule-list** *1*

[Related commands]

Commands	Description
schedule-list list-no	Add or modify schedule list
comd-str schedule-list *list-no*	Apply the command based on the way of schedule list.

Chapter 32 SLA

This chapter is about how to configure SLA on switch, including:

- ✧ SLA overview
- ✧ Default SLA configuration list
- ✧ SLA configuration guide and limit
- ✧ SLA configuration list and instruction
- ✧ Monitoring and maintenance
- ✧ Typical configuration example

32.1 Overview

SLA (Service Level Agreements) is a protocol between service provider and user on service quality, privilege and duty, it is also a telecom service evaluation standard.

Technologically, SLA is a real-time network performance detection and statistic technology, which is able to make statistics for response time, network jitter, delay, packet lose rate and so on. SLA is able to choose different work and monitor the related value according to different application.

32.1.1. SLA modules

1. task

Static concept, it is an end-to-end SLA network performance test task, including layer-2 network delay/jitter test and layer-3 network delay/jitter test.

2. exploration

Dynamic concept, it is used to describe the process of an exploration message being sent and received in task test.

3. test

Dynamic concept, it is used to describe a execution of a task. According to the definition of the task, one task test may contain several exploration(to Echo task, one test contains only one exploration).

4. schedule

Dynamic concept, it is used to describe a schedule of one task, a schedule may contain several seasonal test execution.

32.1.2. Basic SLA function

SLA module is mainly used for network performance measure, which take the result as the proof to make sure user's requirement for performance. We can choose two.

Chapter 33 Environment Monitoring

33.1 Environment monitoring principle

Environment monitoring function is to monitor the critical parameters to the equipments, including: temperature, pressure and so on. When these parameters go wrong, user can take corresponding treasures to prevent faults from happening.

The system can show the chassis temperature and the actual value of 1.2/1.5/1.8/3.3V voltage, and monitor the chassis temperature and 3.3V voltage, emits alarm when they are out of the way.

33.2 Configure environment monitoring

Function	Default
Temperature alarm	Enable
Voltage alarm	Enable
Temperature alarm threshold	High temperature threshold 70°, low temperature threshold 5°
Voltage alarm threshold	High voltage threshold 3460mV, low voltage threshold 3140mV

33.2.1 Default environment monitoring configuration

33.2.2 Configure temperature monitoring

Configure temperature alarm threshold value and enable temperature alarm function

Step	Command	Description
1	**config**	Enter global configuration
2	**alarm temperature threshold Celsius|Fahrenheit**	Configure the temperature alarm threshold, it can be configured Celsiur scale and Fahrenheit scale
	low <*LowValueRange*> **high** <*HighValueRange*>	LowValueRange: 0-30 in Celsiur scale; 32-86 in Fahrenheit scale; HighValueRange: 30-70 in Celsiur scale; 86-158 in Fahrenheit scale
3	**alarm temperature**	Enable temperature alarm function
4	**exit**	Quit from global configuration mode and enter privileged EXEC mode
5	**show hardware**	Show hardware environment monitoring information

Use **no alarm temperature** to disable temperature alarm function.

Use **no alarm temperature threshold** to restore temperature alarm threshold to default value: high temperature threshold value is 70°， low temperature threshold value is 5°.

33.2.3 Voltage monitoring configuration

Configure voltage alarm threshold value and enable voltage alarm function

Step	Command	Description
1	**config**	Enter global configuration mode
2	**alarm volt threshold low** <3000-3300> **high** <3300-3600>	Configure voltage alarm threshold, unit is mV; Low: low voltage threshold High: high voltage threshold
3	**alarm volt**	Enable voltage alarm function
4	**exit**	Quit from global configuration mode and enter privileged EXEC mode
5	**show hardware**	Show hardware environment monitoring information

Use **no alarm volt** to disable voltage alarm function

Use **no alarm volt threshold** to restore voltage alarm threshold value to default value: high voltage value is 3460mV, low voltage threshold is 3140mV.

33.2.4 Monitoring and maintenance

Use **show** to check out the corresponding configuration on hardware monitoring:

Command	Description
show hardware	Show current temperature and voltage value, and temperature & voltage monitoring switch and threshold configuration.

Use **show hardware** to show current equipment temperature and voltage value, if temperature monitoring is enabled, voltage monitoring function and the corresponding threshold configuration. The following example is about the return value:

Raisecom#**show hardware**

Temperature table:

Units Current Min Max Trap Low High Warnings

Celsius 32 31 32 Enable 5 70 0

Fahrenheit 89 87 89 Enable 41 158 0

Volt table(mv):

Referenc	*Current*	*Min*	*Max*	*Trap*	*Low*	*High*	*Warnings*
3300	*3283*	*3283*	*3283*	*Enable*	*3140*	*3460*	*0*
2500	*2513*	*2513*	*2513*	*Disable*	*0*	*0*	*0*
1800	*1814*	*1814*	*1814*	*Disable*	*0*	*0*	*0*
1200	*1252*	*1252*	*1252*	*Disable*	*0*	*0*	*0*

33.2.5 Typical configuration example

Configure the equipment temperature monitoring threshold to 30°-69°, voltage monitoring threshold to 3100-3600mV:

Raisecom#**config**

Raisecom(config)# **alarm temperature threshold Celsius low** *30* **high** *69*

Raisecom(config)# *Set successfully*

Raisecom(config)#**alarm volt threshold low** *3100* **high** *3600*

Raisecom(config)# *Set successfully*

Raisecom#**show hardware**

Temperature table:

Units	*Current*	*Min*	*Max*	*Trap*	*Low*	*High*	*Warnings*
Celsius	*32*	*31*	*33*	*Enable*	*30*	*69*	*0*
Fahrenheit	*89*	*87*	*91*	*Enable*	*86*	*156*	*0*

Volt table(mv):

Referenc	*Current*	*Min*	*Max*	*Trap*	*Low*	*High*	*Warnings*
3300	*3283*	*3283*	*3283*	*Enable*	*3100*	*3600*	*0*
2500	*2513*	*2513*	*2513*	*Disable*	*0*	*0*	*0*
1800	*1814*	*1814*	*1814*	*Disable*	*0*	*0*	*0*
1200	*1252*	*1252*	*1252*	*Disable*	*0*	*0*	*0*

Restore the equipment and voltage monitoring threshold:

Raisecom#**config**

Raisecom(config)# **no alarm temperature threshold**

Raisecom(config)# *Set successfully*

Raisecom(config)# **no alarm volt threshold**

Raisecom(config)# *Set successfully*

Raisecom#**show hardware**

Temperature table:

Units	*Current*	*Min*	*Max*	*Trap*	*Low*	*High*	*Warnings*
Celsius	*32*	*31*	*33*	*Enable*	*5*	*70*	*0*
Fahrenheit	*89*	*87*	*91*	*Enable*	*86*	*156*	*0*

Volt table(mv):

Referenc	*Current*	*Min*	*Max*	*Trap*	*Low*	*High*	*Warnings*
3300	*3283*	*3283*	*3283*	*Enable*	*3140*	*3460*	*0*
2500	*2513*	*2513*	*2513*	*Disable*	*0*	*0*	*0*
1800	*1814*	*1814*	*1814*	*Disable*	*0*	*0*	*0*
1200	*1252*	*1252*	*1252*	*Disable*	*0*	*0*	*0*

Chapter 34 NTP

34.1 NTP configuration

This chapter is mainly about how to configure and maintain NTP, including:

- ✧ NTP principle overview
- ✧ NTP configuration
- ✧ Monitoring and maintenance
- ✧ Typical configuration example
- ✧ NTP trouble shooting

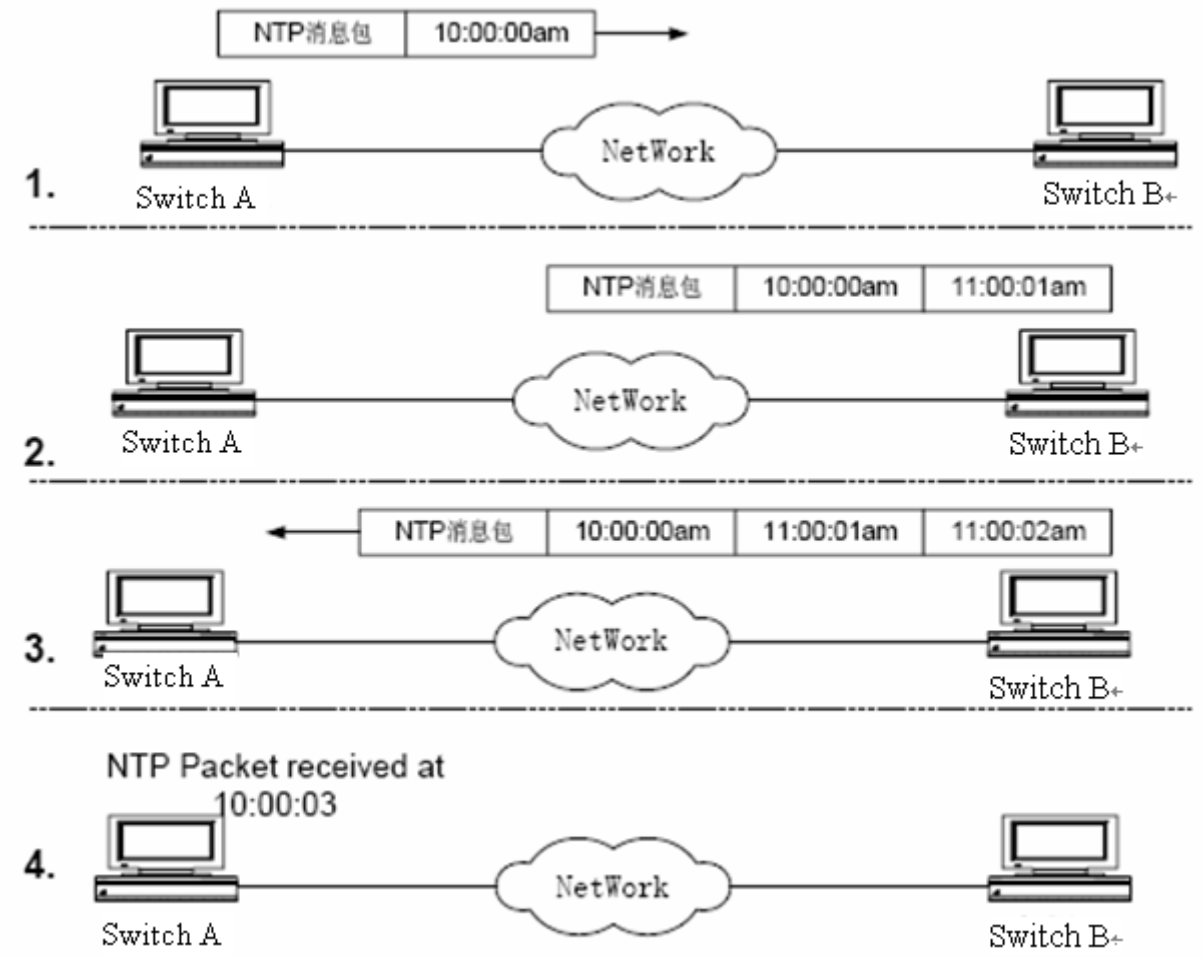
34.1.1 NTP principle overview

As the development and extension of internet all through the world, there are several applications related to time, like real time trade over the network, distributed network computing, traffic schedule and lane management, database management and so on, all these applications need accurate and reliable time.

NTP (Network Time Protocol) is a standard internet protocol used for time synchronization. The usage of NTP is to synchronize the computer time to a certain time criterion. NTP considers fully about the complexity of time synchronization over internet. The mechanism offered by NTP is strict, practical and effective, which is adaptive for network of all kinds on scale, speed and connection state. NTP takes the time message sent by GPS time code as the standard, and uses Client/Server structure, UTC (Universal Time Coordinated) as the time standard. Based on UDP/IP, it uses hierarchical time distributing module which is highly flexible and fits all kind of internet environment. NTP can not only change current time, but also trace time change and modify the time automatically. Even if the there is network fault, the time stability can be ensured. NTP costs little network resources, it also has the solution to make sure network security.

NTP protocol describes carefully about the features of local clock and time server, as well as the way to estimate the error between local clock and time server, and the algorithms used in the process of protocol realization like clock filter, clock selection. When there are several clock servers in the network, the accuracy of local clock can be raised by choosing algorithm to reduce the clock offset. In the same way, when several clock messages are received by a host, with clock filter algorithm the message that has the least error and best performance will be chosen to set local clock.

The basic working principle of NTP is shown below:



The figure shown above shows the basic working principle of NTP, switch A and switch B connect with each other through network, they both have their own system clock to realize automatic synchronization of each system clock. First, the following hypothesis is needed for the process of clock synchronization:

1) Before switch A and switch B are executing system clock synchronization , switch A clock is set to 10:00:00 am, switch B clock is set to 11:00:00 am.
2) Switch B is NTP clock server, or switch A will synchronize its own clock to switch B.
3) The time that a packet transmits from switch A to B is 1 second.

The process of system clock synchronization is shown below:

1) Switch A sends a NTP message to switch B, in the message there is a time stamp that when will the message left switch A, the time stamp is 10:00:00 am (t1).
2) When the NTP message reaches switch B, switch B will add its own time stamp: 11:00:01 am (t2).
3) When NTP leaves switch B, switch B will add its own time stamp to the message: 11:00:02 am (t3)
4) When switch A receives the responding message, a new time stamp will be added: 10:00:03 am (t4).

Up till now, switch A has own enough information to compute two important parameters:

The delay of NTP message back from a cycle: Delay= (t4-t1) – (t3-t2).

The delay of NTP message transmission in a circle: Delay=(t4-t1) – (t3-t2).

The time offset between switch A and switch B: offset=((t2-t1)+(t3-t4))/2.

With the information above, switch A is about to adjust its own clock to synchronize with switch B.

34.1.2 Configure NTP

This part describes how to configure NTP on the switch, including:

- ✧ Default NTP configuration
- ✧ NTP configuration guide
- ✧ NTP server configuration
- ✧ NTP peer configuration
- ✧ Referenced clock source configuration

34.1.2.1Default NTP configuration

Function	Default
Global NTP server	N/A
Global NTP peer	N/A
Referenced clock source	0.0.0.0
NTP state	ntpSlave
version	v3

34.1.2.2NTP configuration guide

1. When the equipment is configured referenced clock source, the equipment will change to synchronized state, and can not be configured to NTP server or peer, either can it be synchronized by other equipments;

2. When configured NTP server or peer, it can not be configured referenced clock source, and then the equipment can do synchronization with other equipments.

34.1.2.3Configure NTP server

By default, converter NTP server IP address is not configured; if the commands of configuring NTP server have been executed, there will be no longer version number, and the default version number is 3.

The configuration steps are shown below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ntp server** *20.0.0.110*	Configure NTP server
3	**exit**	Return to privileged EXEC mode
4	**show ntp associations**	Show NTP connection

Attention:

- If the equipment has been configured to referenced clock source, then configuring NTP server fails; on the opposite, if NTP server or peer has been configured, NTP referenced clock source will be successfully configured.

Use **no ntp server** *ip-address* to delete the configured NTP server.

34.1.2.4Configure NTP peer

By default, peer IP address is not configured, if the command is executed, while version number is not configured, then default version number is 3.

Step	Command	Description
1	**config**	Enter global configuration
2	**ntp peer** *20.0.0.110*	Configure NTP peer
3	**exit**	Return to privileged EXEC mode
4	**show ntp associations**	Show NTP connection

34.1.2.5Configure referenced clock source

By default the equipment is not NTP referenced clock source, if the command has been configured, then default referenced clock is 127.127.1.0, default stratum is 8.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ntp reclock-master**	Configure the equipment to NTP referenced clock source
4	**exit**	Return to global configuration mode
5	**show ntp status**	Show NTP state

Attention: When the equipment is configured to referenced clock source, it can not be synchronized to other equipments; when it has been configured to NTP server or peer, it will not configured to NTP referenced clock source successfully.

Use **no ntp refclock** to cancel the equipment as NTP referenced clock sourece.

34.1.3 Monitoring and maintenance

Use **show ntp status** to show NTP state; use **show ntp association** to show NTP connection.

Command	Description
show ntp status	Show NTP status
show ntp associations	Show NTP connection

Use **show ntp status** to show NTP related status information, including clock state, the selected NTP end, version number, equipment mode, hop second instruction, polling time, clock precision, system stratum, referenced clock source, the latest refreshed local time, current time, root delay, root offset, specified state is shown below:

Raisecom#**show ntp status**

Clock status : synchronized

NTP peer : 20.6.6.9

NTP version : 3

NTP mode : ntpSlave

Leap : 0

Poll : 8

Stratum : 5

*Precision : 2**4*

Reference clock : 20.6.6.9

Reference time : cd6c8915.0c0d3480(Thu Mar 19 09:04:21.047 UTC 2009)

Current clock : cd6d6ee4.0c0d3480(Fri Mar 20 01:24:52.047 UTC 2009)

Root delay : -1.000009

Root dispersion : 0.001380

Use **show ntp associations** to show NTP connection, including opposite end type, synchronization state, opposite end stratum and polling time, delay time, offset, mode, and interval between latest update and executing the commands, the responding packets that have arrived. Specified state is shown below:

Raisecom#**show ntp associations detail**

Server(ip) refid stratum poll when delay offset dispersion mode reach

(s)20.6.6.9 127.127.1.0 4 9 58927 -1.065525 0.005769 0.000000 1 255

Peer(ip) refid stratum poll when delay offset dispersion mode reach

(u)20.6.6.8 0.0.0.0 16 10 58522 0.000000 0.000000 16.000000 0 0

Show detailed connection information:

Server(ip) refid stratum poll when delay offset dispersion mode reach

(s)20.6.6.9 127.127.1.0 4 9 59216 -1.065525 0.005769 0.000000 1 255

filtoffset = 0.000741 0.001415 0.002088 0.002758 0.003422 0.003780 0.004427 0.005769

filtdelay = -1.065526 -1.065525 -1.065525 -1.065526 -1.065525 -1.065525 -1.065525 -1.065525

filtdispersion=16.000000 16.000000 16.000000 16.000000 16.000000 16.000000 16.000000 0.000000

Peer(ip) refid stratum poll when delay offset dispersion mode reach

(u)20.6.6.8 0.0.0.0 16 10 58811 0.000000 0.000000 16.000000 0 0

filtoffset = 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000

filtdelay = 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000 0.000000

filtdispersion= 16.000000 16.000000 16.000000 16.000000 16.000000 16.000000

16.000000 16.000000

34.1.4 Typical configuration example

This part is about an example that NTP client connects NTP server to acquire time.

1. The configuration instruction

Switch-2 is the referenced clock source in the network, switch-1 works in NTP client mode, switch-3 works in NTP active peer mode; switch-1 acquire time from switch-2; when switch-1 is synchronized, switch-3 acquire time from switch-1.

2. The topology

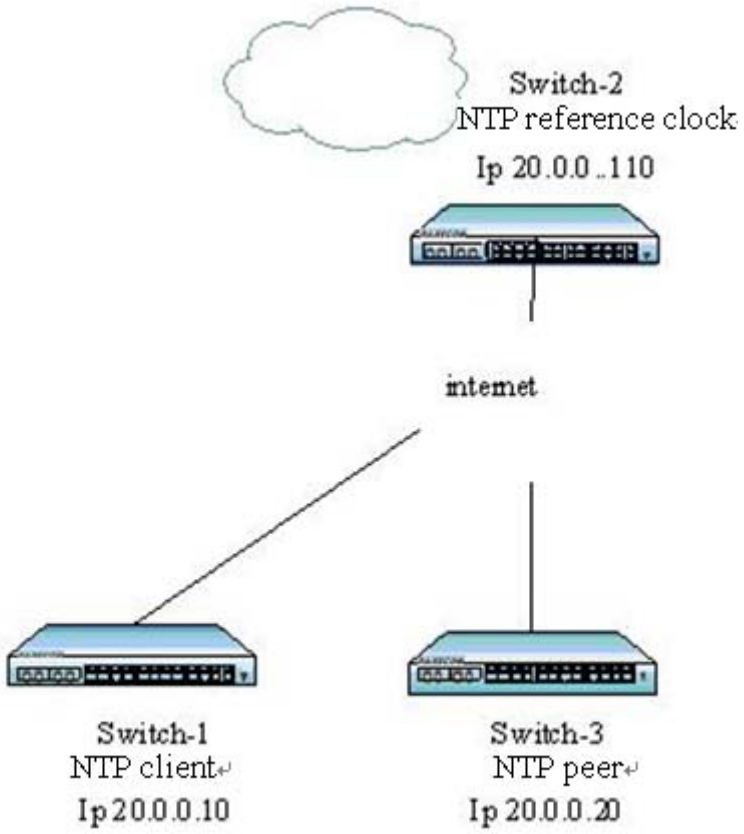


Fig 34-2 the topology of NTP acquiring time

3. The configuration steps:

[switch-2]

Raisecom(config)#**ntp refclock** *127.127.1.0 2*

Raisecom(config)#**interface ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.110 255.0.0.0 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**exit**

Raisecom#**show ntp status**

[switch-1]

Raisecom(config)#**interface ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.10 255.0.0.0 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**ntp server** *20.0.0.110* **version** *v3*

Raisecom#**show ntp associations**

Raisecom#**show ntp status**

[switch-3]

Raisecom(config)#**interface ip** *0*

Raisecom(config-ip)#**ip address** *20.0.0.20 255.0.0.0 1*

Raisecom(config-ip)#**exit**

Raisecom(config)#**ntp peer** *20.0.0.10* **version** *v3*

Raisecom#**show ntp associations**

Raisecom#**show ntp status**

Show the results:

[switch-1]

Raisecom#**show ntp associations**

Server(ip) refid stratum poll when delay offset dispersion mode reach

(s)20.0.0.110 127.127.1.0 2 9 59216 -1.065525 0.005769 0.000000 1 255

Raisecom#**show ntp status**

Clock status : synchronized

NTP peer : 20.0.0.110

NTP version : 3

NTP mode : ntpSlave

Leap : 0

Poll : 8

Stratum : 5

*Precision : 2**4*

Reference clock : 20.0.0.110

Reference time : cd6c8915.0c0d3480(Thu Mar 19 09:04:21.047 UTC 2009)

Current clock : cd6d6ee4.0c0d3480(Fri Mar 20 01:24:52.047 UTC 2009)

Root delay : -1.000009

Root dispersion : 0.001380

[switch-3]

Raisecom#**show ntp associations**

Server(ip) refid stratum poll when delay offset dispersion mode reach

(s)20.0.0.10 20.0.0.110 3 8 59216 -1.065525 0.005769 0.000000 1 255

Raisecom#**show ntp status**

Clock status : synchronized

NTP peer : 20.0.0.10

NTP version : 3

NTP mode : ntpSlave

Leap : 0

Poll : 8

Stratum : 4

*Precision : 2**4*

Reference clock : 20.0.0.10

Reference time : cd6c8915.0c0d3480(Thu Mar 19 09:04:21.047 UTC 2009)

Current clock : cd6d6ee4.0c0d3480(Fri Mar 20 01:24:52.047 UTC 2009)

Root delay : -1.00089

Root dispersion : 0.011380

34.1.5 NTP troubling shooting

When NTP client can not acquire time normally, it may be that NTP service is not enabled on the opposite end or network fault.

Chapter 35 Y.1731 Configuration

This chapter describes how to configure Y.1731 function, including the following:

- ✧ Functional overview of Y.1731
- ✧ Default configuration list of Y.1731
- ✧ Configuration guidance and restrictions of Y.1731
- ✧ Configuration list and itemized explanation ofY.1731
- ✧ Monitoring and maintenance of Y.1731
- ✧ Typical configuration examples of Y.1731

35.1 Overview

With the rapid development of Ethernet technology, Ethernet technology has been widely used in MAN and WAN. As the complexity of MAN and WAN network infrastructure, and the existence of abundant various users, usually require a number of different network operators to work together to provide end-to-end business customers, thus a higher demand bring forward for the Ethernet management maintenance and reliability. Traditional Ethernet has not carrier-managed capabilities, can not detect the second floor of a network failure. In order to achieve the same level of traditional carrier-class transport network service standards, for various research groups and organizations are actively engaged in technology research and standard-setting

IEEE and ITU-T work together to end-to-end business-class OAM technology research, providing a comprehensive OAM tool for carrier-class Ethernet OAM. ITU-Y.1731 proposal published by ITU-T divide Ethernet OAM into fault management and performance monitoring while IEEE802.1ag detailed technically, such as state machine of the fault management and MIB. RAISECOM provides fault management capabilities of compatible ITU-Y.1731 and IEEE802. 1ag standard, as well as performance monitoring function defined in Y.1731, which collectively referred to as functional Y.1731.

Fault Management CFM (Connectivity Fault Management), is an end-to-end business-class OAM protocol for active fault diagnosis of EVC (Ethernet Virtual Connection) for. Through fault management functions effectively reduce network maintenance costs and improve Ethernet maintainability. Fault management functions include end-to-end connectivity fault detection tools (CC) the provision of, end-to-end connectivity fault recognition tools (LB) and fault isolation tools (LT).

Performance Monitoring PM (Performance Monitor), is an end-to-end business-class OAM protocol, used for active performance monitoring of point-to-point EVC (Ethernet Virtual Connection). Through the utilization of performance monitoring functions to make active cycle monitoring on performance indicators, such as the frame loss rate from the local MEP to peer MEP, delay, delay jitter and so on, to promptly notify the user when statistical value of these indicators achieves pre-determined threshold value within a certain period. Performance monitoring functions help users take the initiative to monitoring network of the second floor of transmission quality, and identify problems early.
Fault management function and performance monitoring function collectively refer toY.1731 function.

35.1.1 Components of Y.1731

1. Maintenance Domain

Maintenance Domain is a network running 1731 function, which defines network scope of the OAM management. Level attributes in maintenance domain are divided into 8 (0 ~ 7), the bigger the higher, corresponding to the larger scope of maintenance domain. In the same VLAN scope, the different maintenance domains can be adjacent, nested, but not cross.

2. Service instance

Service Instance, also known as Maintenance Associations, corresponds to a business, can be mapped to a set of S-VLAN. A Maintenance Domain can be configured to several service instances, each service instance has dependency association to several S-VLAN, and VLAN in different dependency association can not be cross-linked. Although the service instances can be mapped to several VLAN, but only a VLAN in a service instance, used to transceiver OAM message, this VLAN is called main VLAN in VLAN instance, in short, service instances VLAN.

A service instance can be configured with several MEP, message sent by MEP in same service instance has same S-VLAN TAG, the same priorities and the same C-VLAN TAG, and MEP can receive OAM message send by other MEP e in same MA.

3. MEP

MEP (Maintenance associations End Point) is a management activity configured on edge of the service instance related to service instance, the most important activity entity in Y.1731. MEP can sent and processed CFM message, whereabouts of MEP service instances and maintenance domain determine VLAN sent by MEP and level. MEP cut-off messages in the same main VLAN at the same level self-closing or lower, and transmit message over its own high-level

4. MIP

MIP is a management activity entity configured within service instance, a MIP is component of 2 MHF (MIP Half Function). MIP can not take the initiative to send CFM message, but can handle and respond to LTM and LBM messages.

5. MP

MEP and MIP are called by a joint name MP.

35.1.2 Basic function of Y.1731

The realization of Y.1731 function based on he correct configuration of the maintenance domain, service instances, MEP and MIP, including the following 4 sub-functions:
Fault detection function (Continuity Check, CC)

Failure confirm functional (loop back, LB)

Fault isolation function (Link Trace, LT)

Performance Monitor function (Performance Monitor, PM)

1. **Fault detection function**

Fault detection function is the use of CC (Continuity Check) protocol to detect the connectivity of Ethernet virtual connection (EVC), to determine the connection status between MP. This function through MEP periodically sent CCM (Continuity Check Message) to achieve, other MEP in the same service instance

receive the message, which determine the status of the remote MEP. If equipment failure or the middle link configuration error, lead that MEP can not receive and process CCM sent by remote MEP. If the MEP did not receive remote CCM messages in 3.5 CCM interval cycle, the existence of that link failure, will in accordance with the alarm priority configuration to send fault alarm.

2. Failure confirm functional

Failure confirm function used to identify connected status of local facilities and remote equipment, this function via source MEP sent LBM (LoopBack Message) and the destination MP to respond to LBR (LoopBack Reply) to determine the connectivity between two MP. MEP send the MP with failure confirms to LBM, after the MP received a LBM message the, it sent 1 LBR to source MEP. If the source MEP received LBR, then confirm the path is connected. Otherwise, confirm the existence of connectivity failure. Failure confirm function function is similar to layer three ping, and therefore failure confirm function form as layer 2 ping in application

3. Fault isolation

Fault isolation is used to determine path from source MEP to the target MP. This function sent LTM through source MEP(Link Trace Message) to target MP, each bridge equipment configuration of LTM transmission path will respond to LTR (Link Trace Reply) to source MEP, reorganize through effective LTR and LTM by record, ultimately confirmed that the path between the MP. Fault isolation is similar to layer three traceroute functions, so in application it forms as Layer 2 traceroute.

4. Performance monitoring function

Performance monitoring function is used for cyclical active monitoring between the local MEP and upsize MEP, such as frame loss rate, delay, delay jitter performance indicators, when in a period the statistical value achieve the pre-set threshold to notice as alarm form

Performance monitoring function can have an actively periodic monitor of three indicators: frame loss rate, delay, and delay jitter indicators.
FLR (frame loss ratio) measurement function is used to carry out active and seasonal measure to the frame loss state between local MEP and peer MEP. The function use the counter values related to CCM frame loss to account the remote/local frame loss ratio between local and remote MEP. It is a two-end measure mode to use CCM measuring FLR, which is based on the precondition that CC function works well, if any end CC sending switch is disabled or if CCM can not receive messages normally, then FLR measurement function will not work.

Delay measurement function is used for active and seasonal measure to the delay between local MEP and peer MEP. It is realized by sending DDM (delay measurement message) from local MEP and returning DMR (delay measurement relay) from peer MEP, by accounting the one-way remote delay, one-way local delay, two-way out and home delay between local and per MEP according to the four time stamps in the message.

Delay jitter measurement function is used for active and seasonal measure to the delay change between local MEP and peer MEP, which is based on delay measure data.

CCM, LBM, LBR, LTM, LTR, DMM, DMR is called Y.1731 OAM message in total, OAM message in short.

Altogether, Y.1731 realizes OAM technology on end-to-end layer, which helps reduce service providers' operation coast and enhance their competition advantages.

35.2 Default configuration list of Y.1731

No.	Property	Default
1	Switch status of defaulted global function	OFF
2	Switch status of defaulted port function	ON
3	configuration status of defaulted maintenance domain	No maintenance domain
4	configuration status of defaulted service instance	No service instance
5	VLAN mapping of the defaulted service instance	No VLAN mapping
6	Example of the defaulteded VLAN mapping services	10 seconds
7	OAM message C-VLAN configuration of defaulted service instance	No C-VLAN
8	OAM massage priority of defaulted service instance	6
9	remote MEP learning switch of defaulted service instace	OFF
10	MEP aging time of defaulted dynamic remote	100min
11	static remote MEP of defaulted service instance	No static remote MEP
12	MEP configuration status of defaulted service instance	No MEP
13	configure status of defaulted MIP	No MIP
14	transmitting switch CCM status of defaulted MEP	OFF
15	data retention time of defaulted wrong CCM Database	100min
16	LT database switch by default	OFF
17	default LT database saving data time	100min
18	default LT database maximum saved data entry	when LT database is enabled, default max saved entry is 100; When it is disabled, default max saved entry is 0;
19	Default malfunction alarm level	Mac RemErrXcon, that is to say, the alarms of port down, remote loss, CCM error and crossover are supported
20	LBM send two ping the default number of	5
21	Default layer-2 PING data TLV length	64
22	Default layer-2 PING source MEP	Auto-search
23	Default layer-2 traceroute beginning TTL	64
24	Default layer-2 traceroute source MEP	Auto-search
25	Default performance monitoring pair	None
26	Default performance monitoring delay target	1000ms
27	Default performance monitoring delay jitter target	1000ms
28	Default performance monitoring frame loss ratio up-limit threshold	100%
29	Default performance monitoring frame	0

	loss ratio lower limit threshold	
30	Default performance monitoring delay up-limit threshold	100%
31	Default performance monitoring delay lower limit threshold	0
32	Default performance monitoring delay jitter up-limit threshold	100%
33	Default performance monitoring delay jitter lower limit threshold	0
34	Default performance monitoring switch	Disable
35	Default performance monitoring alarm switch	Disable
36	Default RFC2544 throughput measurement time-out time	5s
37	Default RFC2544 throughput measurement message length	256 bytes

35.3 CFM configuration constraints and limitations

1. Each device can be configured for 8-level (0-7) maintenance domain (MD); If you specify the maintenance domain names, the allowable string length of domain name is between 1-16 bytes;
2. The maximum number in service instance (MA) configured in each device exist differences in equipment, the details may refer to the list of equipment characteristics and other related document;
3. before delete the maintenance domain, user should delete all MEP of maintenance domain, otherwise deletion of the maintenance domain will lead to failure;
4. When configuring service instance, the allowed string length of MA Name is between 1-13 bytes;
5. Each service instance is mapped to 32 VLAN at most, use the smallest VLAN as master VLAN, MEP in service instance utilize master VLAN for OAM transmitting messages, non-master VLAN is not used for send and receive messages. In overall scope, VLAN mapping associations can not cross, otherwise will lead to the failure in service instance VLAN mapping
6. If the service instance has not yet been mapped to any VLAN, then configure the local MEP in service instance is not allowed
7. If the service instance has been configured MEP, disable delete and modify VLAN mapping of services instance
8. In accordance with standard protocols, CCM transmitting interval in service instance can configure seven kinds of cycle: 3.33 ms, 10ms, 100ms, 1s, 10s, 60s and 600s; later four kinds of time cycle for fault management and configuration, therefore the allowing cycle scope of equipment is 1s, 10s, 60s and 600s.
9. Before amending CCM transmitting interval, user need to close all CCM transmitting switch of MEP in services instance
10. Before delete the service instance user should delete all MEP in service instance, otherwise will lead to the failure of delete services instances;
11. maximum MEP of each device exist differences in equipment, the details may refer to the list of equipment characteristics and other related document
12. A performance monitoring pair can only be configured in 1 service instance;

13. If performance monitoring pair is not configured to the service instance, will lead to the failure of other related performance monitoring configuration, such as the configuration of delay performance monitoring target, target delay jitter, etc.;
14. Service instance performance monitoring function so that after the ban on other performance monitoring configuration commands, such as modifications delay the target detection performance, etc.
15. Upper limit threshold must be higher than the lower threshold in service instance; otherwise configuration will lead to failure.

35.4 CFM configuration list and itemized description

- The overall functional switches and ports functional switch
- Related entities configuration of Y.1731
  - Configure maintain domain MD
  - Configure service instance MA
  - Configure MEP
  - Configure a static remote MEP
  - Configure MIP
- Fault detection
  - Configure CCM transmitting switch
  - Configure CCM transmitting interval
  - Configure learning switch of remote MEP
  - Configure aging time of remote MEP
  - Configure customer VLAN of OAM message
  - Configure OAM message priority
  - Configure retention time of error CCM message
  - Configuration fault alarm level
- Failure confirm - the implementation of layer two ping operation
- Fault isolation
  - The implementation of layer2 traceroute operation
  - Configure switch status of database LT
  - Configure retention time of database LT
  - Configure preservable data entries of database LT
- .Performance Monitoring
  - Configure performance monitoring pair
  - Configure performance monitoring delay and delay jitter target
  - Configure threshold value of performance monitoring
  - Configuration alarm switch of performance monitoring
  - Configure performance monitoring switch
- Rfc2544 throughput measurement
  - Configure overtime of Rfc2544 throughput measurement
  - Start Rfc2544 throughput measuring

35.4.1. Configure overall functional switch of Y.1731

Disable defaulted Y.1731 overall function (Disable).

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ethernet cfm {enable | disable}**	Enable/diaable global functional switch
3	**exit**	Return to privileged user mode
4	**show ethernet cfm**	Show Y.1731 global configuration information

Functions of following example: in Global mode, enable the overall function switch

Raisecom#**config**

Raisecom(config)#**ethernet cfm enable**

Raisecom(config)#**exit**

⚠**Note:**
Although the command contains the keyword "cfm", the functional switch impact that whether CC, LB, LT, PM, RFC2544 take into force within the overall scope;

35.4.1. Configure ports functional switch of Y1731

When Y.1731 port switch function switch disable, MP configured on the port will not take into effect, OAM message of Y.1731 can not be transmitted on port. Enable defaulted functional switch of all ports (enable).

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface line/client** *port-id*	Enter specified *port-id* port mode
3	**ethernet cfm {enable | disable}**	Enable/disable port Y.1731 function
4	**exit**	Return to global configuration mode
5	**exit**	Return privilege mode
6	**show ethernet cfm**	Show Y.1731 overall configuration information

Functions of following example: enable Y.1731 function on ports 3:

Raisecom#**config**

Raisecom(config)#**interface line/client** *3*

Raisecom(config-port)#**ethernet cfm** *enable*

Note: Although the command contains the keyword "cfm", the functional switch impact that whether CC, LB, LT, PM, RFC2544 take into force within the overall scope.

35.4.2. Configure maintenance domain

When configuring maintenance domain, you must specify the level of domain maintenance. RAISECOM Y.1731 supports to configure maintenance domain of IEEE802.1ag style, and maintenance domain of ITU-T Y.1731 style. Name of maintenance domain parameter is optional parameters, if specify domain name , the maintenance domain is IEEE802.1ag style, all MA of maintenance domain is IEEE802.1ag style, MAID field sending CCM Message by all MEP of the maintenance utilize the format IEEE802.1ag; If you do not specify the maintenance domain names, maintenance domain is the ITU-T Y.1731 style, all service

instance of the maintenance domain is the ITU-T Y.1731 styles, MEGID field sending the CCM message by all MEP of the maintenance domain to use format ITU-T Y.1731.

Delete MD: **no ethernet cfm level** *level*

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ethernet cfm domain [md-name** *domain-name***] level** *level*	Configure maintenance domain *domain-name*: name of the maintenance domain, the string length: 1-16 bytes; *level:* the level of maintenance domain, range in: 0-7;
3	**exit**	Return to privileged user mode
4	**show ethernet cfm domain**	Show configuration information of maintenance domain

The function of following example:

Example 1: Configure maintenance domain of style IEEE802.1ag , name md3-1, level 3

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain md-name** *md3-1* **level** *3*

Raisecom(config)#**exit**

Example 2: Configure maintenance domain of ITU-T Y.1731-style, for the three-level

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**exit**

⚠**Note:**

- Level of Specified the maintenance domain can not be repeated, otherwise, will result in failure to configure maintenance domain;
- If user specify maintenance domain name, the maintenance domain name must be unique, otherwise will result in failure to configure maintenance domain;

35.4.3. Configure service instance

When configuring service instance, user need to specify the level of maintenance domain. Service instance name must meet the following requirements: (maintenance domain name, service instance name) composed string is unique in the global scope. If service instance configuration succeeds or already exists, user will enter service instance mode, which is the most important mode of Y.1731 function configuration.

Delete service instance: **no service** *service-instance* **level** *level-id*。

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service** *service-instance* **level** *level*	Create service instance and s to enter the service instance model. *service-instance:* name in service instance,

		the length of 1-13 bytes; *level*: the range of maintenance domain level: 0-7;
3	**exit**	Return to global configuration mode
4	**exit**	Return to privileged user mode
5	**show ethernet cfm domain**	Shows maintenance domain and configuration information in service instance.

Function of following example: Configure the service instance of name ma3-1-4 in a 3-level maintenance domain

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**exit**

Raisecom(config)**#exit**

⚠**Note:**

- If there is no same maintenance domain in specified level, the configuration of the service instance will lead to failure;
- If name of the maintenance domain + name in service instance composed string is not unique, will lead to the failure of MA configuration;
- If configuration in service instance reach the maximum, configuration in service instance will lead to failure

35.4.4. Configure VLAN mapping in service instance

When configuration in service instance is mapped to a VLAN list, VLAN list allows a maximum of 32 VLAN, in VLAN list smallest VLAN is main VLAN in service instance. All MEP in service instance send and receive packets through the main VLAN, not-main VLAN is not used to transceiver packets.

Service instance is mapped to a group of VLAN, namely the VLAN in VLAN list is fully equivalent, as use VLAN for the main transceiver package, which all non-master VLAN in the list is mapped to the master VLAN in logic. This logical VLAN mapping is global and VLAN mapping association of different service instance can be the same, but you can not cross.

The following is illegal:

Counter-Example 1: When service instance ma3-1-1 related to VLAN 10-20 and service instance ma3-1-2 mapping VLAN 15-30. VLAN 16-20 have been mapped repeattly to the master VLAN 10 and the master VLAN 15;

Counter-example 2: When service instance ma3-1-3 mapped to the VLAN 100-120 and service instance ma3-1-4 mapped to the VLAN 90-100, master VLAN 100-120 is mapping to master VLAN 100, then VLAN 100 is mapped to VLAN 90.

Counter-example 3: service instance ma3-1-5 in maintenance domain of Level 3 map to the VLAN 10-20, level 3 of the other service instance in maintenance domain of Level 3 also map to VLAN10-20, used the same master VLAN.

The following is legal:

Positive Example 1: service instance ma3-1-5 in maintenance domain of Level 3 map to VLAN 10-20, Level 5, services ma5-1-1 in maintenance domain of Level 5 map to the VLAN 10-20.

Delete service instance: **no service vlan-list**

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance:* name in service instance, the length of 1-13 bytes; *level*: the range of maintenance domain level: 0-7;
3	**service vlan-list** *vlan-list*	*vlan-list:* vlan list, range in 1-4094;
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm domain**	Shows maintenance domain and configuration information in service instance

Functions of following example: Configure VLAN mapping relation in the service instance ma3-1-4

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *10-25*

Raisecom(config)#**exit**

⚠**Note:**

- If the number of VLAN in VLAN list is more than 32, it will lead to the failure of VLAN mapping;
- If VLAN mapping is cross to VLAN mapping of other service instance, VLAN mapping fail;
- If same VLAN mapping exists in the same services instance, VLAN mapping will lead to the failure;
- If a service instance has been mapping the VLAN, user must delete the VLAN mapping relations before in order to configure a new VLAN mapping;
- If the service instance has been configured MEP, user should first delete the MEP, and then delete the VLAN mapping relation

35.4.5. Configure MEP

Before configuring MEP, user should configure maintenance domain first, then and domain configure service instances in the maintenance domain, and map VLAN in service instance. the direction of MEP currently configured only support the UP, if the command is not specified, the default direction is UP.

Delete designated MEP: **no service mep** *mepid*

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance:* name in service instance,

		the length of 1-13 bytes; *level:* the range of maintenance domain level: 0-7;
3	**service mep** [**up**] **mpid** *mepid* {**port** *port-id* | **line** *line-id* |**client** *client-id* }	Configure MEP in service instance *up:*up-bound MEP mepid:MEPID; port-id:Port ID, value 1 to the largest port ID; *line-id:*Line port ID, value 1 to the largest line port ID; *client-id:*Client port ID, value 1 to the largest Client port ID;
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm local-mep**	Shows maintenance domain and configuration information in service instance

Functions of following example: Configure MEP in the service instance, port 1

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain leve**l *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *10-45*

Raisecom(config-service)#**service mep up mpid 100 port** *1*

Raisecom(config)#**exit**

⚠**Note:**

- If the service instance is not mapped VLAN, will lead to the failure of MEP configuration;
- If specified port already exists MEP in the current service instance, will lead to the failure of MEP configuration;
- If the maximum number of MEP configured in the device has already reached the ceiling, will lead to the failure of MEP configuration
- If the local MEP static or remote MEP of MEPID already exists in the service instance, will lead to the failure of MEP configuration;

35.4.6. Configure a static remote MEP

There is a MEP list in each service instance, which saves all the MEP information in the service instance, including: local MEP, static remote MEP, and dynamic remote MEP. User can use show **ethernet cfm mep level** *level* **service** *service-name* to show all the MEP information under service instance. Local MEP and static remote MEP should be created through management plane, dynamic remote MEP should be created by control plane. When you configure static remote MEP, the dynamic remote MEP of the same MEPID will be covered.

Before configuring static remote MEP, you should configure maintaining domain first, and configure service instance in the maintaining domain. MAC address is optical.

When MEP receives CCM, if the remote MEP that has the same MEPID with CCM can not be found in service instance MEP list (including static remote MEP and dynamic remote MEP), then MEP will take it as

unforeseen CCM.

When MEP receives CCM, if the remote MEP that has the same MEPID with CCM can be found in the service instance MEP list, while static remote MEP has been configured MAC address, then it is needed to compare CCM source MAC address and static remote MEP MAC address. If the result is that the MAC addresses do not match, then MEP will report level 4 CCM fault, and decide if it is needed to send fault alarm according to the alarm level.

Delete the specified static remote MEP:**no service remote mep** *mepid*

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance:* name in service instance, the length of 1-13 bytes; *level:* the range of maintenance domain level: 0-7;
3	**service remote mep mpid** *mepid* **[mac** *ABCD.ABCD.ABCD***]**	Configure static remote MEP。 *mepid*:MEPID, range in 1-8191; *ABCD.ABCD.ABCD*: MAC address; remote MEP
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm mep level** *level* **service** *service-instance*	Show MEP configuration in service instance *level*: range in 0-7 *service-instance*: name of servise instance

Function of following examples: Configure a static remote MEP in service instance, and specify the MAC address of the remote MEP

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service remote mep mpid** *100* **mac** *000e.5e03.5318*

Raisecom(config)#**exit**

35.4.7. Configue MIP

Before configuring MIP, configure MD of the same level. A port can only configure a MIP, the MIP configured after will cover the MIP. configured before.

Delete MIP: no ethernet cfm mip level *level*

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface line/client** *port-id* **Or interface line** *line-id*	Enter port ID *port-id:* Port ID, value 1 to the largest port ID;

	Or interface client *client-id*	*line-id:* Line port ID, value 1 to the largest line port ID; *client-id:* Client port ID, value 1 to the largest Client port ID;
3	**ethernet cfm mip level** *level*	Configure specified MIP *level*: level of maintenance domain 1-7;
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm local-mp**	Show configuration information of local MP , contains MEP and MIP

Functions of the following example: Configure mip of the level of 5 in port 5

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain leve**l *5*

Raisecom(config)#**interface line/client** *5*

Raisecom(config-port)#**ethernet cfm mip level** *5*

35.4.8. Configure transmitting switch CCM

Configure transmitting switch CCM. When transmitting switch CCM of MEP is turned off, disable MEP transmit CCM. MEP message is by default, disable to transmit CCM message.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance:* name in service instance, the length of 1-13 bytes; *level:* the range of maintenance domain level: 0-7;
2	**service cc {enable | disable} mep {***mepid-list* **|all}**	Enable or disable CCM sent byMEP *mepid-list*: MEPID list, range in1-8191; **all**: all configured MEP;
3	**exit**	Return to privileged user mode
4	**show ethernet cfm local-mp**	Show configuration information of local MP.

Functions of the following example: Enable CCM transmitting switch of MEP 1 in the service instance ma3-1-4

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain md3-1 level** *3*

Raisecom(config)#**service ma3-1-4 vlan** *4*

Raisecom(config-service)#**service cc** *enable* **mep** *1*

Raisecom(config- service)#**exit**

Raisecom(config)#**exit**

Note: as a result of the frame loss rate measurements in performance monitoring need calculate by CCM,

so close the CCM transmitting function of MEP in the performance monitoring pair will affect the normal operation of frame loss rate.

35.4.9. Configure CCM transmitting intervel

By default, CCM transmitting interval in service instance is 10 seconds. If the service instance of the existence of CCM switch send by MEP enable, then configure and modify CC transmitting interval do not allowed.

Restoration the default values of CCM message transmitting interval in specified service instance: **no service cc interval**

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance:* name in service instance, the length of 1-13 bytes; *level:* the range of maintenance domain level: 0-7;
3	**service cc interval {1 | 10 |60 |600}**	Configure CCM transmitting interval in service instance. Unit: seconds
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm domain**	Show configuration information of maintenance domain and service instance

Functions of the following example: Set transmitting interval in service instance as 60 seconds

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain md3-1 leve**l *3*

Raisecom(config)#**service ma3-1-4 vlan** *4*

Raisecom(config-service)#**service cc interval** *60*

Raisecom(config- service)#**exit**

Raisecom(config)#**exit**

Note: In order to prevent a large number of MEP inner service instance report CCM error fault at the same time as a result of modifications of CCM transmitting interval. Before configure CCM transmitting interval in service instance, user need to close CCM transmitting switch of MEP in the service instance, otherwise will lead to the failure of CCM transmitting interval configuration, we strongly recommended that before the revision of the CCM transmitting interval, shutdown CCM transmitting switch of all MEP in all the current network equipment, and then amend the CCM transmitting interval.

35.4.10. Configuration remote learning switch

By default, the remote MEP learning function disable, namely if MEP in service instance receive non-expected CCM (see section 1.4.7) it will be reported for the 4-level error CCM failure, and in accordance with fault alarm of the level configuration determine whether to send alarm.

If the remote learning switch MEP in the service instance enable, after MEP receive on- expected CCM, it will create a dynamic remote MEP in the MEP list in service instance to and save the corresponding information of the remote MEP. When receive the same CCM of MEPID once again, CCM has been able to normal.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance:* name in service instance, the length of 1-13 bytes; *level:* the range of maintenance domain level: 0-7;
3	**service remote mep learning {enable | disable}**	Configure rermote MEP learning switch
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm domain**	Show configuration information of local MD and MA

Functions of following example: Enable remote MEP learning switch

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain md3-1 leve**l *3*

Raisecom(config)#**service ma3-1-4 vlan** *4*

Raisecom(config-service)#**service remote mep learning** *enable*

Raisecom(config- service)#**exit**

Raisecom(config)#**exit**

35.4.11. Configure the remote MEP aging time

By default, the remote MEP aging time is 100 minutes.

To restore aging time by default: no ethernet cfm remote mep age-time

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**ethernet cfm remote mep age-time** *minutes*	Configure MEP aging time *minutes*: range in1-65535,unit;min
3	**exit**	Return to privileged user mode
4	**show ethernet cfm**	Show the global configuration mode

Functions of the following example: Configure remote MEP aging time for 101 minutes

Raisecom#**config**

Raisecom(config)# **ethernet cfm remote mep age-time** *101*

Raisecom(config)#**exit**

35.4.12. Configure Client VLAN of Y.1731 OAM message

Defaulted Y.1731 OAM message does not carry C-TAG, when the service instance to configure service instance after CVLAN all MEP sent CCM, LTM, LBM, DMM will use dual-TAG, C-TAG use configuration CVLAN.

Delete Client VLAN of Y.1731 OAM message

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mod *service-instance*: name in service instance length:1-13 bytes; *level*: level of maintenance domain
3	**service cvlan** *vlan*	Configure client vlan of OAM message *vlan*: client VLAN, range in 1-4094
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm domain**	Show configuration information C and service instance

Functions of the following example: Set client VLAN of Y.1731 OAM message for 1001

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain md3-1 level** *3*

Raisecom(config)#**service ma3-1-4 vlan** *4*

Raisecom(config-service)#**service cvlan** *1001*

Raisecom(config- service)#**exit**

Raisecom(config)**#exit**

35.4.13. Configure priority of Y.1731OAMmessage

Defaulted priority of Y.1731 OAM message is 6, after configuring OAM message priority, CCM, LBM, LTM, DMM sent by all MEP message in service instance use the specified priority.

Delete Client VLAN of Y.1731 OAM message: **no service priority**

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mod *service-instance*: name in service instance length:1-13 bytes; *level*: level of maintenance domain
3	**service priority** *priority*	Configure priority of OAM message *priority*: priority ,value 0-7
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm domain**	Show configuration information of maintenance domain and service instance

Functions of the following example: Set the Priority of Y.1731 OAM Message as 2

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain md3-1 level** *3*

Raisecom(config)#**service ma3-1-4 vlan** *4*

Raisecom(config-service)#**service priority** *2*

Raisecom(config- service)**#exit**

Raisecom(config)#**exit**

Note:

- Message types of OAM message in type CCM, LTM, LBM, DMM of Y.1731 use service instance to configure priority; but for OAM message in type LBR, LTR, and DMR the message priority is consistent with LBM, LTM, DMM message received.
- Please pay attention to trust configuration of port COS, this configuration impact on priority of the OAM message, and may modify the priority of OAM message;

35.4.14. Configure retention time error CCM database

Error CCM database is used to save fault information reported by all MEP in the equipment Each record of CCM error information record created time of the error message, use the command does not change the created time of error CCM messages. When the system configures new retention time will immediately check data in the database, if there is data beyond time will be immediately removed. By default, retention time of error CCM time in CC database is 100 minutes.

To restore the retention time of error CCM data: **no ethernet cfm error archive-hold-time**

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**ethernet cfm error archive-hold-time** *minutes*	Configure retention time of error CCM message *minutes*: retention time(min), range in1-65535
3	**exit**	Return to privileged user mode
4	**show ethernet cfm**	Show relative information of cfm

Functions of the following example: Set the retention time of error CCM database as 50

Raisecom#**config**

Raisecom(config)#**ethernet cfm error archive-hold-time** *50*

Raisecom(config)#**exit**

35.4.15. Configure CFM fault alarm level

CC function of Y.1731 can detect five-level of the fault, in accordance with the order of descending order: 5 -cross-connect faults, 4-CCM error fault, 3-Remote MEP loss fault, 2-port state fault and 1-RDI fault. Configure all five types of alarm allowed transmitting

Configure four kinds of fault: cross-connect fault allowed by macRemErrXco, CCM error fault, remote MEP loss fails, the port state fault, namely types of transmitting alarms 2-5;

Configure three kinds of fault: cross-connect fault allowed by remErrXcon, CCM error fault, namely types of transmitting alarms 4-5;

Configure a kind of fault: cross-connect fault allowed by xcon, CCM error fault, namely types of only transmitting alarms 5;

Configure **None** does not transmit any alarm.
Default state is macRemErrXcon.
Restoration types of the transmitting alarm: **no snmp-server cfm-trap**

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance*: name in service instance, length 1-13 bytes; *level*: Configuration C-level fault alarm
3	**snmp-server trap cfm {all| macRemErr | remErr | ccmErr | xcon | none} mep {***mepid-list***|all}**	Configuration C-level fault alarm **all :** enable alarm all **macRemErr:** enable alarm of 2-5; **remErr:** enable alarm of 3-5; **ccmErr:** enable alarm of 4-5; **Xcon:** enable alarm of level 5; **None:** alarm disable; *mepid-list:* meplist, range in1-8191
3	**exit**	Return to privileged user mode
4	**show ethernet cfm local-mp**	Show configuration information of local MP

The following example functions: Set fault alarm level is all:

Raisecom(config-service)#**snmp-server trap cfm all mep** *all*

Raisecom(config-service)#**exit**

⚠**Note:**

- When the MEP detect fault, before troubleshooting, fault detection of MEP at the same level or low-level will not be re-generated;
- When MEP detect a fault, after a post-10s of troubleshooting, fault can be removed;

35.4.16. Execute layer-2 PING operation (fault reset)

Before executing the command, you must make sure that Y.1731 global function switch is enabled, or the operation will fail.

If it is to do layer-2 PING to designated MEPID, Y.1731 needs to find destination MEP MAC address using MEPID, there are two way provided:

firstly, use MEP list, find remote MEP MAC address according to MEP ID, if static remote MEP is found while user has not configured remote MEP MAC address, then the search fails;

secondly, use remote MEP database, when source MEP finds remote MEP and is stable, it will save remote MEP data to remote MEP database in MEP, and find remote MEP MAC from remote MEP database

according to MEPID;

Y.1731 will use 1 as the first choice, the way will continue providing layer-2 PING when CC function does not take effect.

By default LBM sending number is 5, default message TLV length is 64, one available source MEP will found automatically.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *Service-instance:* service instance name, the length is 1-13 bytes; *Level:* maintaining domain level;
3	**ping** {*ABCD.ABCD.ABCD* | **mep** *rmepid* } **[count** *count***]** **[size** *size***]** **[source** *mepid***]**	Execute layer-2 PING, used for fault reset *ABCD.ABCD.ABCD*: remote MP MAC address, valid unicast address *Mepid*: remote MEP ID, range is 1-8191 *Count*: LBM sending number, range is 1024 *Size*: data TLV length, range is 1484 *Mepid*: source MEPID, range is 8191
3	**exit**	Return to global configuration mode
4	**exit**	Return to privileged EXEC mode

Functions of following example:

Raisecom#config

Raisecom(config)#**ethernet cfm** *enable*

Raisecom(config)#**ethernet cfm domain md-name md***3-1* **level** *3*

Raisecom (config)#**service ma***3-1-4* **level** *3*

Raisecom (config-service)#**ping** *000E.5E03.5318* **size** *512*

Sending 5 ethernet cfm loopback messages to 000E.5E03.5318, timeout is 2.5 seconds:

!!!!!

Success rate is 100 percent (5/5).

Ping statistics from 000E.5E03.5318:

Received loopback replys: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

Raisecom (config-service)#**exit**

⚠Note:

- If MEP is not configured in service instance, it will lead to PING failure because there is no source MEP;
- If the designated source MEP fails it will lead to PING failure, for example the designated source MEP does not exist or the designated MEP located Y.1731 function is disabled;
- If designated destination MEPID operates PING, it will fail because of the MAC address that can not find destination MEP according to MEPID;
- If CC function does not take effect, by configuring static remote MEP and

designate MAC address, you can make sure that layer-2 PING operation can be used normally;

- If other user is using designated source MEP to execute PING it may cause operation failure

35.4.17. Execute layer-2 traceroute operation (fault isolation)

Before executing the command, you must make sure that Y.1731 global function is enabled, or it may cause execution failure.

When designating destination MEPID for layer-2 traceroute operation, Y.1731 needs to find destination MEP MAC through MEPID, Y.1731 provides two ways:

firstly, use MEP list to find remote MEP MAC address according to MEPID, if static remote MEP is found while static remote MEP MAC address is not configured by user, or the search fails;

secondly, use remote MEP database to do the searching, when source find remote MEP and keeps steady, it will save remote MEP data to remote MEP database, and find remote MEP MAC according to MEPID from remote MEP database;

Y.1731 takes way 1 as the first choice, which supports layer-2 traceroute when CC function is not available.

By default the original TTL of sending LTM is 64, and one available source MEP will be found.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *Service-instance*: service instance name, length is 1-13 bytes; *Level*: maintaining domain level;
3	**traceroute** {*ABCD.ABCD.ABCD* | **mep** *rmepid*} **[ttl** *ttl***]** **[source** *mepid***]**	Execute layer-2 function, used for fault isolation. *ABCD.ABCD.ABCD*: remote MP MAC address; *Rmepid*: remote MEPID, range is 1-8191; *Ttl*: original TTL, range is 1-255; *Mepid*: source MEPID, range is 1-8191
3	**exit**	Return to global configuration mode
4	**exit**	Return to privileged EXEC mode

Functions of following example:

Raisecom#**config**

Raisecom(config)#**ethernet cfm** *enable*

Raisecom(config)#ethernet cfm domain md-name md3-1 level *3*

Raisecom (config)#**service ma***3-1-4* **level** *3*

Raisecom (config-service)#**traceroute** *000E.5E03.5318 ttl 128*

Results:

TTL: <128>

Tracing the route to 000E.5E03.5318 on domain <md3-1>, level <3>, VLAN <4>.

Traceroute send via port <port-id>.

Hops HostMAC Ingress/EgressPort IsForwarded RelayAction NextHop

---

<1> *<AAAA>* ***<8/1>*** *<yes>* *<**RlyFDB**>* *<AAAA>*

<2> *<AAAA>* ***<2/3>*** *<yes>* *<**RlyFDB**>* *<BBBB>*

!**<3>* *<BBBB>* ***<-/9> *<no>* *<**RlyHit**>* *<CCCC>*

⚠Note:

- If there is no configured MEP in service instance, it may lead to traceroute operation failure because source MEP is not found;
- If the designated source MEP is invalid it may lead to traceroute operation failure, for example, the designated source MEP does not exist or the port that the designated source MEP lays in is shut down;
- If the designated destination MEPID execute traceroute, if you can not find destination MEP MAC address according to MEPID, it may lead to operation failure;
- If CC function fails, by configuring static remote MEP and designate MAC address, layer-2 traceroute can be made sure available;
- If any other user traceroute the designated source MEP it may lead to operation failure;

35.4.18. Configuration switch state of database LT

When the database LT switch is in the enabled state, traceroute information found by the agreement of database LT cache, you can keep track to command **show ethernet cfm traceroute cache**

When the database LT switch is turned off, user can not see the traceroute to discover information of command **show ethernet cfm traceroute-cache**

The default is off.

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**ethernet cfm traceroute cache {enable | disable}**	Configure switch status of database LT
3	**exit**	Return to privileged user mode
4	**show ethernet cfm traceroute-cache**	Show discovery information of traceroute

Functions of the following example: After start of database LT, user can view data information

Raisecom#**config**

Raisecom(config)#**ethernet cfm traceroute cache enable**

Raisecom(config)#**exit**

Raisecom#**show ethernet cfm traceroute-cache**

Note: When database LT is closed, operation of 2-layer traceroute can still be carried out, but the traceroute results will be deleted automatically after the implementation of the traceroute.

35.4.19. Configure data retention time of database LT

When database LT switch is turned on, user can configure retention time of the database. Retention time by default is 100 minutes.

Restore data retention time of database by default: **no ethernet cfm traceroute cache hold-time**

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**ethernet cfm traceroute cache enable**	Enable database LT switch
3	**ethernet cfm traceroute cache hold-time** *minutes*	retention time of the database LT *minutes*: retention time, unit: min, range in1-65535;
4	**exit**	Return to privileged user mode
5	**show ethernet cfm traceroute-cache**	Show data information

Functions of the following example: After the database enable, set retention time for 1000 minutes

Raisecom#**config**

Raisecom(config)#**ethernet cfm traceroute cache** *enable*

Raisecom(config)#**ethernet cfm traceroute cache hold-time** *1000*

Raisecom(config)#**exit**

Raisecom(config)#**show ethernet cfm traceroute-cache**

35.4.20. Configure data entries can be stored in database LT

When the database LT switch enable, user can configure data entries can be stored in database LT. When the database LT switch is turned on, defaulted stored number is 100; when the database LT switch is closed, defaulted entries can be stored is 0.

Restore default values of entries can be stored in database: **no ethernet cfm traceroute cache size**

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**ethernet cfm traceroute cache enable**	Enable database LT
3	**ethernet cfm traceroute cache size** *entrys*	Configure entries can be stored *entrys*: entries can be stored in datebase *entrys*: range in 1-512
4	**exit**	Return to global configuration mode
5	**show ethernet cfm traceroute-cache**	Show data information

Functions of the following example: After the database enable, configure entries can be stored as 150

Raisecom#**config**

Raisecom(config)#**ethernet cfm traceroute cache** *enable*

Raisecom(config)#**ethernet cfm traceroute cache size** *150*

Raisecom(config)#**exit**

35.4.21. Configure performance monitoring pair

Configure performance monitoring pair; specify a local MEP and a remote MEP in the service instance to establish the relationship of point-to-point performance monitoring. This configuration just describes a correspondence from point to point, but the performance monitoring has not yet formally entered into force, user need to perform the **service performance-monitor enable** to start performance monitoring.
Delete command of performance monitoring pair: **no service performance-monitor**

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance*: name in service instance,length:1-13 bytes *level*: level of maintenance domain
3	**service performance-monitor remote** *rmepid* **source** *mepid*	*rmepid*: remote MEPID, range in 1-8191; *mepid*: local MEPID, range in 1-8191;
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm performance-monitor information level** *level* **service** *service-instance*	Show configuration information of performance monitoring *level*: level of maintenance domain *service-instance*: name in service instance,length:1-13 bytes

Functions of the following example: Configure performance monitoring pair in service instance

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *10-45*

Raisecom(config-service)#**service mep up mpid** *100* **port** *1*

Raisecom(config-service)#**service performance-monitor remote** *200* **source** *100*

Raisecom(config)#**exit**

⚠**Note:**

- If specified source MEP does not exist, it will result in configuration failure;
- Only one performance monitoring is able to configure in a service instance to;
- If performance monitoring switch has started in the service instance, it will result in configuration failure;

35.4.22. Configure delay target of performance monitoring

When measuring delay of performance monitoring, each effective data of delay calculated by source MEP, compare the measured data to delay target, respectively, count date of higher than the delay target and date of lower than the delay target, after a 15-minute cycle, if ratio of the number of the target higher than delay and total delay reach pre-configured threshold of the upper limit or lower-limit threshold, transmitting alarm message.

Restore delay of performance monitoring target as default value: **no service performance-monitor delay object**

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance*: name in service instance,length:1-13 bytes *level*: level of maintenance domain
3	**service performance-monitor delay object** *object*	Configure delay target of performance monitoring *object*: delay target, range in 1-1000, unit milliseconds
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm performance-monitor information level** *level* **service** *service-instance*	Show configuration information of performance monitoring *level*: level of maintenance domain *service-instance*: name in service instance,length:1-13 bytes

Functions of the following example: Configure delay target of performance monitoring in service instance as 100 milliseconds

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *10-45*

Raisecom(config-service)#**service mep up mpid 100 port** *1*

Raisecom(config-service)#**service performance-monitor remote 200 source** *100*

Raisecom(config-service)#**service performance-monitor delay-variation object** *100*

Raisecom(config-service)#**exit**

⚠Note:

- Delay target configured by this command refers to one-way delay jitter target, that is, compare the remote delay jitter to the configuration target, if higher than the target, the number of the remote delay jitter higher than the target plus 1. Otherwise, the number of the remote delay jitter lower than the target number plus 1; compare delay jitter of local end to the configuration target, if the target is higher than the target, number of delay jitter in local end higher than the target plus 1, or number of delay jitter in local end lower than the target plus 1; compare round-trip delay jitter to 2 times configure target delay, if higher than 2 times target, the number of round-trip delay jitter higher than target plus 1, or

the number of round-trip delay jitter lower than target plus 1

35.4.23. Configure delay jitter target of performance monitoring

When measuring delay jitter of performance monitoring, each effective data of delay jitter calculated by source MEP, compare the measured data to delay jitter target, respectively, count date of higher than the delay jitter target and date of lower than the delay jitter target, after a 15-minute cycle, if ratio of the number of the target higher than delay jitter and total delay jitter reach pre-configured threshold of the upper limit or lower-limit threshold, transmitting alarm message.

Restore delay jitter of performance monitoring target as default value: **no service performance-monitor delay-variation object**

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance*: name in service instance,length:1-13 bytes *level*: level of maintenance domain
3	**service performance-monitor delay-variation object** *object*	Configure delay jitter of performance monitoring *object*: delay target, range in 1-1000, unit milliseconds
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm performance-monitor information level** *level* **service** *service-instance*	Show configuration information of performance monitoring *level*: level of maintenance domain *service-instance*: name in service instance,length:1-13 bytes

Functions of the following example: Configure delay jitter of performance monitoring in service instance as 100 milliseconds

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *10-45*

Raisecom(config-service)#**service mep up mpid** *100* **port** *1*

Raisecom(config-service)#**service performance-monitor remote** *200* **source** *100*

Raisecom(config-service)#**service performance-monitor delay-variation object** *100*

Raisecom(config-service)#**exit**

Note:

- Delay target configured by this command refers to one-way delay jitter target, that is, compare the remote delay jitter to the configuration target, if higher than the target, the number of the remote delay jitter higher than the target plus 1. Otherwise, the number of the remote delay jitter lower than the target number plus 1; compare delay jitter of local end to the configuration target, if the target is higher than the target, number of delay jitter in local end higher than the target plus 1, or number of delay jitter in local end lower than the target plus 1; compare round-trip delay jitter to 2 times configure target delay, if higher than 2 times target, the number of round-trip delay jitter higher than target plus 1, or the number of round-trip delay jitter lower than target plus 1

35.4.24. Configure performance monitoring threshold

Measurement of performance monitoring, after a 15-minute cycle, compare respective upper limit and lower limit of the measured frame loss rate statistics, the ratio of delay jitter higher than the target ratio and the ratio of delay jitter higher than the target ratio with. If the statistical ratio is higher or equal to upper limit threshold, the upper limit alarm will be decided whether to transmit based on performance monitoring alarm switch, if the statistical ratio is lower than the lower limit threshold, the lower limit alarm will be decided whether to transmit in accordance with performance monitoring alarm switch

Restore thresholds of performance monitoring to the default values: **no service performance-monitor (frame-loss-ratio | delay | delay-variation) (rising-threshold | failing-threshold)**

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance*: name in service instance,length:1-13 bytes *level*: level of maintenance domain
3	**service performance-monitor (frame-loss-ratio | delay | delay-variation) (rising-threshold | failing-threshold)** *threshold*	Configure thresholds of performance monitoring *threshold*: 0 – stand for 0 1 –stand for 0.1% 2 –stand for 0.2% 3 –stand for 0.5% 4 –stand for 1% 5 –stand for 2% 6 –stand for 5% 7 –stand for 100%
4	**exit**	Return to global configuration mode
4	**exit**	Return to privileged user mode
5	**show ethernet cfm performance-monitor information level** *level* **service** *service-instance*	Show configuration information of performance monitoring *level*: level of maintenance domain *service-instance*: name in service instance,length:1-13 bytes

Functions of the following example: Configure frame loss ratio of performance monitoring in service instance as %1

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *10-45*

Raisecom(config-service)#**service mep up mpid 100 port** *1*

Raisecom(config-service)#**service performance-monitor remote 200 source** *100*

Raisecom(config-service)#**service performance-monitor frame-loss-ratio rising-threshold** *4*

Raisecom(config-service)#**exit**

Note: If threshold value of the configured upper limit below the lower limit threshold, it will result in configuration failure.

35.4.25. Configure alarm switch of Performance Monitoring

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance*: name in service instance,length:1-13 bytes *level*: level of maintenance domain
3	**snmp-server trap performance-monitor {enable|disable}**	Configure alarm switch of Performance Monitoringdisable
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm performance-monitor information level** *level* **service** *service-instance*	Show configuration information of performance monitoring *level*: level of maintenance domain *service-instance*: name in service instance,length:1-13 bytes

Functions of the following example: Enable alarm switch of Performance monitoring in service instance

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *10-45*

Raisecom(config-service)#**service mep up mpid 100 port** *1*

Raisecom(config-service)#**snmp-server trap performance-monitor** *{enable | disable}*

Raisecom(config-service)#**exit**

35.4.26. Configure switch status of performance monitoring

Enable or disable performance monitoring in service instance, once enable, configuration of parameters related to performance monitoring disable, for example: delete performance monitoring disable, configure

performance monitoring target disable, thresholds and other performance parameters threshold.

If performance monitoring pair is not configured in the service instance, fail to open switch of performance monitoring.

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance*: name in service instance,length:1-13 bytes *level*: level of maintenance domain
3	**service performance-monitor {enable | disable}**	Configure switch status of performance monitoring
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm performance-monitor information level** *level* **service** *service-instance*	Show configuration information of performance monitoring *level*: level of maintenance domain *service-instance*: name in service instance,length:1-13 bytes

Functions of the following example: Enable switch status of performance monitoring in service instance

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *10-45*

Raisecom(config-service)#**service mep up mpid 100 port** *1*

Raisecom(config-service)#**service performance-monitor remote 200 source** *100*

Raisecom(config-service)#**service performance-monitor** *enable*

Raisecom(config)#**exit**

35.4.27. Configure overtime of Rfc2544 throughput measurement

Configure overtime of rfc2544 throughput measurement, if the measurement of rfc2544 in the overtime period did not receive information on peer MEP, measurement of rfc2544 will automatically stop.

If performance monitoring pair is not configured in service instance, fail to open switch of performance monitoring.

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance*: name in service instance,length:1-13 bytes *level*: level of maintenance domain
3	**service performance-monitor throughput timeout** *seconds*	*Seconds :* overtime, range in2-30, unit:second
4	**exit**	Return to global configuration mode

5	**exit**	Return to privileged user mode
6	**show ethernet cfm performance-monitor information level** *level* **service** *service-instance*	Show configuration information of performance monitoring *level*: level of maintenance domain *service-instance*: name in service instance,length:1-13 bytes

Functions of the following examples: Configure overtime of rfc2544in the service instance as 20 seconds.

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *10-45*

Raisecom(config-service)#**service mep up mpid** *100* **port** *1*

Raisecom(config-service)#**service performance-monitor remote** *200* **source** *100*

Raisecom(config-service)#**service performance-monitor throughput timeout** *20*

Raisecom(config)#**exit**

35.4.28. Start rfc2544 throughput measurement

Start throughput measurement of RFC2544 in service instance, range is the throughput between port of local MEP and port of peer MEP. If the global function switch of y.1371 disable will result in failure to start of rfc2544 throughput measurement.

If performance monitoring pair in service instance is not configured, fail to start throughput measurement of RFC2544.

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**service** *service-instance* **level** *level*	Enter service instance mode *service-instance*: name in service instance,length:1-13 bytes *level*: level of maintenance domain
3	**test throughput object** *band-wide* **[packet-size {64|128|256|512|1024|1280|1518}]**	*band-wide:* target bandwidth, range in 300-112500, unit: kBps **packet-size:** length of measurement massage **64: 64 bytes** **128: 128 bytes** **256: 256 bytes** **512: 512 bytes** **1024: 1024 bytes** **1280: 1280 bytes** **1518: 1518 bytes**
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode

Functions of the following examples: Enable overtime of rfc2544in the service instance, bandwidth of the measurement target is 300kBps

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *10-45*

Raisecom(config-service)#**service mep up mpid 100 por**t *1*

Raisecom(config-service)#**service performance-monitor remote 200 source** *100*

Raisecom(config-service)#**service performance-monitor throughput timeout** *20*

Raisecom(config-service)#**test throughput object 300 packet-size** *256*

Maintenance Domain Leve : 3

*Service : **m**a3-1-4*

Time out : 20 second

Throughput testing between MEP 100 in port 1 and remote mep 200 start!

Press <ctrl+c> to skip, throughput test will run in the background.

Rfc2544 throughput test result: succeded

Far End throughput test result:

Local Send(Bps)	*Remote Recv(Bps)*	*Local Send(pps)*	*Remote Recv(pps)*
300000	*289000*	*1169*	*1168*

Near End throughput result:

Remote Send(Bps)	*Local Recv(Bps)*	*Remote Send(pps)*	*Local Recv(pps)*
300000	*288900*	*1170*	*1164*

Raisecom(config- service)#**exit**

Note:

- In order to prevent throughput measurements out of control, in the rfc2544 measurement, close y.1731 open switch, it will lead to total failure;;
- In order to prevent throughput measurements out of control, in the rfc2544 measurement, the fact that y.1731 function switch of MEP whereabouts disable will lead to total failure;;
- In order to prevent throughput measurements out of control, in the rfc2544 measurement, the fact that delete y.1731 measuring will lead to total failure;;
- As a result of hardware resources conflict, in the same device can only run a measurement of rfc2544 at the same time

35.5 Monitoring and maintenance

Command	Description
show ethernet cfm traceroute-cache	Show traceroute discovery information of database LT
show ethernet cfm local-mp [interface	Show configuration information of local

line/client *port-id* | **level** *level* **]**	MP, contains MEP and MIP
show ethernet cfm remote-mep [**level** *level* [**service** *service-instance* [**mep** *mepid*]]]	Show discovery information of remote MEP
show ethernet cfm errors [**level** *level*]	Show information of error CCM datebase
show ethernet cfm domain [**level** *level*]	Show configuration information of maintenance domain and service instance
show ethernet cfm mep level *level* **service** *service-instance*	Show MEP information in service instance
show ethernet cfm	Show global configuration information of Y.1731
show ethernet cfm performance-monitor level *level* **service** *service-instance*	Show configuration information of performance monitoring
show ethernet cfm performance-monitor {previous *intervals* **quarter | current-quarter | last-24-hour} {frame-loss-ratio | frame-delay | frame-delay- variation}**	Show statistical information of performance monitoring
Show ethernet cfm performance-monitor throughput level *level* **service** *service-instance*	Show measurement result of last RFC2544
clear ethernet cfm traceroute-cache	Delete information of database LT
clear ethernet cfm remote-mep [level *level* **[service** *service-instance* **[mpid** *mepid***]]]**	Delete specified information of remote MEP datebase
clear ethernet cfm errors [**level** *level*]	Delete specified information of remote MEP datebase
clear performance-monitor statistic {all | frame-loss-ratio | delay | delay-variation}	Show statistical information of performance monitoring

35.5.1. Display LT database path discovery information

Command format: show ethernet cfm traceroute-cache

Function: Display entries have been stored in the database LT and retention time, the name of the corresponding MD, rank and vlan associated service instances. It also can display initiation TTL of traceroute discovery, the transceived port of each hop LTM message, status of LTM message transmitting, method of LTM message transmitting as well as MAC address of the next hop the device. When the switch of the LT database is turned off, do not show discovery information of any traceroute.

Show results:

IC_A#**show ethernet cfm traceroute-cache**

The size of the linktrace database: 100 hold-time: 100

Tracing the route to CCCC on domain md1, level 3, VLAN 4.

Hops	*HostMAC*	*Ingress/EgressPort*	*IsForwarded*	*RelayAction*	*NextHop*
1	*AAAA*	*8/1*	*Yes*	*RlyFdb*	*BBBB*
2	*BBBB*	*2/3*	*Yes*	*RlyFdb*	*CCCC*
!3	*CCCC*	*-/9*	*No*	*RlyHit*	*CCCC*

35.5.2. Show local MP configuration information, including MEP and MIP

Command format: show ethernet cfm local-mp [interface line/client *port-id* | level *level*]

Function: View configuration information of local MP, you can view the level of MIP corresponds to MD, the corresponding port ID and MAC address information, you can also view name of the MEP, the corresponding level of MD, port ID, direction of MEP sending, MAC address information, switching status of CCM message, entries have been transmitting and so on. User can choose to display MP on the specified port or MP of designated level.

Show results: The configuration of 3-level MEP, UP direction, shutdown of CCM transmitting, a number of messages have been transmitting as 0.

IC_B#**show ethernet cfm mp local**

Level Type Port Mac Address

---

5 MIP 2 BBBB

Mpid MdName Level Vlan Type Port Mac Address CC-Status SendCCMs

---

1 md3-1 3 4 UP 2 BBBB Disable 0

IC_B#**show ethernet cfm mp local**

Level Type Port Mac Address

---

5 MIP 2 BBBB

Mpid MdName Level Vlan Type Port Mac Address CC-Status SendCCMs

---

1 md3-1 3 4 UP 2 BBBB Disable 0

35.5.3. Show discovery information of the remote MEP

Command format: show ethernet cfm remote-mep [**level** *level* [**service** *service-instance* [**mep** *mepid*]]]

Function: View a remote MEP found by the local MP, show the level of MIP corresponds to MD, MAID, and MAC address information, MEPID, port status, MAC address information, switching state of CCM message, entries have been transmitting and so on. User can choose to display the remote MEP found in specified maintenance domain, the remote MEP found in the designated service instance or the remote MEP found by specified MEP

Showing results: Show MPID of remote MEP for 1, whereabouts of MD for md3, levels of 3, VLAN associated MA where remote MEP exist for 4, the port status is up, the MAC address of the remote MEP for CCCC, a local switch port ID receiving message for 1, a period of 9 seconds.

Raisecom#**show ethernet cfm remote-mep**

MPID MD name Level VLAN PortState MAC IngressPort Age

---

1 md3 3 4 UP CCCC 1 9

Note: According to state machine defined of the agreement IEEE802.1ag, after MEP receiving remote MEP and the first CCM, it shows remote MEP discovery information, remote ME MAC address will be shown all FF. It will not get back to normal till MEP receives the second CCM message of remote MEP.

35.5.4. Show configuration information of maintaining domain and service instance

Command format: show ethernet cfm domain [level *level]*

Function: view the level of generated MD, VLAN associated corresponding MA, user can view transmitting interval of CCM message at the same time, as well as the remote MEP learning switch.
Showing results: The specific configuration can refer to 1.4.2, shows MD configured level of 3 named md3-1, as well as service instance named ma3-1-4 is associated with vlan 4, while equipped with 5-level MD called md5-1

Raisecom#**show ethernet cfm domain**

In maintenance domain md3-1:

Level: 3

Total services: 1

Service Vlan CCMInterval

---

ma3-1-4 4 10

In maintenance domain md5-1:

Level: 5

Total services: 0

Service Vlan CCMInterval

35.5.5. Show MEP information in service instance

Command format: show ethernet cfm mep level *level* service *service-instance*

Function: View MEP of specified service instance, including local MEP, configurable static remote MEP, that the dynamics remote MEP found by MEP.

Showing results: Show a local MEP, a static remote MEP, a specified MAC address: AAAA, a dynamic remote MEP.

Raisecom#**show ethernet cfm mep level** *3* **service** *ma3-1-4*

MPID Type MAC address

---

1 local ABCD.ABCD.ABCD

2 static-remote -

3 dynamic-remote ABCD.ABCD.ABCD

35.5.6. Show global configuration information of Y.1731

Command format: show ethernet cfm

Function: Display the related configuration information of CFM, such as CFM protocol status in the global mode, the CFM status under the port, retention time of error CCM message and aging time of the remote MEP.

Showing results: The global CFM protocol has been opened, the default CFM protocols on port, error retention time for 100, the default aging time of the remote MEP

Raisecom#**show ethernet cfm**

Global CFM Admin Status: enable

Port CFM Enabled Portlist:1-26

Archive hold time of error CCMs: 100

Remote mep aging time: 100

35.5.7. Show configuration information of performance monitoring

Command format: show ethernet cfm performance-monitor information level *level* service *service-instance*

Function: display the relevant configuration of performance monitoring in the service instance, such as configuration of performance monitoring, delay and delay jitter targets, thresholds, performance monitoring status.

Showing Results: The performance monitoring has been configured, enable the Performance Monitoring

Raisecom# **show ethernet cfm performance-monitor level** 3 **service ma***3-1-4*

Level: 3

service: ma3-1-4

Performance-Monitor: enable

Performance-Monitor trap: enable

Frame-Loss-Ratio raising threshold: 2%

Frame-Loss-Ratio failing threshold: 0.2%

Delay raising threshold: 2%

Delay failing threshold: 0.5%

Delay-variation raising threshold: 2%

Delay-variation failing threshold: 0.5%

Throughput timeout: 20 second

S-MEPID: Source MEP ID

D-MEPID: Destination MEP ID

DV : Delay Variation

Obj : Objectiv

S-MEPID D-MEPID Delay Obj DV Obj

---

100 200 100 20

35.5.8. display performance monitoring statistics

Command Format: **show ethernet cfm performance-monitor { previous** *intervals* **quarter | current-quarter | last-24-hour} {frame-loss-ratio | frame-delay | frame-delay- variation} level** *level* **[service** *service-instance***]**

Function: Display statistical information of performance monitoring in service instance, including: general statistical information of frame loss, the current statistical information, 15-minute historical statistical information, a 24-hour historical statistical information; the current statistics of delay, 15-minute historical statistical information, a 24-hour historical statistical information; current statistics of delay jitter, 15-minute historical statistical information, a 24-hour historical statistical information.

Show results:

(Statistical information of the current 15-minute frame loss)

Level: 3 Service:ma3-1-4 Elapsed-time: 100(s)

current 24 hour Far-end FLR statistic

Tx loss ratio

---

10 0 0

current 24 hour Near-end FLR statistic

Tx loss ratio

---

10 1 10

（Statistical information of historical the 15th cycle frame delay）

Level:3 Service:ma3-1-4

BeginTime: 1 day 12 hour 12 minute 50 second

Previous 15 minute Far-end delay statistic

Peer MEPid Min delay Avg delay Max delay Above obj Below obj

---

100 <1 2 16 20 76

Previous 15 minute Near-end delay statistic

Peer MEPid Min delay Avg delay Max delay Above obj Below obj

---

100 <1 2 16 20 76

Previous 15 minute Round-trip delay statistic

Peer MEPid Min delay Avg delay Max delay Above obj Below obj

---

100 <1 4 32 20 76

35.5.9. Show the measurement results of previous RFC2544 throughput

Command Format: **show ethernet cfm performance-monitor throughput level** *level* **service** *service-instance*

Function: Display measurement results information of previous RFC2544 throughput

Show results:

RFC2544 throughput test information:

Throughput testing between MEP 100 in port 1 and remote mep 200:

Expected object: 300 kBps

Packet length: 256

Rfc2544 throughput test result: succeded

Far End throughput result:

Local Send (bps) Remote Recv(bps) Local Send(pps) Remote Recv(pps)

300000 289000 1700 1701

Near End throughput result:

Remote Send (bps) Local Recv(bps) Remote Send(pps) Local Recv(pps)

300000 296000 1710 1708

35.5.10. Clear information of database LT

Clear all the two-layer traceroute information in database LT.

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**clear ethernet cfm traceroute-cache**	Clear information of LT database
4	**exit**	Return to privileged user mode
5	**show ethernet cfm traceroute-cache**	Show data information

Functions of the following example: Clear all information of LT database

Raisecom#**config**

Raisecom(config)#**clear ethernet cfm traceroute-cache**

Raisecom(config)#**exit**

35.5.11. Clear information of remote MEP database

Clear specified information of remote MEP database

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**clear ethernet cfm remote-mep [level** *level* **[service** *service-instance* **[mpid** *mepid***]]]**	Clear information of remote MEP database *service-instance*: name in service instance length:1-13 bytes; *level*: level of maintenance domain *Mepid;* local MEPID
4	**exit**	Return to privileged user mode
5	**show ethernet cfm remote-mep**	Show data information

Functions of the following example: Clear remote MEP information of 3-level maintenance domain

Raisecom#**config**

Raisecom(config)#**clear ethernet cfm remote-mep level** *3*

Raisecom(config)#**exit**

35.5.12. Clear information of error CCM database

Clear specified information of remote MEP database

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**clear ethernet cfm errors** [**level** *level*]	Clear information of remote MEP database *level*: level of maintenance domain range in 0-7
4	**exit**	Return to privileged user mode
5	**show ethernet cfm error**	Show data information

Functions of the following example: Clear specified information of remote MEP database

Raisecom#**config**

Raisecom(config)#**clear ethernet cfm errors level** *3*

Raisecom(config)#**exit**

35.5.13. Clear statistics of performance monitoring

This command only to clear historical statistical information, statistical information of the past 15-minute, , and a 24-hour statistical information, but can not clear the current statistical information

Step	Command	Description
1	**config**	Enter the global configuration mode

2	**service** *service-instance* **level** *level*	Clear information of remote MEP database *service-instance*: name in service instance length:1-13 bytes; *level*: level of maintenance domain
3	**clear performance-monitor statistic** *(all | frame-loss-ratio | delay | delay-variation)*	Configure performance monitor statistics information. **all**: clear all history statistic information; **frame-loss-ratio:** clear frame loss ratio history statistic information; **delay**: clear delay history statistic information. **delay-variation**: clear delay variation history statistic information.
4	**exit**	Return to global configuration mode
5	**exit**	Return to privileged user mode
6	**show ethernet cfm performance-monitor level** *level* **service** *service-instance*	Show configuration information of performance monitoring *level*: level of maintenance domain, range in0-7

Functions of the following example: in service instance mode, enable alarm switch of performance monitoring

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *10-45*

Raisecom(config-service)#**service mep up mpid** 100 **port** *1*

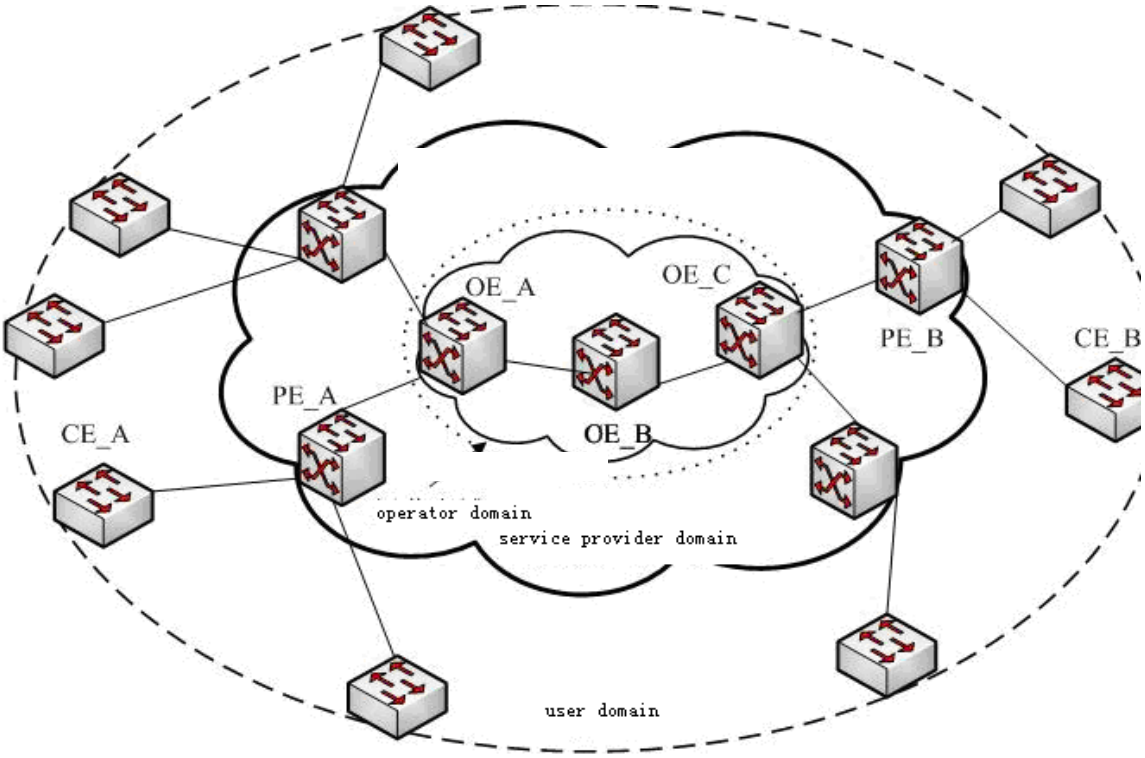
Raisecom(config-service)#**snmp-server performance-monitor trap** *{enable | disable}*

Raisecom(config-service)#**service performance-monitor frame-loss-ratio rising-threshold** *4*

Raisecom(config-service)#**exit**

35.6 A typical configuration guide

Topology as shown:



Metropolitan Area Network will be defined as user domain, service provider domain and operator domain, this three maintenance domain can be divided into three levels: respectively, level 5, level3 and level 1. As shown, CE_A connect to PE_A, PE_A connect to OE_A, OE_A connect to OE_C through OE_B, CE_B connect to PE_B, PE_B connect to OE_C. Configure 3-level MEP and 3-level MIP between PE_A and PE_B, configure 1-level MEP and 1-level MIP between OE_C and OE_A, and configure two 1-level MIP on OE_B. Specific configuration is as follows:

Configuration step of PE_A:

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *100-105*

Raisecom(config-service)#**service cvlan** *10*

Raisecom(config-service)#**service priority** *4*

Raisecom(config-service)#**service mep up mpid** 301 **port** *1*

Raisecom(config-service)#**service cc enable mep** *all*

Raisecom(config-service)#**service remote mep** *302*

Raisecom(config-service)#**service performance-monitor remote** 302 **source** *301*

Raisecom(config-service)#**service performance-monitor delay object** *20*

Raisecom(config-service)#**service performance-monitor delay-variation object** *5*

Raisecom(config-service)#**service performance-monitor frame-loss-ratio rising-threshold** *2*

Raisecom(config-service)#**service performance-monitor delay rising-threshold** *2*

Raisecom(config-service)#**service performance-monitor delay-variation rising-threshold** *2*

Raisecom(config-service)#**snmp-server trap performance-monitor** *enable*

Raisecom(config-service)#**service performance-monitor** *enable*

Raisecom(config-service)#**exit**

Raisecom(config)#**interface line/client** *1*

Raisecom(config-port)#**switch access vlan** *100*

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

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)#**switch mode trunk**

Raisecom(config-port)#**ethernet cfm mip level** *3*

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

Raisecom(config)#**snmp-server cfm-trap** *all*

Raisecom(config)#**ethernet cfm** *enable*

Configuration step of OE_A:

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**ethernet cfm domain md-name ma1-1 level** *1*

Raisecom(config)#**service ma1-1-100 level** *1*

Raisecom(config-service)#**service vlan-list** *100-105*

Raisecom(config-service)#**service mep up mpid 101 port** *1*

Raisecom(config-service)#**service cc enable mep** *all*

Raisecom(config-service)#**service remote mep learning** *enable*

Raisecom(config-service)#**exit**

Raisecom(config)#**interface line/client** *1*

Raisecom(config-port)#**switch mode trunk**

Raisecom(config-port)#**ethernet cfm mip level** *3*

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

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)#**switch mode trunk**

Raisecom(config-port)#**ethernet cfm mip level** *1*

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

Raisecom(config)#**ethernet cfm** *enable*

Configuration step of OE_B:

Raisecom(config)#**ethernet cfm domain md-name ma1-1 level** 1

Raisecom(config)#**service ma1-1-100 level** *1*

Raisecom(config-service)#**service vlan-list** *100-105*

Raisecom(config)**#interface line/client** *1*

Raisecom(config-port)#**switch mode trunk**

Raisecom(config-port)#**ethernet cfm mip level** *1*

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

Raisecom(config)**#interface line/client** *2*

Raisecom(config-port)#**switch mode trunk**

Raisecom(config-port)#**ethernet cfm mip level** *1*

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

Raisecom(config)#**ethernet cfm** *enable*

Configuration step of OE_C:

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)#**ethernet cfm domain md-name ma1-1 level** *1*

Raisecom(config)#**service ma1-1-100 level** *1*

Raisecom(config-service)#**service vlan-list** *100-105*

Raisecom(config-service)#**service mep up mpid 102 port** *1*

Raisecom(config-service)#**service cc enable mep** *all*

Raisecom(config-service)#**service remote mep learning** *enable*

Raisecom(config-service)#**exit**

Raisecom(config)#**interface line/client** *1*

Raisecom(config-port)#**switch mode trunk**

Raisecom(config-port)#**ethernet cfm mip level** *3*

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

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)#**switch mode trunk**

Raisecom(config-port)#**ethernet cfm mip level** *1*

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

Raisecom(config)#**ethernet cfm** *enable*

Configuration step of PE_B

Raisecom(config)#**ethernet cfm domain md-name md5-1 level** *5*

Raisecom(config)#**ethernet cfm domain level** *3*

Raisecom(config)**#interface line/client** *1*

Raisecom(config-port)#**ethernet cfm mip level** *5*

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

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**service vlan-list** *100-105*

Raisecom(config-service)#**service cvlan** *10*

Raisecom(config-service)#**service priority** *4*

Raisecom(config-service)#**service mep up mpid 302** *port 1*

Raisecom(config-service)#**service cc enable mep** a*ll*

Raisecom(config-service)#**service remote me**p *301*

Raisecom(config-service)#**service performance-monitor remote 301 source** *302*

Raisecom(config-service)#**service performance-monitor delay object** *20*

Raisecom(config-service)#**service performance-monitor delay-variation object** *5*

Raisecom(config-service)#**service performance-monitor frame-loss-ratio rising-threshold** *2*

Raisecom(config-service)#**service performance-monitor delay rising-threshold** *2*

Raisecom(config-service)#**service performance-monitor delay-variation rising-threshold** *2*

Raisecom(config-service)#**snmp-server trap performance-monitor** *enable*

Raisecom(config-service)#**service performance-monitor** *enable*

Raisecom(config-service)#**exit**

Raisecom(config)#**interface line/client** *1*

Raisecom(config-port)#**switch access vlan** *100*

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

Raisecom(config)#**interface line/client** *2*

Raisecom(config-port)#**switch mode trunk**

Raisecom(config-port)#**ethernet cfm mip level** *3*

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

Raisecom(config)#**snmp-server cfm-trap** *all*

Raisecom(config)#**ethernet cfm** *enable*

Expression of CC function:
In PE_A, PE_B on, OE_A or OE_C:
By showing a command of remote MEP can display found remote MEP command;
By showing error CCM database can display an error message;

Reflection of LB function:
Suppose MAC address of PE_A is AAAA; MAC address of PE_B is BBBB; MAC address of OE_A is CCCC; MAC address of OE_B is DDDD; the MAC address of OE_C is EEEE.

After configuration of PE_A, OE_A, OE_B, OE_C, PE_B is completed, ping and traceroute MP equipmen at the same level of MEP through MAC address on the device configured MEP

Ping its peer MEPID of MEP on PE_A

Raisecom(config)#**service ma***3-1-4* **level** *3*

Raisecom(config-service)#**ping mep** *302* **source** *301*

Sending 5 ethernet cfm loopback messages to BBBB, timeout is 2.5 seconds:

!!!!!

Success rate is 100 percent (5/5).

Ping statistics from BBBB:

Received loopback replys: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

Ping the MAC of the peer MEP on PE_A

Raisecom(config)#**service ma***3-1-4* **level** *3*

Raisecom(config-service)#**ping BBBB source** *301*

Sending 5 ethernet cfm loopback messages to BBBB, timeout is 2.5 seconds:

!!!!!

Success rate is 100 percent (5/5).

Ping statistics from BBBB:

Received loopback replys: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

Reflection of LT function:

Traceroute its peer MEPID of MEP on PE_A

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**traceroute mep** *302* **source** *301*

TTL: <64>

Tracing the route to BBBB on domain -, level 3, VLAN 100.

Traceroute send via port <1>.

Hops HostMAC Ingress/EgressPort IsForwarded RelayAction NextHop

---

<1> *<AAAA>* ***<2/1>*** *<yes>* *<**RlyFDB**>* *<AAAA>*

<2> *<AAAA>* ***<-/1>*** *<yes>* *<**RlyFDB**>* *<CCCC>*

*<3> <CCCC> <-/-> <yes> <**RlyFDB**> <DDDD>*

*<4> <DDDD> <**1**/-> <yes> <**RlyFDB**> <EEEE>*

!<5> *<EEEE>* *<**2**/-> <no> <**RlyHit**> <BBBB>*

Traceroute its peer MAC of MEP on PE_A

Raisecom(config)#**service ma3-1-4 level** *3*

Raisecom(config-service)#**traceroute mep** *BBBB* **source** *301*

TTL: <64>

Tracing the route to BBBB on domain -, level 3, VLAN 100.

Traceroute send via port <1>.

Hops HostMAC Ingress/EgressPort IsForwarded RelayAction NextHop

---

<1> *<AAAA>* ***<2/1>*** *<yes>* *<**RlyFDB**>* *<AAAA>*

<2> *<AAAA>* ***<-/1>*** *<yes>* *<**RlyFDB**>* *<CCCC>*

<3> *<CCCC>* *<-/->* *<yes>* *<**RlyFDB**>* *<DDDD>*

<4> *<DDDD>* *<**1**/->* *<yes>* *<**RlyFDB**>* *<EEEE>*

!<5> *<EEEE>* *<**2**/->* *<no>* *<**RlyHit**>* *<BBBB>*

Reflection of PM function:

In PE_A, PE_B at:

By showing statistics command display statistical information of the current performance within 15 minutes, performance statistics in current 24-hour period, historical performance statistics within 15 minutes, statistical information, historical performance statistics 24 hours;

Chapter 36 Interface Converter Configuration

36.1 Interface Converter principles

Interface Converter principle is after HDLC or GFP encapsulation for Ethernet data, transmit the packet through traditional PDH lines to achieve Ethernet interface transmission, which can adopt multiple E1 interfaces to transmit Ethernet data, and form a virtual-channel by multiple interfaces inverse multiplexing.

This series product includes RC953-4FE4E1T1, RC953-4FE8E1T1, RC953-4FE4E1T1-BL and RC953-4FE8E1T1-BL.

36.2 Encapsulation mode (HDLC/GFP) configuration

Function	Default
Encapsulation mode of interface converter	HDLC

Set encapsulation mode for interface converter

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**ric encapsulation-type** *(gfp|hdlc)*	Set encapsulation mode for interface converter (GFP or HDLC).
3	Please input '*yes*' to confirm: yes	Input “yes” to confirm.
4	**exit**	Exit global configuration mode and enter Privileged EXEC mode.
5	**reboot**	The configuration becomes effective after reboot.

36.3 Configuration of HDLC encapsulation interface converter

Function	Default value
virtual-channel E1	All E1 interfaces
virtual-channel E1error auto-shutdown	disable
E1 loopback detection	disable
E1 clock mode	Master clock
E1 CRC auto-negotiation	Enable

Local E1 outer-loopback	disable

36.3.1 Virtual-channel

Set E1 interface used in virtual-channel:

Step	Command	Description
1	**config**	Enter Global Configuration Mode
2	**virtual-channel** *<1-1>* **e1** *{1-n}*	Set E1 interface ID used in virtual-channel, n indicates the maximum E1 interfaces on device.
3	**virtual-channel** *<1-1>* **error-shutdown** *(enable|disable)*	Set virtual-channel E1 interface error auto-shutdown enable/ disable
4	**show virtual-channel**	Show virtual-channel information

Delete all E1 in E1 interface by command **no virtual-channel** *1*.

36.3.2 E1 loopback-detection

Step	Command	Description
1	**config**	Enter Global Configuration Mode
2	**e1-loopback-detection** *(all|disable|{1-n})*	Configure E1 loopback-detection enable
3	**show e1-loopback-detection**	show E1 interface loopback detection information

36.3.3 E1 interface

Set E1 interface function:

Step	Command	Description
1	**config**	Enter Global Configuration Mode.
2	**interface e1** *<1-n>*	Enter E1 Interface Mode, n indicates the number of E1 interfaces on the device.
3	**clock-mode** *(master|slave)*	Set E1 clock mode.
4	**crc-auto** *(enable|disable)*	Configure E1 CRC auto-negotiation enable.
5	**local-e1-loopback**	Configure local E1 outer-loopback.
6	**show interface e1** *[<1-n>]*	Show E1 interface information, n indicates the number of E1 interfaces on the device.

Disable local E1 outer-loop back by command **no local-e1-loop back**.

36.3.4 Monitoring and Maintenance

User can view related status information of virtual-channel and E1 interface by **show** command.

Command	Description
show virtual-channel	Show virtual-channel related configuration information.
show e1-loopback-detection	Show related information of E1 loopback detection.
show interface e1	Show E1 interface configuration and status information.

Show virtual-channel E1 configuration, E1 error auto-shutdown configuration and other information on the current device by **show virtual-channel**. The following example is the echo in reality results:

Raisecom#**show virtual-channel**

E1 List:1-8

E1 error-auto-shutdown: Enable

Raisecom#

Display the current configuration of E1 loopback detection, as well as loopback results by **show e1-loopback-detection**, if the result is 0 means that there is no loopback. The following example is the echo in reality results:

Raisecom#**show e1-loopdetection**

E1-ID	*STATE*	*RESULT*
1	*disable*	*0*
2	*disable*	*0*
3	*disable*	*0*
4	*disable*	*0*
5	*disable*	*0*
6	*disable*	*0*
7	*disable*	*0*
8	*disable*	*0*

Raisecom#

Use in shows relevant configuration and status information of E1 interface on the current device by **show interface e1**, including local E1 outer-loop, the clock mode, CRC auto-negotiation enable, as well as E1 linking status and other information. The following example is the echo in reality results:

Raisecom#**show interface e1** *1*

e1 interface infomation:

portid = 1

ClockMode = slave

FrameMode = framed

CrcStatus = enable

LocalLoop = normal

CrcAutoNego = enable

E1 interface type = balance

AlarmStatus = NONE

EthSendPacketNum = 11643

EthReceivePacketNum = 0

EthReceiveErrorPacketNum = 0

Link status = OK

Raisecom#

36.3.5 Examples of typical configuration

Configure device:

Raisecom#**config**

Raisecom(config)# **virtual-channel** *1* **e1** *1-8*

Set successfully

Raisecom(config)#**virtual-channel** *1* **error-shutdown** *enable*

Set successfully

Raisecom#**show virtual-channel**

E1 List:1-8

E1 error-auto-shutdown: Enable

Raisecom(config)#**e1-loopback-detection** *all*

Set successfully

Raisecom(config)#**show e1-loop detection**

E1-ID	*STATE*	*RESULT*
1	*enable*	*0*
2	*enable*	*0*
3	*enable*	*0*
4	*enable*	*0*
5	*enable*	*0*
6	*enable*	*0*
7	*enable*	*0*

8 *enable* 0

Raisecom(config)#

36.4 Configuration of HDLC encapsulation interface converter

Function	Default value
VCAT	enable
LCAS	on
VLI	enable
GFP scrambling code	enable
FCS insertion	enable
VCG member	All E1 interfaces of device
System E1 clock mode	master
E1 loopback detection function	disable
E1 CRC auto-negotiation	enable
Local E1 outer-loopback	disable

36.4.1 VCG configuration

1. Set VCAT:

Step	Command	Description
1	**config**	Enter Global Configuration Mode
2	**interface eopif** *1*	Enter EOP interface mode, 1 indicates EOP interface number on device.
3	**vcat** *(enable|disable)*	Set vcat mode for EOP interface.
4	**show interface eopif** *1*	Show EOP interface information, 1 indicates EOP interface number on device.

2. Set LCAS:

Step	Command	Description
1	**config**	Enter Global Configuration Mode
2	**interface eopif** *1*	Enter EOP interface mode, 1 indicates EOP interface number on device.
3	**lcas** *(on|off)*	Set lcas mode for EOP interface.

4	**show interface eopif** *1*	Show EOP interface information, 1 indicates EOP interface number on device.

3. Set VLI:

Step	Command	Description
1	**config**	Enter Global Configuration Mode
2	**interface eopif** *1*	Enter EOP interface mode, 1 indicates EOP interface number on device.
3	**vli** *(enable|disable)*	Set vli mode for EOP interface.
4	**show interface eopif** *1*	Show EOP interface information, 1 indicates EOP interface number on device.

4. Set GFP scrambling code:

Step	Command	Description
1	**config**	Enter Global Configuration Mode
2	**interface eopif** *1*	Enter EOP interface mode, 1 indicates EOP interface number on device.
3	**gfp-scrambling** *(enable|disable)*	Set GFP scrambling code mode for EOP interface.
4	**show interface eopif** *1*	Show EOP interface information, 1 indicates EOP interface number on device.

5. Set FCS insertion:

Step	Command	Description
1	**config**	Enter Global Configuration Mode
2	**interface eopif** *1*	Enter EOP interface mode, 1 indicates EOP interface number on device.
3	**gfp-fcs** *(enable|disable)*	Set FCS insertion mode of EOP interface.
4	**show interface eopif** *1*	Show EOP interface information, 1 indicates EOP interface number on device.

6. Set VCG member:

Step	Command	Description
1	**config**	Enter Global Configuration Mode
2	**interface eopif** *1*	Enter EOP interface mode, 1 indicates EOP interface number on device.

3	**add e1** *<1-n>*	Add VCG member, n indicates member corresponding E1 interface number.
4	**delete e1** *<1-n>*	Delete VCG member, n indicates member corresponding E1 interface number.
5	**show interface eopif** *1*	Show EOP interface information, 1 indicates EOP interface number on device.

36.4.2 System E1 clock mode

Step	Command	Description
1	**config**	Enter Global Configuration Mode
2	**system-e1-clock** *(internal | line)*	Set system E1 clock.
3	**show ric system-info**	Show ric system information.

36.4.3 E1 loopback-detection

Step	Command	Description
1	**config**	Enter Global Configuration Mode
2	**e1-loopback-detection** *(all|disable)*	Configure E1 loopback-detection enable
3	**show e1-loopback-detection**	show E1 interface loopback detection information

36.4.4 E1 interface

Set E1 interface function:

Step	Command	Description
1	**config**	Enter Global Configuration Mode.
2	**interface e1** *<1-n>*	Enter E1 Interface Mode, n indicates the number of E1 interfaces on the device.
3	**crc-auto** *(enable|disable)*	Configure E1 CRC auto-negotiation enable.
4	**local-e1-loopback**	Configure local E1 outer-loopback.
5	**show interface e1** *[<1-n>]*	Show E1 interface information, n indicates the number of E1 interfaces on the device.

Disable local E1 outer-loop back by command **no local-e1-loop back**.

36.4.5 Monitoring and Maintenance

User can view related status information of EOP/E1 interface by **show** command.

Command	Description
show ric system-info	Show related information of interface converter module.
show e1-loopback-detection	Show related information of E1 loopback detection.
show interface eopif	Show EOP interface configuration and status information.
show interface e1	Show E1 interface configuration and status information.

Show related information of interface converter module, including device model, version, E1 clock, etc. on the current device by **show ric system-info**. The following example is the echo in reality results:

Raisecom(config)#**show ric system-info**

Device type :RC953-4FE4E1

Ric encapsulation type :GFP

Ric chip version :RA1160 V2.2(2009-08-25)

Ric cpld version :1.0

system management mode :Remote

CMF UPI value :03

System E1 clock :line

System E1 clock source :E1-1

SDRAM config :full

Raisecom(config)#

Display the current configuration of E1 loopback detection, as well as loopback results by **show e1-loopback-detection**, if the result is 0 means that there is no loopback. The following example is the echo in reality results:

Raisecom#**show e1-loopdetection**

E1-ID	*STATE*	*RESULT*
1	*disable*	*0*
2	*disable*	*0*
3	*disable*	*0*
4	*disable*	*0*

Raisecom(config)#

Show related configuration and status information of EOP interface on current device by command **show interface eopif**, including LCAS, VCAT, VCG member status, etc. information. The following example is the echo in reality results:

Raisecom(config)#**show interface eopif** *1*

Interface ID :1

VCG ErrorStatus :LFD

LCAS mode config :ON

Encapstype :GFP

FCS mode config :FCS

Provisioned size rx :4

Actual size rx :0

Provisioned size tx :4

Actual size tx :0

GFP Scrambling config :enable

VCAT config :enable

VLI config :enable

Member Info :

Status	*Rx*	*Tx*	*Error*		
1	*FAIL*	*FAIL*	*LOM*	*RxCRC*	*MND*
2	*FAIL*	*FAIL*	*LOM*	*RxCRC*	*MND*
3	*FAIL*	*FAIL*	*LOM*	*RxCRC*	*MND*
4	*FAIL*	*FAIL*	*LOM*	*RxCRC*	*MND*

Member Control Info :

Index	*receive*	*transmit*
1	*FIXED*	*ADD*
2	*FIXED*	*ADD*
3	*FIXED*	*ADD*
4	*FIXED*	*ADD*

Raisecom(config)#

Show related configuration and status information of E1 interface on current device by command **show interface e1**, including local E1 outer-loopback, framed mode and timeslot, CRC auto-negotiation enable, etc. information. The following example is the echo in reality results:

Raisecom(config)#**show interface e1** *1*

e1 interface infomation :

portid = 1

FrameMode = framed

Timeslot = 1-31

CrcStatus = disable

LocalLoop = normal

CrcAutoNego = enable

E1 interface type = unbalance

AlarmStatus = LOS

Raisecom(config)#

36.4.6 Examples of typical configuration

Configure device:

Raisecom#**config**

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

CONFIG-I:Configured from console ...

Raisecom(config)#**system-e1-clock line**

Set successfully

Raisecom(config)#**show ric system-info**

Device type :RC953-4FE4E1

Ric encapsulation type :GFP

Ric chip version :RA1160 V2.2(2009-08-25)

Ric cpld version :1.0

system management mode :Remote

CMF UPI value :03

System E1 clock :line

System E1 clock source :E1-1

SDRAM config :full

Raisecom(config)#**e1-loopback-detection** *all*

Set successfully

Raisecom(config)#**show e1-loopdetection**

E1-ID	*STATE*	*RESULT*
1	*enable*	*0*
2	*enable*	*0*
3	*enable*	*0*
4	*enable*	*0*

Raisecom(config)#**interface eopif** *1*

Raisecom(config-eopport)#**vcat** *enable*

Set successfully

Raisecom(config-eopport)#**lcas** *on*

Set successfully

Raisecom(config-eopport)#**show interface eopif** *1*

Interface ID :1

VCG ErrorStatus :LFD

LCAS mode config :ON

Encapstype :GFP

FCS mode config :FCS

Provisioned size rx :4

Actual size rx :0

Provisioned size tx :4

Actual size tx :0

GFP Scrambling config :enable

VCAT config :enable

VLI config :enable

Member Info :

Status	*Rx*	*Tx*	*Error*		
1	*FAIL*	*FAIL*	*LOM*	*RxCRC*	*MND*
2	*FAIL*	*FAIL*	*LOM*	*RxCRC*	*MND*
3	*FAIL*	*FAIL*	*LOM*	*RxCRC*	*MND*
4	*FAIL*	*FAIL*	*LOM*	*RxCRC*	*MND*

Member Control Info :

Index	*receive*	*transmit*
1	*FIXED*	*ADD*
2	*FIXED*	*ADD*
3	*FIXED*	*ADD*
4	*FIXED*	*ADD*

Raisecom(config-eopport)

Chapter 37 Trouble Shooting Commands

37.1 show buffer

[Function]

Show the buffer information of the port.

[Command Format]

show buffer ***[port*** *<1-26>**]***

[Parameter]

port *<1-26>*: specify the port number (optional).

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

If the port number is not specified, show all the port driver pool information.

[Example]

Raisecom(config)# **show buffer 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

37.2 show diags

[Function]

Show port diagnose information.

[Command Format]

show diags *link-flap*

[Parameter]

link-flap: show UP/DOWN times and their speed(number of UP/DOWN at the last minute).

[Command Modes]

Privileged EXEC; privileged user.

[Example]

Raisecom#**show diags** *1*

```
Port       Total          Last Min
-----------------------------------------
19         2              0
21         2              2
```

37.3 show memory

[Function]

Show memory information.

[Command Format]

show memory

[Command Mode]

Privileged EXEC; privileged user.

[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 -

37.4 show process

[Function]

Show the status and stack information of the process.

[Command Format]

show processes

[Command Modes]

Privileged EXEC, privileged user

[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%)

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%)

2a730d0 tStpTm 3808 250 TSD 0 (6 / 0.0%)

27af260 tIdle 568 251 RDY 0 (281 / 0.0%)

37.5 show tech-support

[Function]

Show technical support information, all the information about trouble shooting.

[Command Format]

show tech-support

[Command Modes]

Privileged EXEC; privileged user.

[Example]

Raisecom#**show tech-support**

37.6 driver

[Function]

The control switch to set device receives any packets.

[Command Format]

driver *{receive-packet|send-packet}* **[ethertype-classify** *{stp| garp| gmrp| gvrp| igmpsnoop| lacp| eapol| loopdetect| rcmp| rcmpdata| rndp| rtdp| arp| ip| relay| others| oam| relay-stp}] {discard|syslog} {enable|disable}* [**port-list** *port-list*]

[Parameters]

receive-packet: packet receiving

send-packet: packet sending

enable: enable

disable: disable

discard: discard packet

syslog: information of syslog

port-list: port list

[Default]

Disable, Ethernet type is all types.

[Command Modes]

Global configuration mode; Privileged user

[Executing Command Instruction]

This command can control packets received or transmitted by the switch. If no type be specified, control all types. If the packets type is specified, only the specified ones will be in control.

Classification of support only accords to Ethernet type, the Ethernet classification including:

stp	STP protocol packets (0x0042)
garp	GARP protocol packets (0x0043)
gmrp	GMRP protocol packets (0x2042)
gvrp	GVRP protocol packets (0x2142)
igmpsnoop	igmpsnoop protocol packets (0x0242)
lacp	slow protocol frame protocol packets (0x8809)
eapol	EAPOL protocol packets (0x888e)
loop	loopback detection protocol packets (0x0898)
rcmp	RCMP protocol control packets (0x0899)
rcmpdata	RCMP protocol data packets (0x0897)
rndp	RNDP protocol packets (0x1a77)
rtdp	RTDP protocol packets (0x1a78)
arp	ARP protocol packets (0x0806)
ip	IP protocol packets (0x0800)
relay	relay protocol packets
others	other Ethernet packets
oam	oam protocol packets
relay-stp	relay-stp protocol packets

[Example]

Syslog all received packets:

Raisecom# **driver receive-packet** *syslog enable*

[Related commands]

Commands	Description
show device-statistics	Show setting and statistics of CPU receive/transmit packets.
clear device-statistics	Clear CPU received and transmitted packets.

37.7 show device-statistics

[Function]

Show device received and transmitted packets.

[Command Format]

show device-statistics {receive|send} [port *portnum***] [detail]**

[Parameters]

receive: received packets

send: send packets

portnum: port

detail

[Command Modes]

Privileged EXEC mode; Privileged user

[Executing Command Instruction]

Use this command to show the switch received or transmitted packets statistics and control configuration information. Only Ethernet type is in support. If not specify port, show switch received and transmitted packets statistics; if specify port, only the specified port statistics will be shown. The command without parameter *detail* won't show type line with total packets 0; and all classified statistic lines will be shown if the command has parameter *detail*.

[Explanation of command execution echo]

Type Action Total

Type of Ethernet including:

stp	STP protocol packets (0x0042)
garp	GARP protocol packets (0x0043)
gmrp	GMRP protocol packets (0x2042)
gvrp	GVRP protocol packets (0x2142)
igmpsnoop	igmpsnoop protocol packets (0x0242)
lacp	slow protocol frame protocol packets (0x8809)
eapol	EAPOL protocol packets (0x888e)
loop	loopback detection protocol packets (0x0898)
rcmp	RCMP protocol control packets (0x0899)
rcmpdata	RCMP protocol data packets (0x0897)
rndp	RNDP protocol packets (0x1a77)
rtdp	RTDP protocol packets (0x1a78)
arp	ARP protocol packets (0x0806)
ip	IP protocol packets (0x0800)
relay	relay protocol packets
others	other Ethernet packets
oam	oam protocol packets
relay-stp	relay-stp protocol packets

ACTION:

L: type the packets out;

D: discard the packets;

-: the function is disabled.

TOTAL: total packets

[Example]

Show all classified statistic of switch received packets:

Raisecom#**show device-statistics receive**

Type	*Action*	*Total*
SlowProtocol	----	*5*
Loopdetect	----	*18*
Rndp	----	*1*
Rtdp	----	*4*
Arp	----	*1*
IP	----	*3*

Show Ethernet classified statistic for packets sent by port 9 of switch:

Raisecom#**show cpu-statistics** *send port 9 detail*

Type	*Action*	*Total*
STP	----	*0*
Garp	----	*0*
Gmrp	----	*0*
Gvrp	----	*0*
IgmpSnoop	----	*0*
SlowProtocol	----	*541*
EAPOL	----	
Loopdetect	----	*0*
Rcmp control	----	*0*
Rcmp data	----	*0*
Rndp	----	*37*
Rtdp	----	*0*
Arp	----	*0*
IP	----	*0*
Relay	------	*0*
others	----	*0*
oam	-----	*0*
relay-stp	-----	*0*

[Related commands]

Commands	Description
clear device-statistics	Clear CPU received and transmitted packets.

37.8 clear device-statistics

[Function]

Clear CPU received and transmitted packets.

[Command Format]

clear device-statistics {receive|send}

[Parameters]

receive: received packets

send: send packets

[Command Modes]

Global configuration mode; Privileged user

[Executing Command Instruction]

Use this command to clear receive/transmit packets statistics of switch to 0.

[Example]

Clear CPU received packets statistics:

Raisecom# **clear device-statistics receive**

[Related commands]

Commands	Description
show device-statistics	Show setting and statistics of CPU receive/transmit packets.

瑞斯康达科技发展股份有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: Building 2, No. 28 of the Shangdi 6th Street, Haidian District, Beijing. Postcode: 100085
Tel: +86-10-82883305 Fax: +86-10-82883056 Email: export@raisecom.com
http://www.raisecom.com