

www.raisecom.com

ISCOM2128EA-MA 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.

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

Copyright Notices.

Copyright ©2011 Raisecom. All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Raisecom Technology Co., Ltd.**

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 ISCOM2128EA-MA 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/contact-us.html>.

If you have comments on the ISCOM2128EA-MA specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Chapter 1	Radius Accounting	1
1.1	Overview	1
1.2	Default configuration	1
1.3	Radius accounting configuration	1
1.4	Monitoring and Maintenance	2
1.5	Typical configuration example	3
Chapter 2	MAC Address Transmission Table Management	4
2.1	MAC transmission table management introduction	4
2.2	MAC address transmission table management configuration	5
2.3	MAC address number limit	10
2.4	Shared VLAN learning function	13
Chapter 3	Physical Layer Interface	15
3.1	Physical ports features	15
3.2	The default configuration for physical ports	15
3.3	Rate and duplex mode configuration	15
3.4	Configure IEEE 802.3X flow control function	17
3.5	Auto-MDIX function configuration	20
3.6	Cable-diagnostics	21
3.7	Maximum transmission unit configuration	22
3.8	Add description for interfaces	22
3.9	Open and close physical layer port	23
3.10	Clear interface statistics	24
3.11	Dynamic statistics time	24
3.12	Monitoring and maintaining	25
3.13	Typical configuration	25
Chapter 4	Link Aggregation	29
4.1	Basic principle	29
4.2	LACP aggregation function	29
4.3	Classification	30
4.4	Manual aggregation	30
4.5	Static LACP aggregation function	31
4.6	Trunk min-active links	32
4.7	Monitoring and maintaining	33
4.8	Typical configuration example	35
Chapter 5	STP Configuration Guide	38
5.1	STP/RSTP principle introduction	38
5.2	Configure STP	41
5.3	Configure edge port	44
5.4	MSTP principle introduction	47
5.5	MSTP configuration	48
5.6	Maintenance and management	58
5.7	Typical configuration instance	66
Chapter 6	DHCP Overview	68
6.1	DHCP client configuration	68
6.2	DHCP Snooping configuration	74
6.3	DHCP Server Configuration	82
6.4	DHCP Relay Configuration	93
6.5	DHCP OPTION	104
Chapter 7	SNMP Configuration Guide	108
7.1	SNMP principle	108
7.2	SNMPv1/v2/v3 management configuration	109
Chapter 8	Loopback Detection Configuration Guide	117
8.1	Loopback detection introduction	117

8.2	Loopback detection default configuration	117
8.3	Loopback detection function configuration	117
8.4	Monitoring and Maintenance	120
8.5	Typical Configuration Examples	120
Chapter 9	QinQ Configuration	122
9.1	QinQ principle overview	122
9.2	Basic QinQ configuration	124
9.3	Configure flexible QinQ	127
9.4	Configure VLAN conversion	130
Chapter 10	VLAN Configuration Guide	140
10.1	VLAN Configuration Principles	140
10.2	Switch VLAN Function Configuration	141
10.3	VLAN Function Configuration	157
10.4	VLAN Function Configuration	163
Chapter 11	ACL Function Configuration	171
11.1	Configuration Description	171
11.2	ACL Introduction	171
11.3	IP ACL Configuration	171
11.4	MAC ACL Function	173
11.5	MAP ACL Function	174
11.6	Application Configuration Based on Hardware ACL	180
11.7	Configuration Function Based on Software IP ACL	183
Chapter 12	QoS Configuration	185
12.1	Configuration Description	185
12.2	QoS Introduction	185
12.3	QoS Enable and Disable	192
12.4	Classification Function Configuration	193
12.5	Policy and Marking Function Configuration	201
12.6	Bit-Rate Limitation and Reshaping Function Configuration	208
12.7	Map Function Configuration	210
12.8	Queue and Adjust Function Mode	216
12.9	QoS Trouble Shoot	219
12.10	QoS Command Reference	219
Chapter 13	802.3ah OAM Function Configuration	222
13.1	802.3ah OAM Principle Introduction	222
13.2	802.3ah OAM Mode Configuration	223
13.3	802.3ah OAM Active Mode Function	224
13.4	802.3ah OAM Passive Function	230
Chapter 14	Optical Module Digital Diagnoses Configuration	238
14.1	Optical Module Digital diagnoses principle	238
14.2	Optical module digital diagnostic configuration	239
Chapter 15	CFM Configuration	241
15.1	CFM Introduction	241
15.2	CFM Default Configuration List	243
15.3	CFM Configuration Guide and Limitation	243
15.4	CFM Configuration List and Specification	243
15.5	Monitoring and Maintenance	254
15.6	Basic Configuration Example	258
Chapter 16	IP Source Guard Configuration	263
16.1	IP Source Guard principle overview	263
16.2	Configure IP Source Guard	263
16.3	Monitoring and maintenance	266
16.4	Typical configuration example	268
16.5	IP Source Guard command list	269
Chapter 17	Ethernet Ring	270
17.1	Overview	270
17.2	Default Ethernet ring configuration list	271
17.3	Configure Ethernet ring	272
17.4	Monitoring and maintenance	275

17.5	Typical application	278
Chapter 18	TACACS+	291
18.1	TACACS+ Theory	291
18.2	TACACS+ Function Configuration	292
Chapter 19	SLA Configuration	294
19.1	SLA overview.....	294
19.2	SLA default configuration list	295
19.3	SLA configuration guide and limit	296
19.4	SLA configuration list and instruction	296
19.5	Monitoring and maintenance	301
19.6	Typical configuration applications	306
Chapter 20	Y.1731 Configuration	312
20.1	Functional overview of Y.1731.....	312
20.2	Default configuration list of Y.1731	314
20.3	CFM configuration constraints and limitations	315
20.4	CFM configuration list and instruction	316
20.5	Monitoring and maintenance	336
20.6	Typical configuration	341
Chapter 21	Switch Port Backup.....	348
21.1	Overview	348
21.2	Configure switch port backup.....	349
21.3	Monitoring and maintenance	352
21.4	Typical configuration example	352
Chapter 22	SSH Management	355
22.1	SSH Function Instruction	355

Release Notes

Date of Release	Manual Version	Software Version	Revisions
20110518	201104		First release

Preface

About This Manual

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

Who Should Read This Manual

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

Relevant Manuals

Raisecom NView System User Manual

Raisecom Nview System Installation and Deployment Manual

... User Manual

... Commands Notebook

Organization

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

Chapter 1 Overview

This chapter briefly introduces the basic function of ...

Chapter 2 Configuration Management

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

Chapter 3 Performance Management

This chapter focuses on performance management function of

Chapter 4 Device Maintenance Management

This chapter introduces the device maintenance management function of

Appendix A Alarm Type

The alarm types supported by

Compliance

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

YD/T900-1997 SDH Equipment Technical Requirements - Clock

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

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

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

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

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

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

YD/T1179- 2002 Technical Specification of Ethernet over SDH

G.703 Physical/electrical characteristics of hierarchical digital interfaces

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

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

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

G.781 Synchronization layer functions

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

G.784 Synchronous digital hierarchy (SDH) management

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

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

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

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

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

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

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

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

G.841 Types and characteristics of SDH network protection architectures

G.842 Interworking of SDH network protection architectures

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

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

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

I.731 ATM Types and general characteristics of ATM equipment

I.732 ATM Functional characteristics of ATM equipment

IEEE 802.1Q Virtual Local Area Networks (LANs)

IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering

IEEE 802.3 CSMA/CD Access Method and Physical Layer Instruction

Chapter 1 Radius Accounting

1.1 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 log in the OLT, the logging time and even the operation.

1.2 Default configuration

By default Radius accounting is disabled.

1.3 Radius accounting configuration

1.3.1 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 <i>{enable / disable}</i>	Enable or disable Radius accounting
2	show aaa accounting	Show Radius accounting configuration

1.3.2 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 <i>A.B.C.D [acct-port]</i>	Configure the IP address and UDP port number of Radius accounting server. <i>A.B.C.D</i> : is the IP address of accounting server <i>Acct-port</i> : 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

1.3.3 Configure the shared key that communicate with the Radius Accounting server

This command is used to configure the key which communicates with the Radius accounting server, the key must be corresponding with Radius accounting server key, or they will charge fail. Key is empty by default.

Step	Command	Description
1	radius accounting-server key <i>WORD</i>	Configure the key which communicates with the Radius accounting server. <i>WORD</i> : shared key and should be configured to a string with length not more than 255 characters. Command of no radius accounting-server key can restored shared key to the default value.
2	show radius-server	Show Radius configuration information.

1.3.4 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 <i>{online / offline}</i>	Configure the strategy of accounting fail <i>online</i> : accounting fail permits login <i>offline</i> : accounting fail not permits login
2	show aaa accounting	Show Radius accounting configuration

1.3.5 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 <i><0-300></i>	Configure accounting update message period. <i><0-300></i> : 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 aaa accounting	Show Radius accounting configuration.

1.4 Monitoring and Maintenance

Command	Description
---------	-------------

show aaa accounting	Show Radius accounting configuration.
----------------------------	---------------------------------------

show radius-server	Show Radius configuration.
---------------------------	----------------------------

1.5 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 2 MAC Address Transmission Table Management

2.1 MAC transmission table management introduction

2.1.1 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:

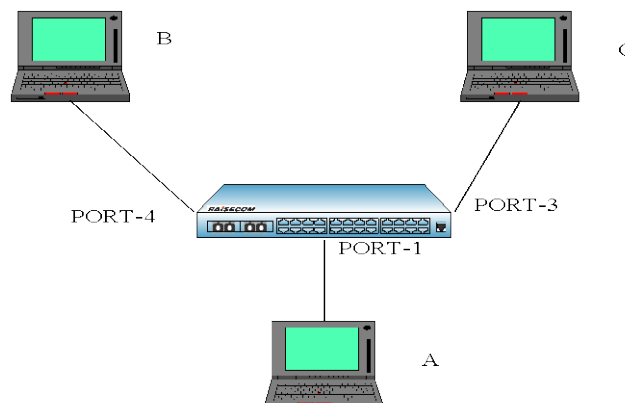
- Unicast: when there is table item that fits the message destination MAC address in the MAC address transmission table, the switch will transmit it directly from the transmission egress port of the table item;
- Broadcast: when the messages that the switch received from the destination address are all 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.

2.1.2 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:



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.

2.1.3 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.

2.2 MAC address transmission table management configuration

2.2.1 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

2.2.2 Static MAC address configuration

Step	Command	Description
1	config	Enter global configuration mode
2	mac-address-table static unicast <i>HHHH.HHHH.HHHH</i> vlan <i>vlan_id</i> port <i>port-number</i>	Set the static MAC address. <i>HHHH.HHHH.HHHH</i> is the static MAC address which will be set; format is hex, dotted notation for every four characters. Vlan_id range is 1-4094. <i>port-number</i> is the physical port number.
3	mac-address-table static multicast <i>HHHH.HHHH.HHHH</i> vlan <i>vlan_id</i> port <i>port-list</i>	Set the static MAC address. <i>HHHH.HHHH.HHHH</i> is the static MAC address which will be set; format is hex, dotted notation for every four characters. Vlan_id range is 1-4094. <i>port-number</i> 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 <i>port-number</i> vlan <i>vlan_id</i>]	Show (port or VLAN) static address. <i>port-number</i> is physical port, range is 1-26. <i>vlan_id</i> : range is 1-4094.

Notice:

- The switch MAC address, multicasting address, FFFF.FFFF.FFFF and 0000.0000.0000 cannot be configured as the static MAC address.
- At present configurable static unicast MAC address amount are different on the devices.

2.2.3 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 <i>time</i> }	Set the aging time of MAC address table. 0 stands for MAC address will not be aged <i>time</i> 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 of **no mac-address-table aging-time**.

2.2.4 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 <i>{enable/disable}</i> port-list {all {1-26}}	Enable or disable the MAC address learning function of physical port. <i>enable</i> : enable MAC address learning function. <i>disable</i> : disable MAC address learning function. <i>MAX_PORT_NUM</i> : the maximum port number that the equipment support
3	exit	Exit from global configuration mode to privileged EXEC mode.
4	show interface port [<i>port-number</i>]	Show port status. <i>port-number</i> : physical port, range is 1-26.

2.2.5 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 <i>{all/dynamic/static}</i>	<i>all</i> : delete all the 2 MAC addresses in the MAC address table <i>dynamic</i> : delete dynamic MAC addresses in the MAC address table <i>static</i> : delete static MAC addresses in the MAC address table

2.2.6 Configure static MAC address privilege

Note: RC551 device doesn't support this configuration.

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 <i>HHHH.HHHH.HHHH</i> vlan <i>vlan_id</i> port <i>port-number</i> [priority <0-7>]	Set static MAC address <i>HHHH.HHHH.HHHH</i> is the static MAC address which will be set; format is hex, dotted notation for every four characters. <i>vlan_id</i> VLAN ID, range is 1~4094. <i>port-number</i> 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 <i>port-number</i> vlan <i>vlan_id</i>]	Show (port or VLAN) static address <i>port-number</i> physical port number <i>vlan_id</i> 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**.

2.2.7 enable/disable static MAC strategy

Note: RC551 device doesn't support this configuration.

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

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

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

Note: RC551 device doesn't support this configuration.

Static MAC address can be set non-rate-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
2	mac-address-table static unicast	Set static MAC configuration

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

2.2.9 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 <i>port-number</i>	Show the switch port MAC address <i>Port-number</i> physical port, range is 1~26
show mac-address-table l2-address vlan <i>vlan_id</i>	Show the switch port MAC address <i>vlan_id</i> VLAN ID, range is 1~4094
show mac-address-table l2-address count port <i>port-number</i>	Show the switch port MAC address number Count stands for the MAC address number related to the statistics <i>port-number</i> physical port number, range is 1~26.
show mac-address-table l2-address count	Show mac-address-table count
show mac-address-table l2-address count vlan <i>vlan_id</i>	Show the switch VLAN MAC address Count stands for the MAC address number related to the statistics <i>vlan_id</i> VLAN ID, range is 1~4094
show mac-address-table static	Show the switch static MAC address configuration information
show mac-policy portlist <i>portlist</i>	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 <i>HHHH.HHHH.HHHH</i> <i>HHHH.HHHH.HHHH</i>	Search for MAC address static MAC address which is to be set, format is hex, dotted notation for every four characters.

2.2.10 Typical configuration example

Note: RC551 device doesn't support this configuration.

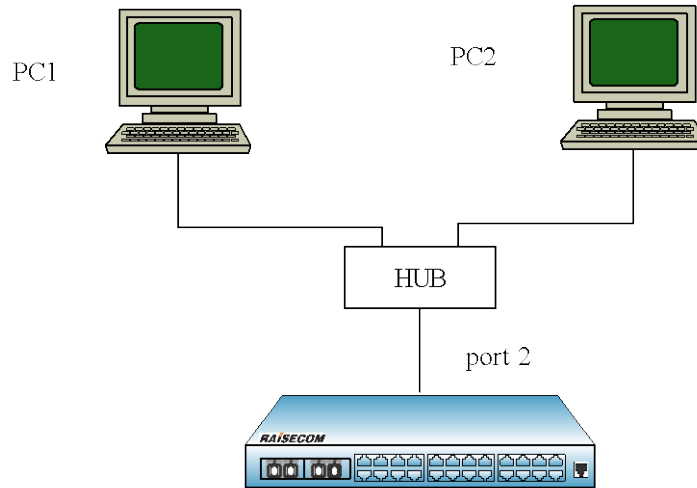
➤ Destination:

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



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 port 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.

2.3 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.

Ethernet switches specify MAC-address-table threshold on a port, and don't limit other VLAN. To the message.

2.3.1 Configure the default MAC address number limit

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

2.3.2 Configure the MAC address number

Note: RC551 device doesn't support this configuration.

Step	Command	Description
1	config	Enter global configuration mode
2	interface { port line client } <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical port mode
3	mac-address-table threshold <i><PORT_MAC_MIN_THRESHOLD_STR -</i> <i>PORT_MAC_MAX_THRESHOLD_STR></i>	Configure the MAC address learning upper limit <i>PORT_MAC_MIN_THRESHOLD_STR</i> value upper limit <i>PORT_MAC_MAX_THRESHOLD_STR</i> value lower limit
4	mac-address-table threshold <i><PORT_MAC_MIN_THRESHOLD_STR</i> <i>-PORT_MAC_MAX_THRESHOLD_STR></i> vlan <1-4094>	Configure mac-address-table upper limit.
5	no mac-address-table threshold	Configure mac-address-table upper limit as default value.
6	exit	Quit global configuration mode and enter privileged EXEC mode
7	show mac-address-table threshold port-list {1- MAX_PORT_NUM }	Show mac address table threshold value

2.3.3 Monitoring and maintaining

Command	Description
show mac-address-table threshold port-list {1- MAX_PORT_NUM }	Show mac address table threshold value

show mac-address l2

 Show interface MAC address number that
has been learned

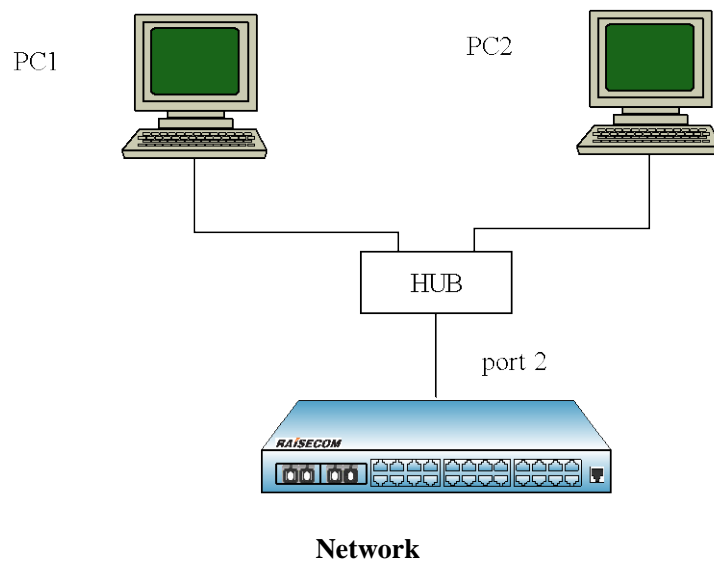
2.3.4 Typical configuration example

Note: RC551 device doesn't support this configuration.

➤ 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



➤ 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.

2.4 Shared VLAN learning function

Note: RC551 device doesn't support this configuration.

2.4.1 The default SVL configuration

Function	Default value
SVL feature	Disabled
Interface SVL default VLAN list	Empty
SVL default VLAN	VLAN 1

2.4.2 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 port <i><1-MAX_PORT_NUM></i>	Enter port configuration mode <i>1-MAX_PORT_NUM</i> the port number that the equipment supports
4	switchport svl vlanlist {1-4094}	Optional, Set the shared VLAN list of the port
5	exit	Enter global configuration mode
6	svl default vlan <1-4094>	Set SVL default VLAN <i>1-4094</i> : VLAN ID
7	exit	Quit global configuration mode and enter privileged EXEC mode
8	show svl	Show SVL state
9	show switchport <i>[<1-MAX_PORT_NUM>] svl vlanlist</i>	Show interface shared VLAN list <i>1-MAX_PORT_NUM</i> 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.

2.4.3 Monitoring and maintaining

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

2.4.4 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 port 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

1 1-4

Chapter 3 Physical Layer Interface

3.1 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 auto-sensing 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.

3.2 The default configuration for physical ports

By default, the physical port commands are shown below:

Command	Default value
Rate configuration	The rate of electronic port and 100M optical port is auto negotiated, 100M optical 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-sensing and straight Ethernet cable function	Normal mode
Port maximum transmission unit	1522 byte
Interface description	port: port-number
Interface on/off configuration	on
Dynamic statistical refresh frequency	2s

3.3 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 port <i>port-number</i> interface range <i>port-list</i>	Enter Ethernet physical interface configuration mode or physical interface range configuration mode. <i>port-number</i> is the physical interface, range is 1-26. <i>port-list</i> range is 1-26, use “,” and “-” for multiple interfaces configuration.
3	speed { <i>auto/10/100/1000</i> } duplex { <i>full/half</i> }	Set the speed and duplex mode of the port. <i>auto</i> : represents that both the speed and duplex are set according to the result of auto negotiation. <i>10</i> : represents that the speed is set to 10Mbps. <i>100</i> : represents that the speed is set to 100Mbps. <i>1000</i> : represents that the speed is set to 1000Mbps. <i>full</i> : set the duplex mode to full duplex. <i>half</i> : 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 port <i>port-number</i>	Show the status for the port. <i>port-number</i> : 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 cannot 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 cannot 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**

Raisecom (config)#**interface port 15**

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

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

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

Raisecom (config)#**exit**

Raisecom#**show interface port 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 port 1**

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

Port 1 only supports 100M/FD!/ port1 support only 100M/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 port 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 port 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 port 25**

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

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

3.4 Configure IEEE 802.3X flow control function

The flow control function of Raisecom series switches is set on both RX and TX direction separately. By default, flow control function is disabled on all ports. For the sub-card ports, if no sub-card, flow control command fail.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>port-number</i>	Enter Ethernet physical interface configuration mode or range configuration mode.

	interface range <i>port-list</i>	<i>port_number</i> physical ports, range is 1-26. <i>port-list</i> , range is 1-26, use “,” and “-” for multiple ports.
3	flowcontrol { <i>on/off</i> }	Enable/disable the flow control function on RX and TX direction. <i>on</i> : enable the flow control function of the port. <i>off</i> : 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 port <i>port-number</i>	Show the traffic control of the port. <i>port_number</i> physical port number, range is 1-26.

Example 1: set port 10 flow control function on.

Raisecom#**config**

Raisecom(config)# **interface port 10**

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

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

Raisecom(config)# **exit**

Raisecom#**show interface port 10**

R: Receive Direction

S: Send Direction

Status: Forwarding status

Port	Admin	Operate	Speed/Duplex	Flowctr(R/S)	Maclearn	Status
10	enable	down	auto	on/on	enable	Forward

Example 2: set port 25 (no sub-card) flow control function on.

Raisecom#**config**

Raisecom(config)# **interface port 25**

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

Port 25 is unavailable!

The flow control function on both RX and TX direction is set separately. By default, flow control function is disabled on all ports.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>port-number</i> interface range <i>port-list</i>	Enter Ethernet physical interface configuration mode or range configuration mode. <i>port_number</i> physical ports, range is 1-26. <i>port-list</i> , range is 1-26, use “,” and “-” for multiple ports.
3	flowcontrol { <i>receive/send</i> }{ <i>on/off</i> }	Enable/disable the flow control function on RX and TX direction. Send represents the traffic control function at TX

		direction. <i>receive</i> : represents the traffic control function at RX direction. <i>on</i> : enable the flow control function of the port. <i>off</i> : 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 port <i>port-number</i>	Show the traffic control of the port. <i>port_number</i> physical port number, range is 1-26.

Example 1: Set the flow control for port 10.

Raisecom#**config**

Raisecom (config)# **interface port 10**

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

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

Raisecom (config)#**exit**

Raisecom#**show interface port 10**

R: RX Direction

S: tx Direction

<i>Port</i>	<i>Admin</i>	<i>Operate</i>	<i>Speed/Duplex</i>	<i>Flowcontrol(R/S)</i>	<i>Mac-learning</i>	<i>Status</i>

10	enable	down	auto	on/off	enable	Forward

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 port <i>port-number</i> interface range <i>port-list</i>	Enter physical port mode or interface range configuration mode. <i>port_number</i> physical port number, range is 1-26 <i>port-list</i> port list, range is 1-26, use ',' and '-' for multiple setting.
3	flowcontrol <i>{receive/send}{on/off}</i>	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 port
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 port 10**

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

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

Raisecom(config)#**exit**

Raisecom#**show interface port 10**

R: Receive Direction

S: Send Direction

Status: Forwarding status

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

10	enable	down	auto	on/off	enable

3.5 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 port <i>port-number</i> interface range <i>port-list</i>	Enter physical port mode or interface range configuration mode; <i>port_number</i> : physical interface number; <i>port-list</i> : port list, use ',' and '-' for multiple setting.
3	mdi (<i>auto</i> <i>normal</i> <i>across</i>)	Configure port MDI mode; <i>auto</i> : linear ordering auto reserve mode <i>normal</i> : normal mode <i>across</i> : 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 [< <i>1-MAX_PORT_STR</i> >]	Show port MDI state < <i>1-MAX_PORT_STR</i> >: physical port

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

Raisecom#**config**

Raisecom(config)# **interface port 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

3.6 Cable-diagnostics

Note: RC551 series device doesn't support this configuration.

Circuit diagnostics is aimed at Ethernet port connection, and users can use this function view state of physical link. Cables information is as below:

Inquires the cable state:

- Normal
- Open
- Shorted
- Error

Inquires the error position

- Cable sends error position
- Cable accepts error position

Step	Command	Description
1	test cable-diagnostics port-list (<i>all / portlist</i>)	Start cable-diagnostics <i>all</i> : all physical ports <i>portlist</i> : physical portlist
2	show cable-diagnostics port-list (<i>all / portlist</i>)	Show cable-diagnostics <i>all</i> : all physical ports <i>portlist</i> : physical portlist

For Example: Start a cable-diagnostics and show the result.

Raisecom#**test cable-diagnostics port-list all**

Raisecom#**show cable-diagnostics port-list all**

Port	Attribute	Time	RX Stat	RX Len(m)	TX Stat	TX Len(m)
1	Issued	01/01/2000 08:05:33	Open	1	Open	1
2	Issued	01/01/2000 08:05:33	Open	1	Open	1
3	Issued	01/01/2000 08:05:34	Open	1	Open	1
4	Issued	01/01/2000 08:05:34	Open	1	Open	1
5	Issued	01/01/2000 08:05:34	Open	1	Open	1
6	Issued	01/01/2000 08:05:34	Open	1	Open	1
7	Issued	01/01/2000 08:05:34	Open	1	Open	1
8	Issued	01/01/2000 08:05:34	Normal	0	Normal	0
9	Issued	01/01/2000 08:05:34	Open	1	Open	1
10	Issued	01/01/2000 08:05:34	Open	1	Open	1

.....

24	Issued	01/01/2000 08:05:34	Open	1	Open	1
25	Not Support	N/A	N/A	0	N/A	0
26	Not Support	N/A	N/A	0	N/A	0

Related status:

- Normal
- Open
- Shorted
- Error
- N/A

Properties:

- Issued
- Not Issued
- Testing
- Not Support

3.7 Maximum transmission unit configuration

Step	Command	Description
1	config	Enter global configuration mode
2	system mtu <1500-8000> system mtu <MIN_FRAME_LEN_STR -MAX_FRAME_LEN_STR>	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

The command of **no system mtu** is used to delete 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

3.8 Add description for interfaces

Description of the Physical port can be added. The command of **no description** can restore the default configuration.

Step	Command	Description
1	config	Enter global configuration mode

2	interface port <i>port-number</i>	Enter physical layer port configuration mode or volume configuration mode <i>port-number</i> : physical port number, range is 1-26
3	[no]description WORD	Add physical port or IP interface description <i>WORD</i> : specify class-map description. 64 character the most, cannot 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 port [<1-MAXPORT>] detail	Show port information <1-MAXPORT> port number.

Example 1: add description for physical port 8.

```
Raisecom#config
```

```
Raisecom(config)# interface port 20
```

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

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

```
Raisecom(config)#exit
```

```
Raisecom#show interface port 8 detail
```

```
Port      Description
-----
8         this-is-a-port
```

3.9 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 port <i>port-number</i> interface range <i>port-list</i>	Enter physical layer port configuration mode or volume configuration mode. <i>port-number</i> : physical port number. <i>port-list</i> : 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 port <i>port-number</i>	Show port state <i>port-number</i> : physical port number.

Example 1: Close port 20.

Raisecom#**config**

Raisecom(config)# **interface port 20**

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

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

Raisecom(config)#**exit**

Raisecom#**show interface port 20**

R: Receive Direction

S: Send Direction

Port	Admin	Operate	Speed/Duplex	Flowctr(R/S)	Maclearn	Status
20	enable	down	auto	off/off	enable	Forward

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

Raisecom#**config**

Raisecom(config)#**interface port 25**

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

Port 25 is unavailable!

3.10 Clear interface statistics

Step	Command	Description
1	config	Enter global configuration
2	clear interface {port port-num client line } statistics	Clear interface statistics <i>port-num</i> : port number

Example 1: Clear statistica on port 8.

Raisecom#**config**

Raisecom(config)**clear interface port 8 statistics**

Set successfully

3.11 Dynamic statistics time

Dynamic statistics time is defaulted to 2s.

Step	Command	Description
1	config	Enter global configuration
2	dynamic statistics time <2-60>	Set dynamic statistics time
3	exit	Quit global configuration mode

4 **show interface port *portid* statistics dynamic**

The command of **no dynamic statistics time** can restore the default value.

3.12 Monitoring and maintaining

Use **show** to show port state.

Step	Command	Description
1	show interface port <i>port-number</i>	Show port state <i>port_number</i> physical port number.
2	show interface port [<i><1-MAXPORT></i>] description	Show port information. <i><1-MAXPORT></i> port number.
3	show interface { port <i>port-num/</i> client line } statistics	Show interface statistics
4	show interface port <i>portid</i> statistics dynamic [<i>detail</i>]	Show interface dynamic statistics
5	show interface client <i>clientid</i> statistics dynamic [<i>detail</i>]	Show client interfac dynamic statistics
6	show interface line <i>lineid</i> statistics dynamic [<i>detail</i>]	Show line interface dynamic statistics
7	show system mtu	Show system mtu

For example: Show port 8 state.

Raisecom#**show interface port 8**

R: Receive Direction

S: Send Direction

Status: Forwarding status

Port	Admin	Operate	Speed/Duplex	Flowctr(R/S)	Maclearn	Status
8	enable	down	auto	off/off	enable	Forward

Show port description.

Raisecom#**show interface port 8 descriptor**

Port Description

8 *this-is-a-port*

3.13 Typical configuration

Show Port 9 statistics.

Port 9

Input Normal Statistics:

<i>InOctets:</i>	<i>15,960</i>
<i>InUcastPkts:</i>	<i>183</i>
<i>InMulticastPkts:</i>	<i>0</i>
<i>InBroadcastPkts:</i>	<i>10</i>

Input Error Statistics:

<i>DropEvents(Pkts):</i>	<i>0</i>
<i>CRCAlignErrors(Pkts):</i>	<i>0</i>
<i>UndersizePkts:</i>	<i>0</i>
<i>OversizePkts:</i>	<i>0</i>
<i>Fragments(Pkts):</i>	<i>0</i>
<i>Jabbers(Pkts):</i>	<i>0</i>
<i>Collisions(Pkts):</i>	<i>0</i>

Output Normal Statistics:

<i>OutOctets:</i>	<i>12,846</i>
<i>OutUcastPkts:</i>	<i>164</i>
<i>OutMulticastPkts:</i>	<i>0</i>
<i>OutBroadcastPkts:</i>	<i>1</i>

Output Error Statistics:

<i>OutputError(Pkts):</i>	<i>0</i>
<i>OutputDiscard(Pkts):</i>	<i>0</i>
<i>Abort(Pkts):</i>	<i>0</i>
<i>Differred(Pkts):</i>	<i>0</i>
<i>LateCollisions(Pkts):</i>	<i>0</i>
<i>NoCarrier(Pkts):</i>	<i>0</i>
<i>LostCarrier(Pkts):</i>	<i>0</i>
<i>MacTransmitError(Pkts):</i>	<i>0</i>

Bit Statistics:

<i>Ingress Bits:</i>	<i>127,680</i>
<i>Egress Bits:</i>	<i>102,768</i>

Please press <Ctrl+C> to stop.

2. Set dynamic statistics time as 10s on port 5.

Raisecom#config**Raisecom(config)#dynamic statistics time 10****Raisecom(config)#exit****Raisecom#show interface port 5 statistics dynamic***Dynamic statistics period: 10 seconds**Port 5*
-----*Input Normal Statistics:*

```

InOctets:                15,960
InUcastPkts:             183
InMulticastPkts:         0
InBroadcastPkts:         10
Output Normal Statistics:
  OutOctets:              12,846
  OutUcastPkts:           164
  OutMulticastPkts:       0
  OutBroadcastPkts:       1
Bit Statistics:
  Ingress Bits:           127,680
Egress Bits:              102,768
Speed during 10 seconds Statistics:
  Ingress Speed(bps):     12700
  Egress Speed(bps):      10270
  Ingress Speed(pps):     18
  Egress Speed(pps):      15
Please press <Ctrl+C> to stop.

```

3. Restore dynamic statistics time to default value on port 12.

Raisecom#**config**

Raisecom(config)#**no dynamic statistics time**

Raisecom(config)#**exit**

Raisecom#**show interface port 12 statistics dynamic detail**

```

Dynamic statistics period: 2 seconds
Port      12
-----
Input Normal Statistics:
  InOctets:                15,960
  InUcastPkts:             183
  InMulticastPkts:         0
  InBroadcastPkts:         10
Input Error Statistics:
  DropEvents(Pkts):        0
  CRCAlignErrors(Pkts):    0
  UndersizePkts:           0
  OversizePkts:            0
  Fragments(Pkts):         0
  Jabbers(Pkts):           0
  Collisions(Pkts):        0
Output Normal Statistics:
  OutOctets:              12,846

```

<i>OutUcastPkts:</i>	<i>164</i>
<i>OutMulticastPkts:</i>	<i>0</i>
<i>OutBroadcastPkts:</i>	<i>1</i>
<i>Output Error Statistics:</i>	
<i>OutputError(Pkts):</i>	<i>0</i>
<i>OutputDiscard(Pkts):</i>	<i>0</i>
<i>Abort(Pkts):</i>	<i>0</i>
<i>Differred(Pkts):</i>	<i>0</i>
<i>LateCollisions(Pkts):</i>	<i>0</i>
<i>NoCarrier(Pkts):</i>	<i>0</i>
<i>LostCarrier(Pkts):</i>	<i>0</i>
<i>MacTransmitError(Pkts):</i>	<i>0</i>
<i>Bit Statistics:</i>	
<i>Ingress Bits:</i>	<i>127,680</i>
<i>Egress Bits:</i>	<i>102,768</i>
<i>Speed during 2 seconds Statistics:</i>	
<i>Ingress Speed(bps):</i>	<i>63800</i>
<i>Egress Speed(bps):</i>	<i>51300</i>
<i>Ingress Speed(pps):</i>	<i>93</i>
<i>Egress Speed(pps):</i>	<i>82</i>

Please press <Ctrl+C> to stop.

Chapter 4 Link Aggregation

4.1 Basic principle

Link aggregation is to combine several physical Ethernet port into a logical aggregation group. Use the upper class entity of link aggregation service to take the physical links in the same aggregation group as a logical link.

Link aggregation is able to achieve egress/ingress load-sharing among the aggregation member port to increase bandwidth. At the same time, the member ports of the same aggregation group will dynamically backup each other, which increase the connection stability.

In the same link aggregation, members group able to achieve egress/ingress load-sharing must have a consistent configuration. These configurations include STP, QoS, QinQ, VLAN, port attributes, MAC address learning and so on, as following table shows:

Classification	Details
STP configuration consistent	Port STP enable / disable status, the link attributes connected to the port (such as point-to-point or not-point-to-point), the port traceroute cost, STP priority, message transmitting rate limit, loopback protection configuration or not, Root protection configuration or not, the edge port or not.
QoS configuration consistent	Flow control, flow shaping, congestion avoidance, port speed-limit, SP queues, WRR queue scheduling, WFQ queues, port priority, port trust mode.
QinQ configuration consistent	Port QinQ function enable/ disable status, the added outer-layer VLAN Tag, the strategy to add outer layer VLAN Tag for different inner layer VLANID
VLAN configuration consistent	Port allowed VLAN, port default VLAN ID, port link type (i.e., Trunk, Hybrid, and Access type), sub-net VLAN configuration, protocol VLAN configuration, VLAN packet with a Tag or not
Port Property configuration consistent	Whether to join the isolation group on port, port speed, duplex mode, and up / down status.
MAC address learning configuration consistent	Whether have the MAC address learning function, whether the port with restrictions to number of the greatest learning MAC addresses, whether to continue forwarding control. after MAC table

4.2 LACP aggregation function

LACP (Link Aggregation Control Protocol, Link Aggregation Control Protocol) is a standard protocol based on IEEE802.3ad. LACP protocol has interactive information with peer end through LACPDU (Link Aggregation Control Protocol Data Unit). Enable a port LACP protocol, the port will notify peer-end system LACP protocol priority by transmitting LACPDU, the system MAC, port LACP protocol priority, port ID and operation Key. After Receipt of LACPDU on peer-end, will compare one of the information with other ports information received to select the port can be in **Selected** state and thus both sides can agree on **Selected** state. When operation Key is the link

aggregation, the aggregation control depending on port configuration (i.e., rate, duplex mode, up / down status, basic configuration and other information) automatically generates a configuration combination. In link aggregation the port in **Selected** status have the same operation Key.

In a static aggregation group, the port may be in two states: active or standby: both active port and standby port can transmit and receive lacp protocol, but standby ports cannot forward the user messages.

In a static aggregation group, the system set the port in active or standby status in accordance with the following principles:

System according to whether they found a neighbor, port rate, port priority, port ID priority, choose the highest priority port as the default port, the default port is in active state, with the same rate of the default port, peer-end equipment and operation key ports on peer-end equipment are also in active state. Other ports are in a standby state.

4.3 Classification

In accordance with the different aggregation methods, link aggregation can be divided into two categories:

- manual aggregation
- static LACP aggregation

4.4 Manual aggregation

4.4.1 Default configuration

Function	Default
Link aggregation function	Enable
Link aggregation group	Does not exist, need to configure manually
Loading-sharing mode	Source, destination MAC address logic OR result selects the forwarding port

4.4.2 Manual aggregation configuration

Trunk group

Users can configure the link aggregation function as the following steps:

Step	Command	Description
1	config	Enter global configuration mode
2	trunk group <i>trunk-group-id portlist</i>	Add a aggregation group <i>trunk-group-id</i> : created aggregation ID, range in 1-6. <i>portlist</i> : The physical port ID list, using ',' and '-' to do multi-port input.
3	trunk {enable/disable}	Enable or disable link aggregation
4	exit	Exit global configuration mode and enter the

5	show trunk	privileged user mode Show enable link aggregation or not at present, load balancing mode of link aggregation, group member ports set by all of current trunk groups and the member port currently in effect.
---	-------------------	---

Use **no trunk group** *trunk-group-id* to delete specified aggregation.

Loading-sharing mode

There are six kinds of link aggregation load-sharing mode:

mac: select the forward port based on source MAC address.

dmac: select the forward port based on destination MAC address.

sxordmac: select the forward port based on the result of logical operation “or” of source MAC address, destination MAC address.

sip: select the forward port based on source IP address.

dip: select the forward port based on target IP address.

sxordip: select the forward port based on the result of logical operation “or” of source MAC address, destination MAC address.

Step	Command	Description
1	config	Enter global configuration mode
2	trunk loading-sharing mode { <i>smac</i> / <i>dmac</i> / <i>sxordmac</i> / <i>sip</i> / <i>dip</i> / <i>sxordip</i> }	Configure loading-sharing mode for all link aggregation.
3	exit	Exit global configuration mode
4	show trunk	Show enable link aggregation or not at present, load balancing mode of link aggregation, group member ports set by all of current trunk groups and the member port currently in effect.

Use **no trunk loading-sharing mode** to restore the default mode of link aggregation loading-sharing.

Note: This command is only supported in part of the equipment; the specific circumstances need to refer to the command manual.

4.5 Static LACP aggregation function

4.5.1 Default configuration

Function	Default value
Link aggregation	On
Link aggregation group	Does not exist, manual configuration is needed
Loading-sharing mode	Source, destination MAC address logic OR result selects the transmission port

4.5.2 Configure static LACP aggregation

Follow the following step to configure link aggregation:

Step	Command	Description
1	config	Enter global configuration
2	lacp system-priority <i>system-priority</i>	Configure the system LACP protocol priority
3	trunk group <i>trunk-group-id portlist</i>	Create a static LACP aggregation group; <i>trunk-group-id</i> : the created aggregation group number, range is 1-6; <i>portlist</i> : physical port number list, use ',' and '-' to do multi-interface input
4	interface interface-type interface-number	Enter Ethernet port view
5	lacp port-priority <i>port-priority</i>	Configure the port LACP protocol priority
6	lacp mode <i>{active/passive}</i>	Configure the port LACP protocol mode
7	trunk {enable/disable}	Enable/disable link aggregation
8	show trunk	Show if link aggregation is on, link aggregation load balancing mode, the group member port configured by all the aggregation groups and the effective member port
9	show lacp sys-id	Shows device ID of local-end system, including the system LACP protocol priority and system MAC address.
10	show lacp internal	Show configuration and status of local-end system LACP protocol port
11	show lacp neighbor	Show port LACP protocol neighbor information
12	show lacp statistics	Show port LACP protocol statistics information

Use **no trunk group** *trunk-group-id* to delete the specified aggregation group.

4.6 Trunk min-active links

4.6.1 Default configuration

Feature	Default Value
Trunk min-active link	On
The min-active links	1
Trunk group	No exist, configured by manually
Load-sharing	The port number is computed by the last three bits of message source MAC and destination MAC address XOR result.

4.6.2 Function configuration

Step	Command	Description
1	config	Enter global configuration
2	trunk group <i>trunk-group-id</i> min-active links <i>threshold</i>	Configure min-active links to threshold

4.7 Monitoring and maintaining

Use **show** to look over link aggregation configuration.

Command	Description
show trunk	Show enable link aggregation or not at present, load balancing mode of link aggregation, group member ports set by all of current trunk groups and the member port currently in effect.
show lacp sys-id	Shows device ID of local-end system, including the system LACP protocol priority and system MAC address.
show lacp internal	Show configuration and status of local-end system LACP protocol port
show lacp neighbor	Show port LACP protocol neighbor information
show lacp statistics	Show port LACP protocol statistics information

Use **show trunk** to show if link aggregation is enabled, link aggregation load-sharing mode, all the group member port that is configured by aggregation group and the current effective member port. The current effective member port is the port list that the port state is UP in the configured group member ports. The example below is echo in the actual result:

Raisecom#**show trunk**

```

Trunk: Enable
Loading sharing mode: SXORDMAC
Loading sharing ticket algorithm: :
Trunk Group      Member Ports      Efficient Ports
.....:-
3                 1,4-6,8           1,4

```

Use **show lacp sys-id** shows LACP protocol global enabled situation as well as Device ID including LACP priority and system MAC addresses.

Raisecom#**show lacp sys-id**

Global LACP function: Enabled

```
32768, 000E.5E3D.3C79
```

Use **show lacp internal** display LACP protocol port configuration and status in local-end system.

Show LACP protocol neighbor information, flag, port priority, device ID, Age, operation keys, peer port ID, status of peer port state machine.

There are two kinds port status: Active and standby.

Active indicates that the port has been selected to participate in transmitting. Standby indicates that the port is not selected, and does not participate in forwarding.

Signs are expressed by two letters, the meaning are as following:

S - Device is requesting Slow LACPDUs

F - Device is requesting Fast LACPDUs

A - Device is in Active mode

P - Device is in Passive mode

Admin Key port and operation key port are belonged to same trunk group number.

Status of the port state machine is composed by 8 bit: bit 0 is in the lowest position.

Bit 0: LACP is enabled flag. 1: enable; 0: disabled

Bit 1: LACP flag of the timeout. 1 indicated a short time-out; 0 indicates a long time-out

Bit 2: that the port where the sender whether the link aggregation. 1: yes; 0: no

Bit 3: Transmitting end considers port link is in synchronization status or not. 1: yes; 0: no

Bit 4: Transmitting end considers port link is in the collection status or not. 1: yes; 0: no

Bit 5: Transmitting end considers port link is in distribution state. 1: yes; 0: no

Bit 6: Receiver state machine in transmitting end is in default status. 1: yes; 0: o

Bit 7: Receiver state machine in transmitting end is in timeout status. 1: yes; 0: no

Raisecom#show lacp internal

Flags:

S - Device is requesting Slow LACPDUs

F - Device is requesting Fast LACPDUs

A - Device is in Active mode

P - Device is in Passive mode

Port State	Flags	Port-Pri	Admin-key	Oper-key	Port-State
.....-					
1 standby	SA	32768	0x1	0x1	0x7D
2 active	SA	32768	0x1	0x1	0x3D
3 standby	SA	32768	0x1	0x1	0x7D
4 standby	SA	200	0x1	0x1	0x7D

Use **show lacp neighbor** display port LACP protocol neighbor information.

LACP protocol neighbor information in showing port, concluding flag, port priority, device ID, age, operation key, peer port ID and peer port state machine state.

Age refers to time of the port received the final LACP protocol message to the present time.

The meaning of Flag and port state machine state is the same as command **show lacp internal**

Raisecom#show lacp neighbor

Flags:

S - Device is requesting Slow LACPDUs

F - Device is requesting Fast LACPDUs

A - Device is in Active mode

P - Device is in Passive mode

Port	Flags	Port-Pri	Dev-ID	Age	Oper-key	Parter-Port	Port-State
.....-							
1	SP	0	0000.0000.0000	0s 0x0	0x0		0x8
2	SA	32768	000B.4634.9580	26s 0x1	0x2		0x3D
3	SP	0	0000.0000.0000	0s 0x0	0x0		0x8
4	SP	0	0000.0000.0000	0s 0x0	0x0		0x8

show lacp statistics is used to show port LACP protocol statistics, including the total transceiver number of LACP message, transceiver number of Marker message, transceiver number of Marker Response message and the number of error messages.

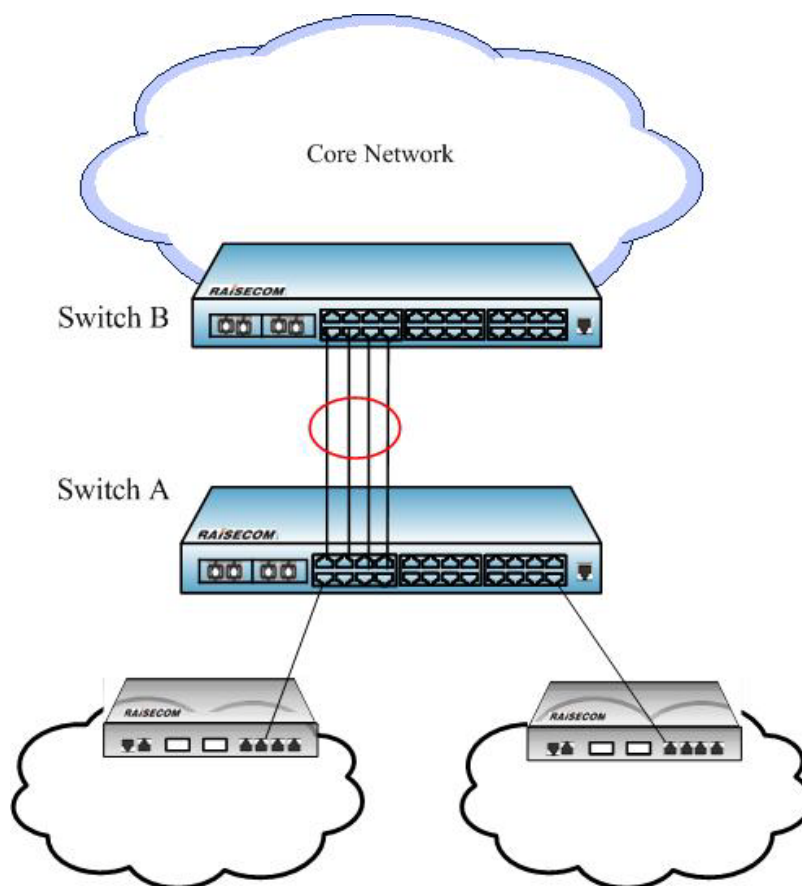
Raisecom#**show lacp statistics**

LACPDUs			Marker		Marker Response		LACPDUS
Port	Send	Recv	Send	Recv	Send	Recv	Pkts Err
.....-							
1	89	0	0	0	0	0	0
2	90	102	0	0	0	0	0
3	89	0	0	0	0	0	0
4	89	0	0	0	0	0	0

4.8 Typical configuration example

4.8.1 Manual aggregation

SwitchA uses 4 ports aggregation to access Switch B, through which egress/ingress load can be shared between the members. SwitchA access ports are port1~port 4.



SwitchA configuration step

1) Configure aggregation group, join the port into the aggregation group:

SwitchA **#config**

SwitchA (config)**#trunk-group 1port 1-4**

2) Configure the load-sharing mode of trunk link aggregation:

SwitchA (config)**#trunk loading-sharing mode smac**

3) Enable link aggregation function:

SwitchA (config)**#trunk enable**

SwitchA (config)**#exit**

SwitchA **#show trunk**

Trunk: Enable

Loading sharing mode: SMAC

Loading sharing ticket algorithm: :

<i>Trunk Group</i>	<i>Member Ports</i>	<i>Efficient Ports</i>
--------------------	---------------------	------------------------

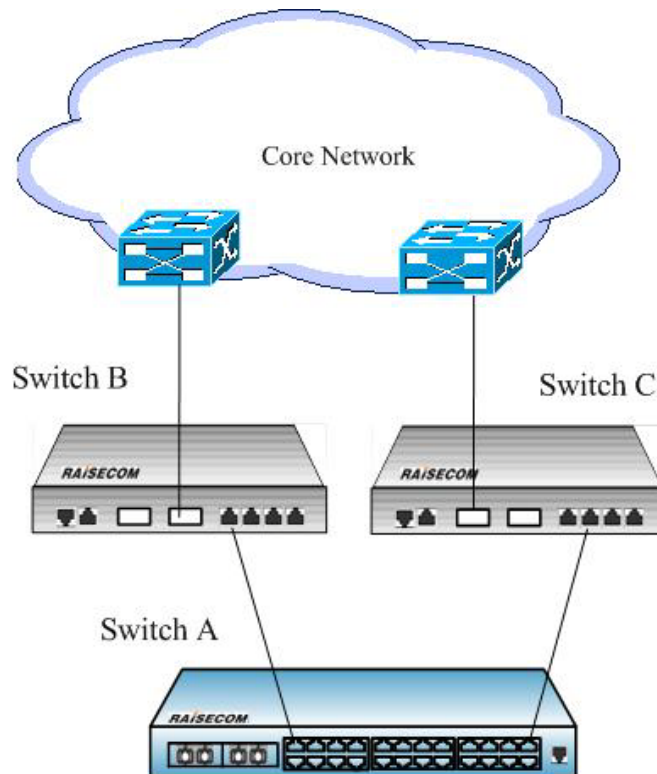
.....:-

<i>1</i>	<i>1-4</i>	<i>1-4</i>
----------	------------	------------

SwitchB has the same configuration with Switch A.

4.8.2 Static LACP aggregation

Static LACP has the typical Dual-homing application topology as below, on SwitchA configures trunk group, in the mode of static LACP. The SwitchB and SwitchC, without supporting LACP, may realize redundancy backup for high reliability.



The following steps are only for SwitchA because SwitchB and Switch C need not the configuration

Configuration step

1) Configure static LACP aggregation group, join the port into the trunk group:

SwitchA #**config**

SwitchA (config)#**trunk-group 1 port 1,24 lacp-static**

2) Enable trunk function:

SwitchA (config)#**trunk enable**

SwitchA (config)#**exit**

SwitchA #**show trunk**

Trunk: Enable

Loading sharing mode: SMAC

Loading sharing ticket algorithm: ;

Trunk Group

Member Ports

Efficient Ports

.....:-

1

1,24

1

Chapter 5 STP Configuration Guide

5.1 STP/RSTP principle introduction

5.1.1 STP purpose

STP (Spanning Tree Protocol) is founded according to 802.1D created by IEEE association, which is used for deleting data link layer physical loop protocol in local area network. The equipments that is running the protocol find loop in the network through exchanging message, and stop some ports selectively, then cut the loop network structure into tree network without any loop, which stop message breeding and looping endlessly, and avoid the host's message handling ability to decline because of receiving the same message.

STP has two meanings, narrowly-defined STP strands for the STP protocol defined in IEEE 802.1D, broadly-defined STP stands for the STP protocol defined in IEEE 802.1D and the modified spanning tree protocols based on it.

5.1.2 STP message

The protocol message STP uses is BPDU (Bridge Protocol Data Unit), which is also called configuration message.

STP transmits BPDU among equipments to make sure the network topology structure. There is enough information to make sure that the equipment finishes the spanning tree's computing.

BPDU is sorted into two types in STP:

- Configuration BPDU: the message that is doing spanning tree computing and spanning tree topology maintenance.
- TCN BPDU (Topology Change Notification BPDU): the messages used for informing the related equipments network topology change when topology structure changes.

5.1.3 STP overview

1. Root bridge

Root bridge is necessary for tree form network structure, so the concept of Root Bridge is taken into STP. There is only one root bridge all through the network, which changes according to network topology's change, so it is not stable.

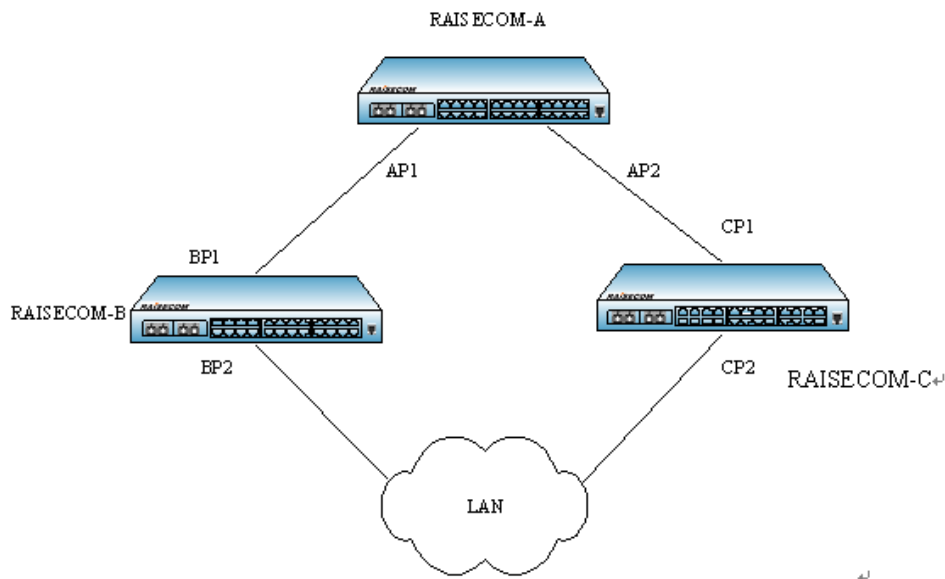
After network convergence, the root bridge will create and send out configuration BPDU in accordance with a certain time interval, while the other equipments will transmit the configuration BPDU, to keep the topology stability.

2. Root port

Root port means the port that is nearest to root bridge on a not-Root Bridge equipment, which sees to the communication to root bridge. There is only one root port on not-Root Bridge equipment, no root

port on root bridge.

3. The designated bridge and port



The designated bridge and port

The designated bridge and port is shown above, AP1, AP2, BP1, BP2, CP1, CP2 stands for the ports of Device A, Device B, Device C respectively.

Device A uses port AP1 to transmit configuration message to Device B, then the designated bridge of Device B is Device A, the designated port is AP1 of Device A.

There are two equipments that connect local area network: Device B and Device C. If Device B sees to transmitting configuration messages to LAN, the LAN designated bridge is Device B, the designated port is BP2 of Device B.

Notice: all the ports on root bridge are designated ports.

4. path cost

Path cost is the reference value for STP selecting links. By computing path cost, STP chooses the 'strong' link, jams the redundant links and cuts the network into tree form network structure without any loop.

5.1.4 Basic principle

STP algorithm:

✧ Initialized state:

Each equipment will generate the BPDU message information that take itself as root bridge when it is initialized, the path cost is 0, designates bridge ID as the equipment its own ID, and designated port is the local port.

✧ Optimal allocation information selection:

Each device sends out its own configuration information, and receives the configuration information of the other equipments. The process when each port receives configuration information is shown below:

- When the configuration information the port received is lower in priority than its own one, the equipment will drop the information received, and take no action to the port's configuration information.
- When the configuration information the port received is higher in priority than its own one, the equipment will replace the configuration information content of its own with the received configuration information content.
- Compare all the ports' configuration information and select the optimal configuration information.

Configuration information compare principle:

- The smaller ID configuration information has higher priority;
- If root bridge ID is the same, compare the following configuration information priority and take the higher priority as the root bridge: the designed bridge ID, the designed port ID, the designed port ID, the port ID that receives the configuration information.

✧ Root bridge selection

When the network is initialized, all the STP equipments in the network will take themselves' root bridge, the root bridge ID is its own bridge ID. Through exchanging configuration information, the root bridge ID will be compared between the equipments, and the equipment that has the smallest root bridge ID in the network will be selected as the root bridge.

✧ Root port, the designed port selection

Root port is the port which has the least root bridge path cost, which is used for transmitting data to root node. If several ports have the same path cost to root bridge, the port that has the lowest port priority will be the root port.

Designated port: the port that transmits data to the downstream switch, at the same time sends STP message to maintain the spanning tree state.

STP configuration information transmission mechanism:

- When the network is initialized, all the equipments will take themselves as root bridge, and generate the configuration message that take themselves as root, then send the message out in the term of Hello Time;
- If the port that received configuration information is root port, and the received configuration information is higher in priority than the port configuration information, then the equipment will add Message Age which is taken in configuration message in a certain principle, and start timer to time this configuration, at the same time the configuration information will be transmitted from the designated port of the equipment.
- If the configuration message the designated port received is lower in priority than its own port's configuration message, it will send out better configuration message as response immediately.
- If there is fault on one path, the root port on the path will no longer receive any configuration information new, while the old configuration information will be dropped because of overtime, then the equipment will regenerate the configuration information that take itself as root and send out BPDU and TCN BPDU to trigger spanning tree's re-computing and get a new path to replace the faulted link, which will revert network connection.

However, the new configuration information getting from re-computing will not spread all through the network immediately, so the old root port and designated port will not realize the network topology change and continue transmitting data in the old path. If the newly selected root port and designated port start data transmitting immediately, provisional loop may happen.

STP timer:

- Forward Delay: the delay time of the switch state transformation. Link fault will trigger the network re-compute the spanning tree, and the spanning tree structure will change

correspondingly. But the new configuration information that has just been re-computed will not spread all through the net immediately, if the newly selected root port and the designated port start data transmission immediately, it may bring temporary path loop. To stop it, STP take state transformation mechanism. The root port and designated port need to go through a betweenness stage before transmitting data, the stage can enter Forwarding stage only after two times Forward Delay time delay, which confirms that the configuration message has spread all through the network;

- Hello Time is used for detecting if there is fault in the link. The switch will send hello message out every Hello Time to check out if the link has any fault;
- Max Age is the parameter used to judge if the configuration information stored in the switch is 'out of time', the switch will drop the overtime configuration information.

5.1.5 RSTP principle overview

RSTP adds the mechanism that the port can transform from jam state to transmission state on the base of ordinary STP protocol, which quickens the topology convergence speed. In the pot to pot link that is connected with only two switch ports, proposal/agreement mechanism can be brought in and only the designated port's one handshake with downstream bridge, so that the link can be transformed quickly. The port that is connected directly to the terminal, not the other bridges, is defined as edge port, which can go directly into transmission state without out any delay. Because the bridge cannot know if the port is connected with the terminal, manual configuration is needed.

5.1.6 STP related protocol and standard

The related protocol includes:

- IEEE 802.1D: Spanning Tree Protocol;
- IEEE 802.1w: Rapid Spanning Tree Protocol;
- IEEE 802.1s: Multiple Spanning Tree Protocol.

5.2 Configure STP

5.2.1 Default STP configuration

Function	Default
Global STP function	Disable
Port STP function	Enable
STP and port priority	128
STP and system priority	32768
Network diameter	7
Port cost	Usually according to the physical feature the default value is shown below: 10Mbps: 2000000 100Mbps: 200000 1000Mbps: 20000 10Gbps: 2000
The maximum package number every hello time	3

max-age timer	20s
hello-time timer	2s
forward-delay timer	15s

5.2.2 root

Step	Command	Description
1	config	Enter global configuration mode
2	spanning-tree root <i>{primary, secondary}</i>	Set the switch to root switch or back-up root switch for spanning tree
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show STP configuration

5.2.3 Port priority configuration

Step	Command	Description
1	config	Enter global configuration
2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical port mode
3	[no] spanning-tree priority <i><0-240></i>	Set port priority for spanning tree
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show STP configuration

5.2.4 Switch priority configuration

Step	Command	Description
1	config	Enter global configuration mode
2	[no] spanning-tree priority <i><0-61440></i>	Set the switch priority for spanning tree <i>0-61440</i> the switch priority
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show STP configuration

5.2.5 path-cost

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical port mode <i>1-MAX_PORT_NUM</i> : the equipment port number
3	[no] spanning-tree path-cost <i><0-200000000></i>	Set port inner path cost for spanning tree <i>0-200000000</i> : port inner path cost
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show STP configuration

5.2.6 transmit-limit

Use this command to configure the maximum BPDU number that is allowed to be sent every Hello Time for MSTP. The parameter is a relative value, without any unit. The larger the parameter is set, the larger the message number that is allowed to be sent every Hello Time, and the more switch resource will be cost. Like time parameter, the configuration will take effect only in the root switch. By default, the value is 3. The configuration step is show below:

Step	Command	Description
1	config	Enter global configuration mode
2	[no] spanning-tree transit-limit <i><1-10></i>	Set the switch maximum sending rate
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show MSTP configuration

5.2.7 STP timer

- The switch has three time parameter: Forward Delay, Hello Time and Max Age:
 - Hello Time: the time interval of the switch sending the bridge configuration information (BPDU), which is used for the switch to detect if there is default with the link. Every Hello Time, the switch will send hello message to the switches around to make sure if there is default with the link.

The default value is 2s, user can change the value according to the network situation. When there are frequent changes in the network links, the value can be shortened to enhance the spanning tree protocol stability. Contrarily, enlarging the value will reduce the resource occupancy rate to system CPU of STP.

- Forward Delay: confirm the time parameter of the switch's state transplant. Link fault will bring the network re-computing the spanning tree, and the STP structure will change accordingly, but the new configuration information by computing will not spread all through the network. If the newly selected root port and the specified port start data transmission immediately, provisional route cycle may happen. To prevent this, the

protocol take a state transplant mechanism: the root port and designated port will have to go through a betweenness before data transmission, and only when the betweenness goes through Forward Delay can the ports enter transmission state. This delay confirms that the new configuration information has spread all through the network.

The default value is 15s, user can change it according to the situation, increase the value when the network topology change is not frequent, and decrease it on the contrary.

- **Max Age:** the bridge configuration information that STP uses has lifecycle to judge if the configuration information is out of time. The switch will drop the outdated configuration information. When the bridge configuration information is out of time, the spanning tree protocol will re-compute the spanning tree.

The default value is 20s, a smaller value will result in the spanning tree re-computing much too frequent, while a value that is much too large will lead to the spanning tree protocol unfitness to the network topology structure change.

Step	Command	Description
1	config	Enter global configuration mode
2	[no] spanning-tree hello-time <1-10>	Set the switch time parameter Hello Time
3	[no] spanning-tree forward-delay <4-30>	Set the switch time parameter Forward Delay
4	[no] spanning-tree max-age <6-40>	Set the switch time parameter Max Age
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

5.3 Configure edge port

5.3.1 STP mcheck

There are two working mode on the switch that supports MSTP: STP compatible mode and MSTP mode. If in a network the port of the switch that is running MSTP is connected with the switch that is running STP, the port will change into STP compatible mode automatically. But if the switch that is running STP is removed, the port cannot change into MSTP mode automatically, but still works in STP compatible mode. Of course, if the port receives new STP message later, the port will return to STP compatible mode. The configuration step is shown below:

Step	Command	Description
1	Config	Enter global configuration mode
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> the maximum port number that the equipment supports.
3	spanning-tree mcheck	Force the port to move back to MSTP mode
4	exit	Return to global configuration mode

5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

5.3.2 STP/RSTP mode

Step	Command	Description
1	config	Enter global configuration mode
3	spanning-tree mode <i>{stp/rstp/mstp}</i>	Configure spanning tree work mode
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

5.3.3 link-type

The two ports that is connected by point to point link can move to transmission state rapidly through transmitting synchronal message, which decreases unnecessary transmission delay time. By default, MSTP sets the link type of the port according to duplex state. Full duplex port is thought to be point to point link, while half duplex is thought to be shared link.

Users can configure by hand to force the current Ethernet ports and point-to-point link connected, but if the link point-to-point link is not a problem in the system would, under normal circumstances, the proposed user of this configuration is set automatically, by Automatic port discovery is linked with point-to-point link. Reverse order no spanning-tree link-type link state port to restore the default values. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> : the maximum port number that the equipment supports
3	spanning-tree link-type <i>{point-to-point / shared}</i>	Set the port's link type
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration.

5.3.4 clear statistics

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> the maximum port number that the equipment supports.
3	spanning-tree clear statistics	Clear the port stat. information to zero
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

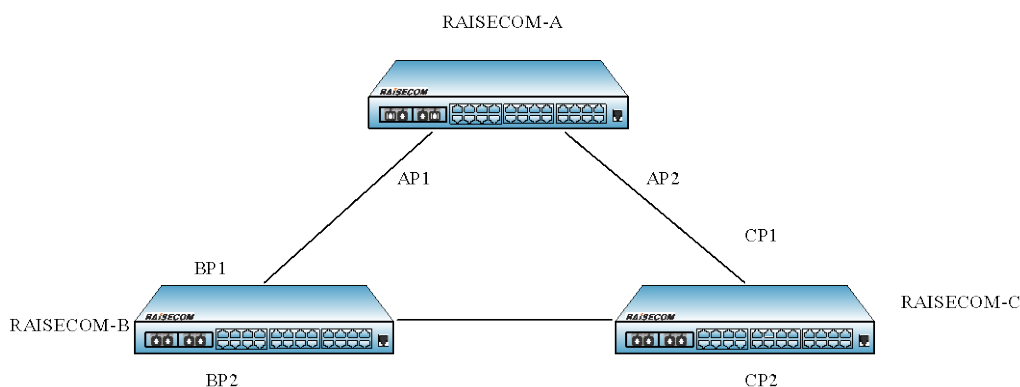
5.3.5 Monitoring and maintaining

Command	Description
show spanning-tree	Show the basic information of spanning tree.
show spanning-tree detail	Show the detailed information of the spanning tree.
show spanning-tree port-list <i>[portlist]</i>	Show the basic information of the spanning tree port list.
show spanning-tree port-list <i>[portlist] detail</i>	Show the detailed information of the spanning tree port list.

5.3.6 Typical configuration instance

There are 3 RAISECOM switch, A, B, C increase according to the equipment MAC address. By configuring the switch priority to select the root bridge to A or B freely, so that the topology can be changed.

Network structure figure:



Network structure

Configuration steps:

Open A, B, C global STP:

```
Raisecom(config)#spanning-tree enable
```

Set the STP working mode of port AP1, AP2, BP1, BP2, CP1, CP2 to RSTP;

By default, check out the stable topology structure:

```
Raisecom#show spanning-tree
```

A: the switch's AP1, AP2, as the designated port is in normal transmission state;

B: the switch's BP1, as the root port, is in normal transmission state, while BP2 is in block state;

C: the switch's CP1, as the root port, is in normal transmission state, while CP2 is in block state;

Set the priority of B to 4096, and repeat the following step:

```
Raisecom(config)#spanning-tree priority 4096
```

When the topology is stable the root bridge will change into A, the port AP2, BP1 between A and c will be in block state.

MSTP configuration.

5.4 MSTP principle introduction

5.4.1 MSTP overview

MST regions (Multiple Spanning Tree Regions), is made of several switches in the switch network and the network segments between them. These switches have all started MSTP, own the same region name, VLAN to spanning tree mapping configuration and the same MSTP modification class configuration, and have physical link connection.

MSTI (Multiple Spanning Tree Instance) is the spanning tree in the MST region. A MST region can create several spanning trees through MSTP, each tree is independent.

VLAN mapping table is an attribution of MST region. IST and CST (Common Spanning Tree) constitute the switch network spanning tree (Common and Internal Spanning Tree). IST is part of CIST in MST region, which is a special multi-spanning tree instance.

CST is the simple spanning tree connecting all the MST region in the switch network. If each MST is seen as a 'switch', CST is a spanning tree computed by the 'switches' using STP and RSTP.

CIST is a single spanning tree connected with all the MST region in the switch network, which is formed by IST and CST.

Region root means the tree root of IST and MSTI in the MST region. The topology of each spanning tree in the MST region is different, so the region root may be different as well. Common Root Bridge means the tree root of CIST.

5.4.2 MSTP principle

MSTP divide the two-layer network into several MST region, between each region the CST is

created by computing, while in the region several spanning tree is created by computing by computing, each spanning tree is called a MSTI.

➤ The computing of CIST spanning tree

After comparing the configuration information, the switch that has the highest priority all through the network will be selected as the tree root of the switch. In each MST region MSTP will create IST through computing, while MSTP will treat each MST region as a single switch, and create CST in the MST region by computing. CST and IST constitute the switch network CIST.

➤ MSTI computing

In the MST region, according to the mapping relationship between VLAN and the spanning tree instance, MSTP will generate different spanning tree instance for different VLAN. Each spanning tree will make calculation respectively, the calculation process is similar with the process of STP/RSTP spanning tree computing.

➤ STP algorithm process

It is the same with STP/RSTP.

5.5 MSTP configuration

5.5.1 The default MSTP configuration

Function	Default value
Global MSTP function	Disabled
PORT MSTP function	Enabled
Max jump number of MST region	20
The priority of STP port	128
The system priority of STP	32768
Network diameter	7
Port cost	According to the physical features, the usual situation by default is show below: 10Mbps: 2000000 100Mbps: 200000 1000Mbps: 20000 10Gbps: 2000
Max packet sent out number every Hello Time	3
max-age timer	20s
hello-time timer	2s
forward-delay timer	15s
MST region modifying priority	0

5.5.2 region-configuration

When the switch running in MSTP mode, the switch can be configured the region information where

it belongs to. Which MST region a switch belongs to is determined by the region name, VLAN mapping table and MSTP modification configuration. By the following steps user can put the current switch into a special MST region.

Note: MST region configuration view is used here. To configure MST region name, modification class and the relationship between VLAN and instances, it is needed to enter MST region view. If the configuration is not enabled, then the configuration information will only be recorded but not activated. The configuration is shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	spanning-tree region-configuration	Enter MST region configuration mode
3	[no] name <i>name</i>	Set MST region name
4	[no] revision-level <i>level</i>	Set MST region modification class; <i>level</i> : modification class, range is 0-65535, the default value is 0
5	instance <i><0-4095></i> vlan <i><1-4094></i>	Set mapping relationship from VLAN to instances for MST region. <i>0-4095</i> : the instance number; <i>1-4094</i> : VLAN ID
6	exit	Return to global configuration mode
7	spanning-tree region-configuration active	Activate MST region configuration information
8	exit	Return to privileged EXEC mode
9	show spanning-tree region-configuration	Show MST region configuration information.

5.5.3 max-hop

MST region maximum hop number confines the scope of MST region. Only when the configured switch is the region root, can the configured maximum hop number be taken as MST region maximum hop number, while other not-region root switches configuration is not valid on it.

From the root switch of the spanning tree in the region, BPDU in the region hop number will decrease by 1 when transmitted by one switch, and the switch will drop the configuration information that receives 0 hop number. It will make the switch that is out of the max hop number not being able to take part in the spanning tree calculation, which confines the scope of MST region.

For instance: if the maximum hop number of the region root switch is set to 1, the spanning tree function in the region is not available, because only this switch takes part in the spanning tree computing. By default, the maximum hop number is 20, or to hop down 19 steps along the spanning tree path from the region root. The configuration is shown below:

Step	Command	Description
1	config	Enter global configuration mode

2	[no] spanning-tree max-hops <1-40>	Set the maximum hop number of the switch MST region
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show MSTP configuration

5.5.4 root

On the one hand, MSTP can configure the switch priority, and then after a spanning tree calculation, to determine the root of the tree root switch to back up or exchange; On the other hand, the user can also specify the order directly. It should be noted that if the root switch designated direct way, then the whole network, users can not modify the proposed switch to any of the priority; Otherwise, the root cause designated switch or switch back up the root is invalid.

Users can instance instance-id parameter to determine the root switch, or switch to back up the root of the entry into force of instance. If the instance-id value is 0, or omit parameters instance instance-id, the current switch will be designated as the root of the CIST or switch to back up the root switch.

In the instance of the current switch in the type of root is independent of each other, that is, it can be used as an instance of the root switch or switch back up the root, at the same time as other instances of tree roots or switch to back up the root switch. But at the same instance of a tree, the same cannot switch it as a root switch and root as a backup switch.

At the same time, the user can not be designated as an instance of spanning tree two or more root switch; On the contrary, the user can specify multiple spanning tree with a back-up roots. Under normal circumstances, the proposal for a user to specify a spanning tree roots and a number of back-up roots.

When the root switch failure or shutdown, the switch can replace the backup root root switch into the corresponding instance of the root switch. However, at this time if the user has set up a new root switch, then switch back up the root will not be a root switch. If a user to configure a number of instances spanning tree root switch back up, when the root switch fails, MSTP will choose the smallest of the MAC address of the switch as a backup root switch.

By default, the switch cannot be taken as the root switch of the spanning tree or the back-up root switch of the spanning tree. Use **no spanning-tree[instance instance-id] root** revert command to restore the default configuration. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	spanning-tree [instance instance-id] root {primary, secondary}	For a certain spanning tree instance, set the switch as the root switch or back-up root switch. <i>instance-id</i> instance number, range is 0-4095
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show MSTP configuration

5.5.5 priority

Spanning tree protocol spanning tree calculation, the elections need to root port (root port) and designated ports (designated port), in the path of the port costs in line under the premise of the port-side ID of the smaller ports more vulnerable to root for the election or designated port. Users can set up port priority, to reduce port ID, and then there's the purpose of controlling spanning tree protocol to choose a specific port to become the root port or the designated port. With the same priority, the port that has smaller number has higher priority.

Same with the priority of configuring the switch, port priority is independent in different cases. Users can use **instance** instance-id parameter to determine the configuration of port-priority case. If the instance-id value is 0 or parameters **instance** instance-id is omitted, it is configured for the CIST port priority.

Note: The value of priority must be a multiple of 16, such as 0,16,32,48 and so on, the default value of 128. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical port mode; <i>MAX_PORT_NUM</i> : the maximum port number that the equipment supports
3	[no] spanning-tree [instance instance-id] priority <0-240>	Set port priority for a certain spanning tree instance <i>instance-id</i> : instance number, range is 0-4095 <i>0-240</i> : port priority value
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

5.5.6 priority

Bridge ID switch determines if the size of this switch can be selected as the root of the tree. Through the allocation of a smaller priority, the smaller switches Bridge ID can be got so that a certain switch can be the spanning tree root. Priority same, small MAC address for the small roots.

Same with the configuration root and backup root, the priority is independent with each other in different instance configurations. Users can use **instance** instance-id parameter to determine the priority allocation of instance. If the instance-id value is 0, or when the parameters **instance** instance-id is omitted, it is configured for the CIST bridge priority.

Note: The value of priority must be in multiples of 4096, such as 0, 4096, 8192, and so on, the default value is 32,768. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode.
2	[no] spanning-tree [instance instance-id] priority <0-61440>	Set port priority for a certain spanning tree instance. <i>instance-id</i> : instance number, range is 0-4095. <i>0-61440</i> : port priority value.

3	exit	Return to privileged EXEC mode.
4	show spanning-tree	Show MSTP configuration.

5.5.7 bridge-diameter

RSTP in the agreement, the network diameter refers to the number of switches in the network to exchange up to the path that, switch the number of nodes. MSTP in the agreement, the network diameter settings only effective CIST for example MSTI invalid. And in the same region, no matter how many nodes path, just as a computing node. This fact, the network should be defined as the diameter across the region up to that path, the number of regions. If the network has only one region, then running network diameter is 1.

MST with the region of the largest jump a few similar, if and only if the switch configuration for the CIST root switch, configure the entry into force.

Comparison of the MST's largest region is used to jump a few region characterization of the size of the network diameter is the characterization of the entire network of the size of a parameter. Network that the greater the diameter of a larger network.

When the user switches to configure the network parameters in diameter, MSTP through the switch will automatically calculate the Hello Time, Forward Delay, and Max Age three times to set the parameters for a better value.

Default network with a diameter of 7, the corresponding three time are their default values respectively. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	[no] spanning-tree bridge-diameter <2-7>	Set the diameter of the switch network
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show MSTP configuration

5.5.8 path-cost

When STP is computing the spanning tree, it is needed to vote root port and designated port, the less the port patch costs, the easier the port be voted as root port or designated port. Users can use **instance** instance-id parameter to determine the instance of the port inner path cost of the configured port. If the instance-id value is 0, or when the parameters **instance** instance-id is omitted, it is configured for the CIST inner patch cost.

Usually port cost depends on the physical features, the default case is:

- 10Mbps is 2000000;
- 100Mbps is 200000;
- 1000Mbps is 20000;

Specific configuration is as follows:

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical interface mode. <i>MAX_PORT_NUM</i> : the maximum port number that the equipment supports.
3	[no] spanning-tree [instance instance-id] path-cost <0-200000000>	Set the port inner patch cost for a certain spanning tree instance. <i>instance-id</i> : instance number, range is 0-4095. <i>200000000</i> : the maximum patch cost value.
4	exit	Return to global configuration mode.
5	exit	Return to privileged EXEC mode.
6	show spanning-tree	Show MSTP configuration.

5.5.9 transit-limit

Use the command to configure the maximum BPDU number that is allowed to be sent every Hello Time for MSTP. This parameter is a relative value, not units, the configuration parameters have been greater, each with Hello Time allowed to send the message, the more the number, but also will take up more resources to switch. With the same parameters of the time, only the root switch configuration comes into force.

By default, this value is 3. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode.
2	[no] spanning-tree transit-limit <1-10>	Set the switch port maximum sending rate.
3	exit	Return to privileged EXEC mode.
4	show spanning-tree	Show MSTP configuration.

5.5.10 STP timer

- There are three time parameter: Forward Delay, Hello Time and Max Age:
 - Hello Time: the time interval of the switch's sending BPDU, which is used to determine if there is fault in the link. Every Hello Time the switch will send hello message to the switches nearby to make sure if there is fault with the link.

The default value is 2s, user can change the value according to the network state. If there is frequent change in network links, the value can be shortened in a certain degree to enhance STP stability. On the opposite, enlarging the value will decrease STP resource taken rate to the system CPU.

- Forward Delay: to make sure the time parameter of the switch state safe transformation. Link fault will bring in the re-computing of the spanning tree and the corresponding change of the network structure, but the new configuration information that is

re-computed cannot spread all through the network. If the newly elected root port and designated port started immediately transmit the data, may cause a temporary path of the loop. To this end an agreement to adopt a state transfer mechanism: the root port and designated port will go through a betweenness before data re-transmission (state of learning), a state in the middle Forward Delay after delay of time before they can enter the state forward. The delay to ensure that the new configuration information has been spread throughout the network.

Default value is 15 seconds, the user can adjust the value of the actual situation, when the network topology changes frequently are not able to reduce the value, increasing the contrary.

- **Max Age:** the bridge configuration information that is used by the spanning tree protocol has life cycle to determine whether the configuration information is out of date. The switch will discard the configuration information out of date. When the bridge configuration information expired, spanning tree protocol will be re-spanning tree.

Default is 20 seconds, the value is too small will lead to weight spanning tree calculation too often, too much will lead to spanning tree protocol in a timely manner can not adapt to the network topology.

The entire network to exchange all of the switches used CIST root switch on the three parameters of the time, only in the root switch configuration on the entry into force. Specific configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	[no] spanning-tree hello-time <1-10>	Set the switch time parameter Hello Time
3	[no] spanning-tree forward-delay <4-30>	Set the switch time parameter Forward Delay
4	[no] spanning-tree max-age <6-40>	Set the switch time parameter Max Age
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

5.5.11 edge port

Edge port: the port that has no direct connection to the switch or indirect connection to any switch through the network.

Configure the edge port so that the port state can transform into transmission state rapidly, without waiting for; for Ethernet port that is has direct connection with user's terminal equipment, it is supposed to be set to edge port for rapid transformation to transmission state.

If a port is set to edge port auto detection (auto), then the attribution of the edge port is decided by the actual situation. If a port is set to edge port (force-true), when the port receive BPDU the actual running value will become not-edge port, which will keep the state until the configuration is changed.

By default, all the network switch ports will be set to auto-detect. The reverse command **no spanning-tree edged-port** restores the default value of the edge port attribution. Specific

configuration is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> : the maximum port number that the equipment supports
3	spanning-tree edged-port <i>{auto force-true force-false}</i>	Set the edge port attribution.
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

5.5.12 STP mcheck

Switch port in support of MSTP has two work modes: STP compatibility mode and MSTP mode. Supposed that in a network switch-port running MSTP connecting a switch operating STP, the port will be automatically moved to STP compatibility mode. But if switch running STP remove, the port cannot automatically moved to MSTP mode, and still work in STP compatibility mode. At this time McHeck operation force it to the MSTP mode. Of course, if this port receive new STP message, the port will return to STP compatibility mode. The specific configurations are as follows:

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical port mode. <i>MAX_PORT_NUM</i> : the maximum port number that the equipment supports.
3	spanning-tree mcheck	Force the port to MSTP mode.
4	exit	Return to global configuration mode.
5	exit	Return to privileged EXEC mode.
6	show spanning-tree	Show MSTP configuration.

5.5.13 STP/MSTP mode

When STP is enabled, two spanning tree mode is supported: STP compatible mode and MSTP mode.

- STP compatible mode: do not implement the rapid transformation from alternate port to root port. Only STP configuration BPDU and topology change notice (STP TCN BPDU) will be sent out. The un-identified part will be dropped when MST BPDU is received.
- MSTP mode: sending MSTP BPDU. If the opposite end of the local switch port is running STP, the port will move to STP compatible mode. If the opposite end of the local switch port is

running RSTP, the local will keep MSTP and take it only as out region information.

The steps to configure the switch spanning tree mode are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	spanning-tree mode <i>{stp mstp}</i>	Set the spanning tree running mode
3	exit	Return to privileged EXEC mode
4	show spanning-tree	Show MSTP configuration

5.5.14 Link type

By transmitting synchronal message the two ports that is connected by point to point link can move to transmission state rapidly, which reduces the unnecessary transmission delay. By default, MSTP set the link type of the port according to duplex state. Full duplex port is seen as point to point link, while half duplex port is seen as shared link.

Users can configure by hand to force the current Ethernet ports and point-to-point links connected, but the system will get into trouble if the link is not point to point link, usually it is supposed that this configuration is set to be auto so that the system will find out if the ports are connected with point to point link. Reverse command **no spanning-tree link-type** recovers the default value of the link state of the port. Specific configuration is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> the maximum port number that the equipment supports
3	spanning-tree link-type <i>{point-to-point shared}</i>	Set the link type of the port
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

5.5.15 Rootguard

Reselect when the bridge received a packet in higher priority, but the new elections weak network connectivity, and consumes CPU resources. As for the network with MSTP enabled, if someone send higher-priority BPDU message to attack, networks would be instable caused by continual election. But generally speaking, each bridge priority has been configured in the network planning stage, the more edge, the lower priority. Therefore, down streaming port generally will not received the highest priority packet than that of the bridge, unless of malicious attacks. For these ports, users can open rootguard, and refused to deal with the packet with high priority than bridge. If received

higher-priority packet, it will block ports for a period of time, to prevent more attacks against upper link.

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode MAX_PORT_NUM the maximum port number that the equipment supports.
3	spanning-tree rootguard {enable / shared}	Set rootguard.
4	show spanning-tree port-list detail	Show MSTP configuration.

5.5.16 Loopguard

Spanning tree has two main functions: prevent loop back and link backup. Loopback prevention requires a topological cut in a tree shape, and link backup needed when the topology has redundant links. Spanning tree is through the obstruction to prevent loopback, and when the link has the failure, enable redundant links for link backup function.

Spanning tree module would periodically exchanged messages, if in a certain time didn't receive a message that regard it as link failures. Then take the election, freeing the backup port. But in practical applications, it may not caused by link failures. In this case, if release the backup port , it will bring a loop back .

The loopguard will not selection when the port in a certain period of time doesn't receive a message, , keep original condition.

Note: The loopguard and link backup are opposite, i.e. they will not take effect at the same time.

Step	Command	Description
1	config	Enter global configuration mode.
2	interface port <1-MAX_PORT_NUM>	Enter Ethernet physical port mode. MAX_PORT_NUM the maximum port number that the equipment supports.
3	spanning-tree loopguard {enable/shared}	Set loopguard.
4	show spanning-tree port-list detail	Show MSTP configuration.

5.5.17 static clear

MSTP counts each MSTP port BPDU message number of the following types: ingress STP message, ingress RSTP message, ingress MSTP message, egress STP configuration message, egress SRTP message (to the switch that is running MSTP, it will be zero forever), egress MSTP message.

The steps to clear MST port statistics are as follows:

Step	Command	Description
1	config	Enter global configuration mode

2	interface port <i><1-MAX_PORT_NUM></i>	Enter Ethernet physical port mode <i>MAX_PORT_NUM</i> the maximum port number that the equipment support
3	spanning-tree clear statistics	Clear the port statistics to zero
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show spanning-tree	Show MSTP configuration

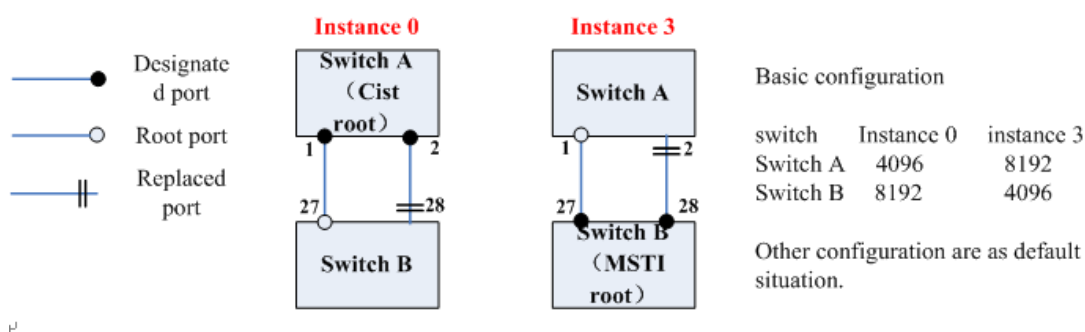
5.6 Maintenance and management

- show spanning-tree region-configuration: show MST region configuration.
- show spanning-tree [instance instance-id]: show multi-spanning tree instance basic information.
- show spanning-tree [instance instance-id] detail: show multi-spanning tree instance detail.
- show spanning-tree [instance instance-id] port-list[portlist]: show the basic information of multi-spanning tree instance port list.
- show spanning-tree [instance instance-id] port-list[portlist] detail: show the detail of multi-spanning tree instance port list.

5.6.1 Show instances

The result shown in the following sections are all according to the instance configuration described in the section, the switch that is for display is switch B in the example, the switch that uses this example is rc2828f (28 ports in all).

1. Topology voting figure and basic configuration



2. MST command configuration

<p>Switch A:</p> <pre> Raisecom#hostname SW_A SW_A#config SW_A(config)#create vlan 11-20 active SW_A(config)#interface port 1 SW_A(config-port)#switchport mode trunk SW_A(config-port)#switchport trunk allowed vlan 11-20 SW_A(config-port)#exit SW_A(config)#interface port 2 SW_A(config-port)#switchport mode trunk SW_A(config-port)#switchport trunk allowed vlan 11-20 SW_A(config-port)#exit SW_A(config)#spanning-tree enable SW_A(config)#spanning-tree mode mstp SW_A(config)#spanning-tree region-configuration SW_A(config-region)#name aaa SW_A(config-region)#revision-level 2 SW_A(config-region)#instance 3 vlan 11-20 SW_A(config-region)#exit SW_A(config)#spanning-tree region-configuration active SW_A(config)#spanning-tree instance 0 priority 4096 SW_A(config)#spanning-tree instance 3 priority 8192 </pre>	<p>Switch B:</p> <pre> Raisecom#hostname SW_B SW_B#config SW_B(config)#create vlan 11-20 active SW_B(config)#interface port 27 SW_B(config-port)#switchport mode trunk SW_B(config-port)#switchport trunk allowed vlan 11-20 SW_B(config-port)#exit SW_B(config)#interface port 28 SW_B(config-port)#switchport mode trunk SW_B(config-port)#switchport trunk allowed vlan 11-20 SW_B(config-port)#exit SW_B(config)#spanning-tree enable SW_B(config)#spanning-tree mode mstp SW_B(config)#spanning-tree region-configuration SW_B(config-region)#name aaa SW_B(config-region)#revision-level 2 SW_B(config-region)#instance 3 vlan 11-20 SW_B(config-region)#exit SW_B(config)#spanning-tree region-configuration active SW_B(config)#spanning-tree instance 0 priority 8192 SW_B(config)#spanning-tree instance 3 priority 4096 </pre>
---	---

5.6.2 Show MST region configuration information

- Command: **show spanning-tree region-configuration**
- Function: to show MST region configuration information, including: the inactive and valid region, modification class and VLAN mapping table.
- Show result:

Raisecom#**show spanning-tree region-configuration**

Configured:

```

.....-
Name: aaa
Revision level: 2      Instances configured: 2
Instance      Vlans Mapped
....          .....
0              1-10,21-4094

```

Operational:

```

.....-
Name: aaa
Revision level: 2      Instances running: 2
Digest: 0x213106D1D279FAE00D24B8297D35EC69
Instance      Vlans Mapped
....
0             1-10,21-4094
3             11-20

```

5.6.3 Show multi-spanning tree instance basic information

- Command: **show spanning-tree** [instance instance-id]
- Function: show all the spanning tree instances or the given spanning tree instance and the port basic information of the instance. Without the parameter **instance** instruction, all the instances and instance port information will be shown.
- Show the result:

Raisecom# **show spanning-tree**

```

MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 0
.....-
BridgeId: Mac 000E.5E00.1864  priority 8192
Root: Mac 000E.83E3.7580  Priority 4096  ExternalRootCost 0
RegionalRoot: Mac 000E.83E3.7580  Priority 4096  InternalRootCost 200000
Operational: hello time 2, forward delay 15, max age 20
Configured: hello time 2, forward delay 15, max age 20
            transmit limit 3, max hops 20, diameter 7

```

PortId	PortState	PortRole	PathCost	PortPriority	LinkType	TrunkPort
1	discarding	disabled	200000	128	point-to-point	no
2	discarding	disabled	200000	128	point-to-point	no
3	discarding	disabled	200000	128	point-to-point	no
4	discarding	disabled	200000	128	point-to-point	no
5	discarding	disabled	200000	128	point-to-point	no
6	discarding	disabled	200000	128	point-to-point	no
7	discarding	disabled	200000	128	point-to-point	no
8	discarding	disabled	200000	128	point-to-point	no
9	discarding	disabled	200000	128	point-to-point	no
10	discarding	disabled	200000	128	point-to-point	no
11	discarding	disabled	200000	128	point-to-point	no

12	discarding	disabled	200000	128	point-to-point	no
13	discarding	disabled	200000	128	point-to-point	no
14	discarding	disabled	200000	128	point-to-point	no
15	discarding	disabled	200000	128	point-to-point	no
16	discarding	disabled	200000	128	point-to-point	no
17	discarding	disabled	200000	128	point-to-point	no
18	discarding	disabled	200000	128	point-to-point	no
19	discarding	disabled	200000	128	point-to-point	no
20	discarding	disabled	200000	128	point-to-point	no
21	discarding	disabled	200000	128	point-to-point	no
22	discarding	disabled	200000	128	point-to-point	no
23	discarding	disabled	200000	128	point-to-point	no
24	discarding	disabled	200000	128	point-to-point	no
25	discarding	disabled	200000	128	point-to-point	no
26	discarding	disabled	200000	128	point-to-point	no
27	forwarding	root	200000	128	point-to-point	no
28	discarding	alternate	200000	128	point-to-point	no

MST ID: 3

```

.....-
BridgeId: Mac 000E.5E00.1864  priority 32768
RegionalRoot: Mac 000E.5E00.1864  Priority 32768  InternalRootCost 0
PortId  PortState  PortRole  PathCost PortPriority  LinkType  TrunkPort
.....:
27  forwarding designated  200000  128  point-to-point  no
28  forwarding designated  200000  128  point-to-point  no

```

5.6.4 Show multi-spanning tree instance detail

- Command: **show spanning-tree [instance instance-id] detail**
- Function: show all the spanning tree instances or the given spanning tree and the detail of the instance port. Without the parameter **instance**, all the instances and the detail of the instance port.
- Show the result:

Raisecom# **show spanning-tree instance 0 detail**

```

MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 0
.....-
BridgeId: Mac 000E.5E00.1864  priority 8192
Root: Mac 000E.83E3.7580  Priority 4096  ExternalRootCost 0
RegionalRoot: Mac 000E.83E3.7580  Priority 4096  InternalRootCost 200000
Operational: hello time 2, forward delay 15, max age 20

```

*Configured: hello time 2, forward delay 15, max age 20
transmit limit 3, max hops 20, diameter 7*

Port 1 :

*State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0*

Port 2 :

*State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0*

Port 3 :

*State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0*

Port 4 :

*State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0*

Port 5 :

*State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0*

Port 6 :

*State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0*

Port 7 :

*State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0*

Port 8 :

*State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0*

Port 9 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 10 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 11 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 12 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 13 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 14 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 15 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 16 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 17 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 18 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 19 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 20 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 21 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 22 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 23 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 24 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 25 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0

RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 26 :

State:discarding Role:disabled Priority:128 Cost:200000 TrunkPort:no
Root: Mac 0000.0000.0000 Priority 0 ExternalPathCost 0
RegionalRoot: Mac 0000.0000.0000 Priority 0 InternalPathCost 0
DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 27 :

State:forwarding Role:root Priority:128 Cost:200000 TrunkPort:no
Root: Mac 000E.83E3.7580 Priority 4096 ExternalPathCost 0
RegionalRoot: Mac 000E.83E3.7580 Priority 4096 InternalPathCost 0
DesignatedBridge: Mac 000E.83E3.7580 Priority 4096 DesignatedPort 32769

Port 28 :

State:discarding Role:alternate Priority:128 Cost:200000 TrunkPort:no
Root: Mac 000E.83E3.7580 Priority 4096 ExternalPathCost 0
RegionalRoot: Mac 000E.83E3.7580 Priority 4096 InternalPathCost 0
DesignatedBridge: Mac 000E.83E3.7580 Priority 4096 DesignatedPort 32770

5.6.5 Show the basic information of multi-spanning tree instance port list

- Command: **show spanning-tree [instance instance-id] port-list [portlist]**
- Function: show all the spanning tree instances or the given spanning tree instance and the port basic information of the instance. Without the parameter **instance** instruction, all the instances and instance port information will be shown.
- Show the result:

Raisecom# **show spanning-tree port-list 27**

```
Port ID:27
EdgedPort:  admin: auto    oper: no
LinkType:   admin: auto    oper: point-to-point
Partner MSTP Mode: mstp
Bpdus send:209 (TCN<0> Config<0> RST<0> MST<209>)
Bpdus received:212 (TCN<0> Config<0> RST<212> MST<0>)
Instance PortState PortRole PortCost(admin/oper) PortPriority
:::
0 forwarding root 200000/200000 128
3 forwarding designated 200000/200000 128
```

5.6.6 Show the detail of multi-spanning tree instance port list

- Command: **show spanning-tree [instance instance-id] detail**
- Function: show all the spanning tree instances or the given spanning tree and the detail of the instance port. Without the parameter instance, all the instances and the detail of the instance

port.

- Show the result:

Raisecom# **show spanning-tree port-list 28 detail**

```
Port ID:28
EdgedPort:  admin: auto    oper: no
LinkType:   admin: auto    oper: point-to-point
Partner MSTP Mode: mstp
Bpdus send:241 (TCN<0> Config<0> RST<0> MST<241>)
Bpdus received:243 (TCN<0> Config<0> RST<0> MST<243>)
This port In mst0 Info:
State:discarding Role:alternate Priority:128 Cost: 200000
Root: Mac 000E.83E3.7580 Priority 4096 ExternalPathCost 0
RegionalRoot: Mac 000E.83E3.7580 Priority 4096 InternalPathCost 0
DesignatedBridge: Mac 000E.83E3.7580 Priority 4096 DesignatedPort 32770
This port In mst3 Info:
State:forwarding Role:designated Priority:128 Cost: 200000
RegionalRoot: Mac 000E.5E00.1864 Priority 32768 InternalPathCost 0
DesignatedBridge: Mac 000E.5E00.1864 Priority 32768 DesignatedPort 32796
```

5.7 Typical configuration instance

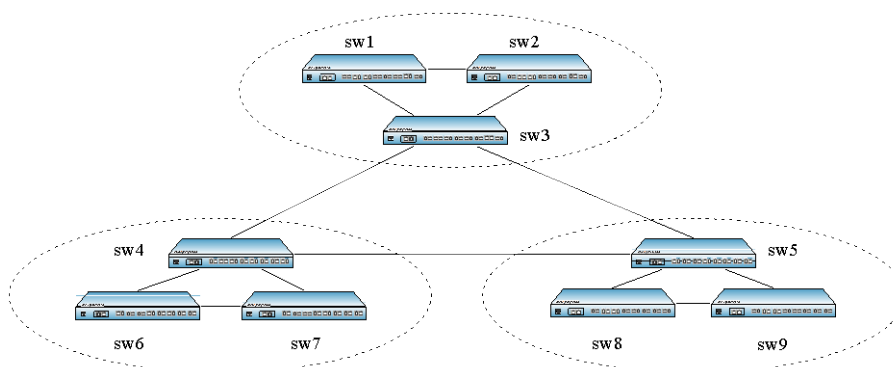
- Destination:

Set sw1, sw2, sw3 to the same MST region MST1, modification class to 2, and map VLAN1 to instance 1, VLAN2 to instance 2, other VLAN to CIST;

Set MST2, MST3 to contain sw4/sw6/sw7, sw5/sw8/sw9, the correspondence that VLAN map to instance is similar to MST1.

Show the final spanning tree voting, configure the CIST that take sw3/sw4/sw5 as switch.

- Network figure



- Configuration step:

Step 1:

Configure MST region configuration information, the region name is MST, modification class is 2, map VLAN2 to instance 2, others to CIST, and enable the configuration information

Raisecom#**config**

Raisecom(config)#**spanning-tree region-configuration**

Raisecom(config-region)#**name MST1**

Raisecom(config-region)#**revision-level 2**

Raisecom(config-region)#**instance 1 vlan 1**

Raisecom(config-region)#**instance 2 vlan 2**

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

Step 2:

Configure MST2 and MST3 in the same way.

Step 3:

To look over the spanning tree configuration information, instance 1 information:

Raisecom#**show spanning-tree region-configuration**

Raisecom#**show spanning-tree instance 1**

MST1, MST2, MST3 form as complete single spanning tree.

Step 4:

Set the electric physical port on MST1, MST2, MST3 region to the member port of VLAN1;

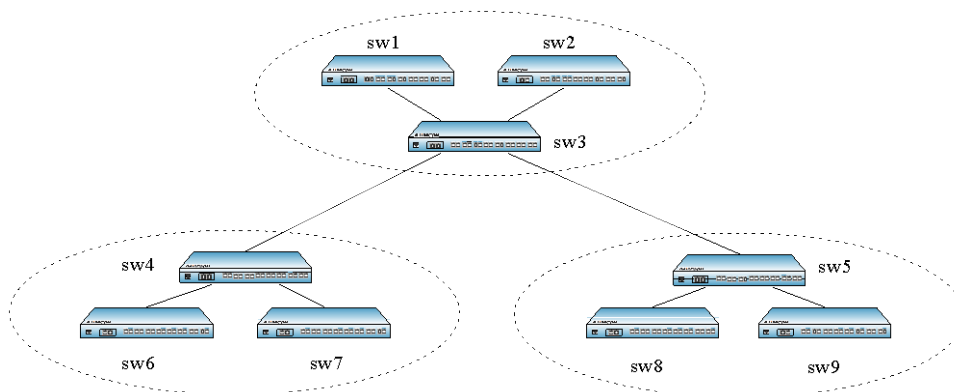
In MST1 region configure the bridge priority of sw3 to 4096, the priority of other switches larger than 4096;

In MST2 region configure the bridge priority of sw4 to 8192, the priority of other switches larger than 8192;

In MST2 region configure the bridge priority of sw5 to 8192, the priority of other switches larger than 8192;

In each region, the topology will vote and create single spanning tree according to STP/RSTP, and create a final tree, the root of which is sw3, and the connection between sw4 and sw5 will be stopped.

There is only one MST1 in MST1/MST2/MST3 region, sw3/sw4/sw5 is thought to be root, the topology picture is as follows:



Chapter 6 DHCP Overview

6.1 DHCP client configuration

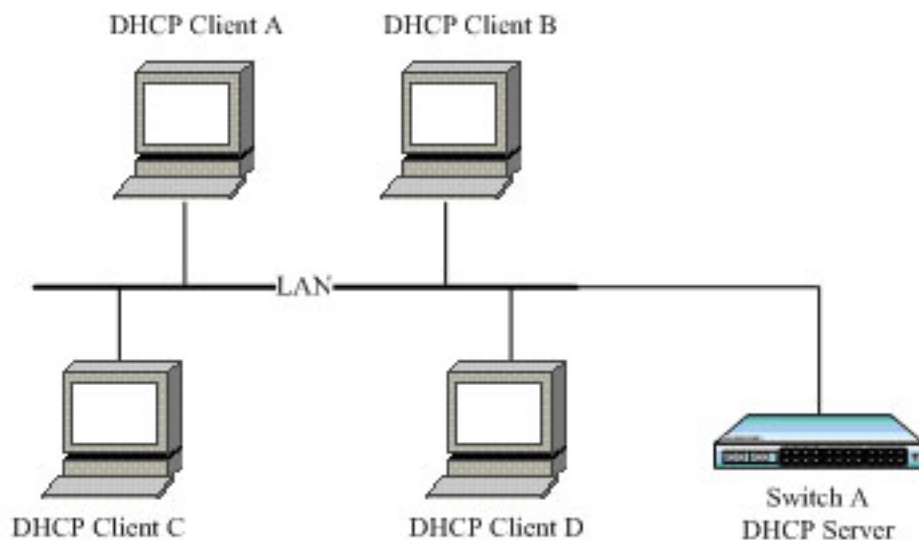
6.1.1 DHCP client overview

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 not 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:

- Large network scale, it is much too verbose for manual configuration, and cluster management is difficult.
- In the network the host number is larger than supported IP address number, the system cannot 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.
- 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.



Typical DHCP Client application

6.1.2 Configure DHCP Client

The part is about how to configure DHCP Client on the switch.

Note: 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.

Default DHCP Client configuration

Function	Default value
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

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 cannot 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
- After switches enabled, if the local has no configuration files, then switches will start DHCP client and apply IP address in VLAN1

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), root path (option 17), NTP server (option 42).

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)

Note:

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

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)

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

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

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

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 <i>myhost</i>	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

Note: 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.

6.1.3 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

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

```

Hostname:                raisecomFTTH
Class-ID:                raisecomFTTH-ROS_4.9.771
Client-ID:               raisecomFTTH-000e5e034be5-IF0

Assigned IP Addr:        20.0.0.1
Subnet mask:              255.0.0.0
Default Gateway:         --
Client lease Starts:      Jan-01-2000 12:47:19
Client lease Ends:        Jan-01-2000 13:17:19
Client lease duration:    1800(sec)
DHCP Server:              20.0.0.10

Tftp server name:         --
Tftp server IP Addr:      20.0.0.110
Startup_config filename:  /raisecom/config/0906081
NTP server IP Addr:       20.0.0.110
Root path:                /raisecom/image/2109A#0906053#0906054;2924GF##0906122

```

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

```

Hostname:                raisecomFTTH
Class-ID:                raisecomFTTH-ROS_4.9.771
Client-ID:               raisecomFTTH-000e5e034be5-IF0
DHCP Client is requesting for a lease.

```

Feedback 3: Disable DHCP Client on IP interface 0 :

```

Hostname:                Raisecom
Class-ID:                Raisecom-3.5.856
Client-ID:               Raisecom-000e5e48e596-IF0
DHCP Client is disabled.

```

Feedback 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.

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

6.1.4 Typical configuration example

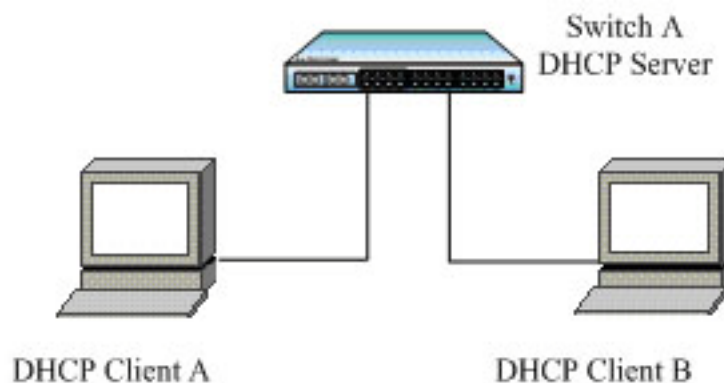
The example is simple but classical on the process of configuring DHCP Client.

1. Configuration instruction:

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

- Configure direct ip pool on DHCP Server, and enable DHCP Server globally.
- Configure the two DHCP client acquiring IP address and other configuration information by DHCP.

2. Topology



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-ROS_4.9.771*
 Client-ID: *raisecomFTTH-000e5e034be5-IF0*

 Assigned IP Addr: *20.0.0.1*

```

Subnet mask:          255.0.0.0
Default Gateway:      --
Client lease Starts:   Jan-01-2000 12:47:19
Client lease Ends:     Jan-01-2000 13:17:19
Client lease duration: 1800(sec)
DHCP Server:          20.0.0.10

Tftp server name:      --
Tftp server IP Addr:   20.0.0.110
Startup_config filename: /raisecom/config/0906081
NTP server IP Addr:    20.0.0.110
Root path:             /raisecom/image/2109A#0906053#0906054;2924GF##0906122

```

6.1.5 DHCP Client trouble shooting

- Make sure that DHCP server is able to support option 1, option 3, option 66, option 67, option 150, option 17, option 42. If some option is not supported, DHCP cannot get information of this kind, but for still can get IP address.
- 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 cannot get IP address.

6.2 DHCP Snooping configuration

6.2.1 DHCP Snooping principle

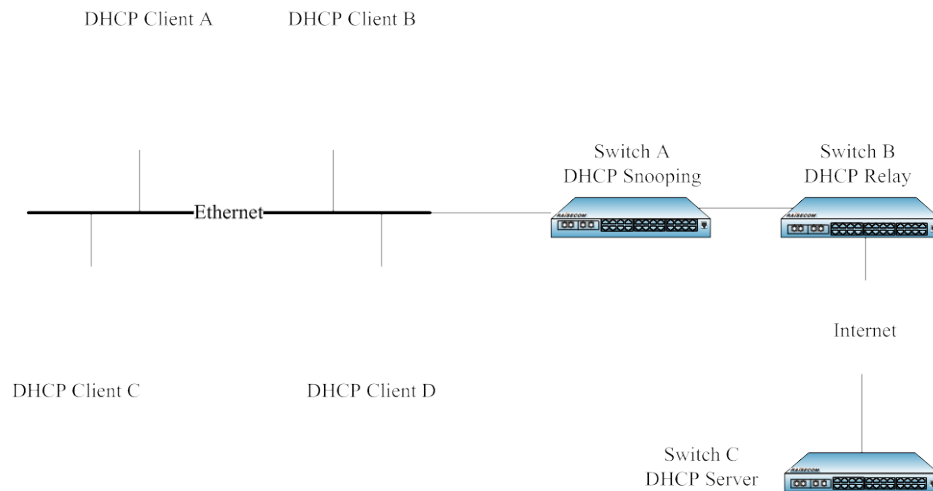
Basic Introduction:

If there is private DHCP server in the network, user may get wrong IP address. DHCP Snooping is a safe feature of DHCP, it provides network safety by filtrating the unbelievable DHCP message and establishing and maintaining a DHCP Snooping binding database (or DHCP Snooping binding table). To let user get IP address from valid DHCP server, DHCP Snooping safety mechanism allows the port to be set to creditable port and untrust port. It divides creditable port from untrust port on the switch, filtrates the untrust DHCP response message to insure the network safety. It is like firewall between untrust host and DHCP server.

Untrust DHCP message is the message that the host received from the network or outside the firewall. When DHCP Snooping is used in the network that provides network services, untrust message is from other network which does not belong to the server network, like user switch. The messages that are from unknown equipments may be attacking source, so it is untrust.

In the network that provides services, the creditable port is connected with DHCP server; the untrust port is connected with client side, or with other equipments in the network. The untrust port will drop the DHCP-ACK, DHCP-NAK and DHCP-OFFER message that is received from DHCP response (because these equipments that are connected with untrust ports should not make any response to DHCP server); while the response message received b the creditable port will be transmitted normally, which will prevent pseudo-server deception and make sure that user can get the correct IP address.

The figures below are typical network applications of DHCP Snooping:



DHCP Snooping typical network structure

Option 82 overview:

Option 82 is the Relay Agent Information option of DHCP message, which is identified in request document RFC3046. When DHCP Client sent request message to DHCP Server, if it is needed to cross DHCP Snooping, DHCP Snooping will add Option 82 to request message. Option 82 contains much sub-option. The option 82 introduced here support sub-option 1 and sub-option 2:

sub-option 1: circuit ID is defined in it

sub-option 2: remote ID is defined in it

sub-option 1: sub-option 1 is a sub-option of Option 82, which is circuit ID sub-option. A sub-option is usually configured on DHCP Snooping equipment or repeaters, which defines the port number of the switch port that needs to carry DHCP client when transmitting messages and the port's VLAN number. Usually sub-option1 and sub-option 2 need to be used together to note the information of DHCP source port.

Sub-option 2: it is also a sub-option of Option 82, which is Remote ID. This sub-option is usually also configured on DHCP repeater, which defines the MAC address information of the equipments that carry Snooping or repeater equipment. Usually sub-option 1 needs to be used together to note DHCP source port information.

Option 82 actualize the address information of DHCP client and DHCP snooping equipment or repeater equipment's record on DHCP server, with the help of other software it could actualize DHCP distribution restriction and billing function. For example, combined with IP Source Guard, the reception of IP address + MAC address can be defended effectively.

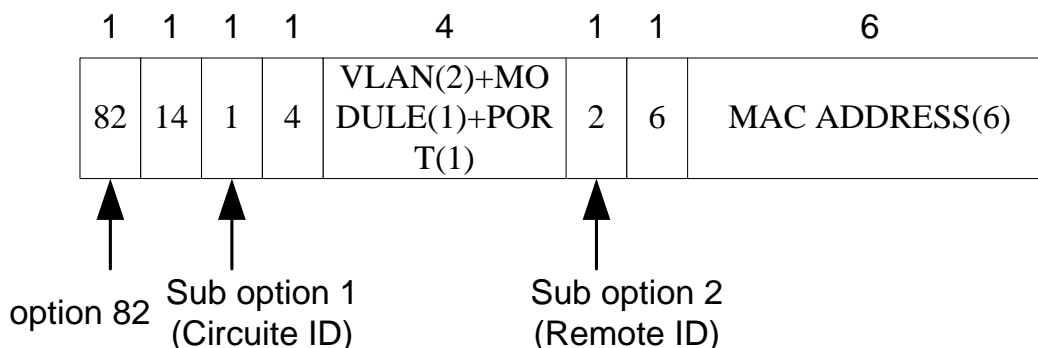
Option 82 handling actions:

- 1: When the switch receives a request message without Option 82 words, if it supports Option 82, Option 82 will be added and transmitted.
- 2: When the switch receives a request message without Option 82 words, if it supports Option 82, Option 82 will be transmitted; if not, the message will be dropped.

3: When the switch receives a request message without Option 82 words, if it supports Option 82, Option 82 will be deleted and transmitted; if not, the message will be dropped.

The structure of Option 82 message:

Option 82 obeys 'TLV' option format, fig 1-2 shows its message structure:



Option 82 message structure

Configure DHCP Snooping

✧ Default DHCP Snooping configuration

Function	Default value
Global DHCP Snooping state	Disabled
Port DHCP Snooping state	Enabled
Port trust state	Untrusted
DHCP Snooping supporting Option 82	Disabled

✧ DHCP Snooping configuration guide

- Make sure that the switch DHCP Server or DHCP Relay is not enabled;
- Global DHCP Snooping must be enabled;
- If DHCP Snooping is not enabled on the port, DHCP Snooping cannot be available on the switch;
- After DHCP Snooping is on, DHCP Server or DHCP Relay cannot be started on the switch;
- If only DHCP Snooping is enabled, while DHCP Snooping supporting Option 82 is not, the switch will not insert Option 82 in the message nor handle the message that contains Option 82;
- Make sure the port that connects DHCP server is trust, while the port that connects client side is untrust.

✧ Configure global DHCP Snooping

By default, global DHCP Snooping is off. Only when global DHCP Snooping is enabled can the switch DHCP Snooping take effect. To enable global DHCP Snooping, take the following steps:

The configuration step is shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp snooping	Enable global DHCP Snooping
3	exit	Return to privileged EXEC mode
4	show ip dhcp snooping	Show DHCP Snooping configuration

Notice: If the switch enables DHCP Server or DHCP Relay, global DHCP Snooping cannot be started. On the opposite, if the switch enables DHCP Snooping, DHCP Server or DHCP Relay cannot be started.

Use global configuration command **no ip dhcp snooping** to disable global DHCP Snooping.

✧ Configure port DHCP Snooping

By default, DHCP Snooping is on, use **no ip dhcp snooping port-list** to close port DHCP Snooping.

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp snooping port-list 4-9	Enable DHCP Snooping on port 4-9
3	exit	Return to privileged EXEC mode
4	show ip dhcp snooping	Show DHCP Snooping configuration

✧ Configure port trust

Untrust port will drop DHCP-ACK, DHCP-NAK, DHCP-OFFER message received from DHCP server response (because these equipments connected by untrust ports should not make any DHCP server response). While the DHCP server response message received by credible port will be transmitted normally.

Note: By default, all the ports' DHCP Snooping of the switch is on. But until global DHCP Snooping is on can they be available. That is to say, if global DHCP Snooping is off, and only port DHCP Snooping is on, DCHP Snooping cannot take effect.

Trust port connects DHCP server or the ports of others switches, while untrust port connects user or network, which keeps away from server deception, and makes sure user can get the correct IP address.

Follow the steps below to set the designated port to credit port.

Step	Command	description
1	config	Enter global configuration mode
2	interface port 15	Enter port configuration mode

3	ip dhcp snooping trust	Configure credit port
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp snooping	Show DHCP Snooping configuration

Notice:

- Only when port trust is started in global DHCP Snooping and the port has also started DHCP Snooping can it take effect. Use **no ip dhcp snooping trust** to set the port to untrust port.
- In port configuration mode use **no ip dhcp snooping trust** to set the port to untrust port and delete it from trust port list.

✧ Configure DHCP Snooping supporting Option 82

Following the steps below, user can enable DHCP Snooping supporting Option 82, and the switch will add Option 82 option into the DHCP request message that receives Option 82; delete Option 82 in the DHCP response message that contains Option 82. The received DHCP request message that contains Option 82 will be handled according to the configured strategy and transmitted, while to the response message that don't contain Option 82 option, the switch will not take any action and transmit it directly.

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp snooping information option	Enable DHCP Snooping supporting Option 82
3	exit	Return to privileged EXEC mode
4	show ip dhcp snooping	Show DHCP Snooping configuration

Notice:

- DHCP Snooping supporting Option 82 function is global, but it reacts on the port. It can be enable only in global DHCP Snooping, and only when the port start DHCP Snooping can Option 82 take effect on the port.
- Use global configuration command **no ip dhcp snooping information option** to stop DHCP Snooping supporting Option 82.

6.2.2 Monitoring and maintaining

Use the command **show** to look over the switch DHCP Snooping running state and configuration state and help monitoring and maintaining.

Command	Description
show ip dhcp snooping	Show DHCP Snooping configuration

Use **show ip dhcp snooping** to show DHCP Snooping configuration information, including global DHCP Snooping state, if Option 82 is supported, port DHCP Snooping state and port trust. Specific

steps are as follows:

Raisecom#show ip dhcp snooping

DHCP Snooping: Enabled

Option 82: Enabled

<i>Port</i>	<i>Enabled Status</i>	<i>Trusted</i>

<i>1</i>	<i>enabled</i>	<i>no</i>
<i>2</i>	<i>enabled</i>	<i>no</i>
<i>3</i>	<i>enabled</i>	<i>no</i>
<i>4</i>	<i>enabled</i>	<i>no</i>
<i>5</i>	<i>enabled</i>	<i>no</i>
<i>6</i>	<i>enabled</i>	<i>no</i>
<i>7</i>	<i>enabled</i>	<i>no</i>
<i>8</i>	<i>enabled</i>	<i>no</i>
<i>9</i>	<i>enabled</i>	<i>no</i>
<i>10</i>	<i>enabled</i>	<i>no</i>
<i>11</i>	<i>enabled</i>	<i>no</i>
<i>12</i>	<i>enabled</i>	<i>no</i>
<i>13</i>	<i>enabled</i>	<i>no</i>
<i>14</i>	<i>enabled</i>	<i>no</i>
<i>15</i>	<i>enabled</i>	<i>yes</i>
<i>16</i>	<i>enabled</i>	<i>no</i>
<i>17</i>	<i>enabled</i>	<i>no</i>
<i>18</i>	<i>enabled</i>	<i>no</i>
<i>19</i>	<i>enabled</i>	<i>no</i>
<i>20</i>	<i>enabled</i>	<i>no</i>
<i>21</i>	<i>enabled</i>	<i>no</i>
<i>22</i>	<i>enabled</i>	<i>no</i>
<i>23</i>	<i>enabled</i>	<i>no</i>
<i>24</i>	<i>enabled</i>	<i>no</i>
<i>25</i>	<i>enabled</i>	<i>no</i>
<i>26</i>	<i>enabled</i>	<i>no</i>

Raisecom#show ip dhcp snooping binding

<i>Ip Address</i>	<i>Mac Address</i>	<i>Lease(sec)</i>	<i>Type</i>	<i>VLAN</i>	<i>Port</i>

<i>20.168.0.3</i>	<i>000E.5E00.91E0</i>	<i>1650</i>	<i>dhcp-snooping</i>	<i>1</i>	<i>17</i>

Current Binding: 1

History Max Binding: 1

6.2.3 Typical topology

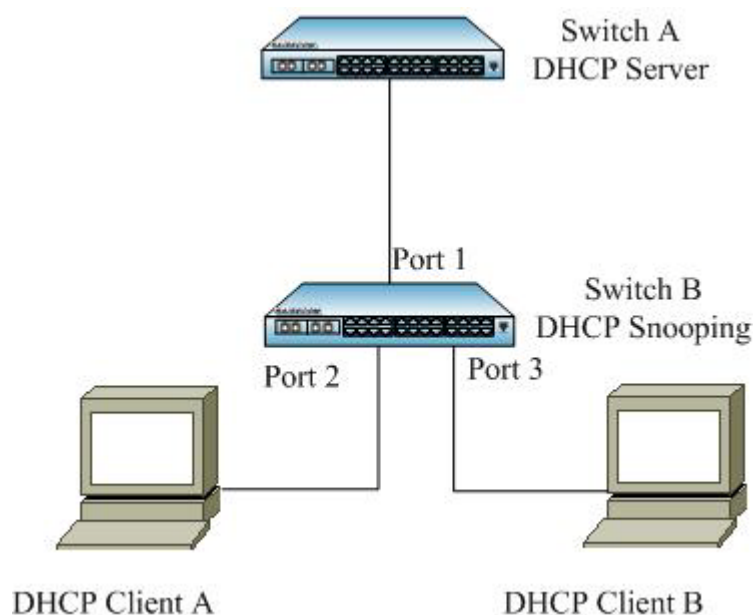
This part gives an introduction to an example that a DHCP client connects to a DHCP server and gets an IP address dynamically through DHCP Snooping. It shows straight-through configuration of DHCP Snooping.

1. Configuration explanation:

This example is a simple and typical DHCP configuration. The two DHCP clients use DHCP ports 2, 3 respectively to connect to the DHCP server.

- Configure the correct address pool on the DHCP Server, and enable the DHCP Server function globally.
- Enable DHCP Snooping function globally on the DHCP Snooping equipment, and enable DHCP Snooping on the port, set port 1 to trust port, and configure DHCP Snooping supporting Option 82, use the default strategy Replace to handle the request messages from the client side.

2. Topology picture



Typical DHCP Snooping configuration topology

3. Configuration step

Configure DHCP Snooping:

- Enable global DHCP Snooping:


```
Raisecom#config
Raisecom(config)#ip dhcp snooping
```
- Port enable DHCP Snooping:


```
Raisecom(config)# ip dhcp snooping port-list 1-3
```
- Set port 3 to DHCP Snooping trust port:


```
Raisecom(config)# interface port 1
Raisecom(config_port)# ip dhcp snooping trust
```
- Enable DHCP Snooping supporting Option 82:

Raisecom(config)#ip dhcp snooping information option

4. Show the result

On ISCOM switch use command **show ip dhcp snooping** to look over the switch DHCP Snooping running state and configuration state, on the client side use **show ip dhcp client** to show client IP address application. Specific contents are as follows:

Raisecom#show ip dhcp snooping

DHCP Snooping: Enabled

Option 82: Enabled

	<i>Port</i>	<i>Enabled Status</i>	<i>Trusted</i>

<i>1</i>	<i>enabled</i>	<i>yes</i>	
<i>2</i>	<i>enabled</i>	<i>no</i>	
<i>3</i>	<i>enabled</i>	<i>no</i>	
<i>...</i>	<i>...</i>		<i>...</i>

Raisecom#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
  
```

6.2.4 DHCP snooping trouble shooting

If DHCP client cannot get network address normally through DHCP Snooping, it may be one of the following situations:

- If global DHCP Snooping and port DHCP Snooping are enabled at the same time;
- If DHCP Snooping do not open Option 82 option, when DHCP Snooping receives the message that contains Option 82 it will be dropped directly;
- If DHCP Snooping Option 82 option is enabled, and the request message handling strategy is set to be DROP, then the messages that contain Option 82 will be dropped;
- If the port is not configured as DHCP Snooping trust port, all the response messages to the ports mentioned above will be dropped.

If above configuration cannot make it running, check if Route enabled on device opened DHCP Snooping and DHCP server IP is correct.

6.3 DHCP Server Configuration

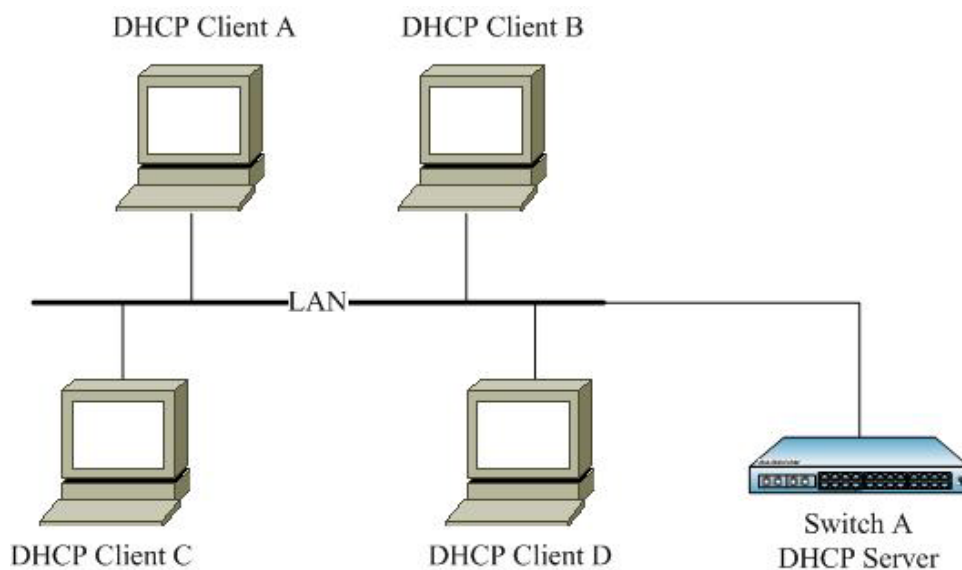
6.3.1 DHCP Server principle overview

Dynamic Host Configuration Protocol (DHCP) let the client acquire configuration information protocol in TCP/IP network, which is based on BOOTP protocol, and adds the function of automatic distribution useful network address and so on based on BOOTP protocol. The two protocol can make interoperability through some mechanism. DHCP offers the network hosts configuration parameters, which are made of two parts: one is to transmit special configuration information to network hosts, the other one is to assign network addresses to the hosts. DHCP is based on client/server mode, in this mode specific host assigns network addresses and transmits network configuration parameters to network hosts, the designated hosts are called server.

Usually, in the following situations DHCP server will be used to accomplish IP address distribution:

- (1) When the network scope is too large for manual configuration or centralized management to the whole network.
- (2) When the network host number is larger than the IP address number that the network supports, and cannot give each host a stable IP address; there is also user number limit who can get into the network at the same time (for example, Internet access service provider belongs to the situation), lots of users have to acquire their own IP address dynamically from DHCP server.
- (3) When there is not so many hosts who need stable IP address, and most hosts have no the need for stable IP address.

In typical DHCP application, there is usually one DHCP server and several client (like PC and portable machine), the typical DHCP application is shown below:



DHCP typical usage

6.3.2 Configure DHCP Server

Only ISCOM3000 serial switches support border upon surrogate IP address configuration.

Default DHCP Server configuration

Function	Default value
Global DHCP Server state	Disabled
IP port DHCP Server state	Disabled
Address pool	N/A
Lease table timeout	Maximum timeout: 1080 minutes Least timeout: 30 minutes Default timeout: 30 minutes
Neighbour proxy address	N/A

DHCP Server configuration guide

- Make sure that DHCP Snooping on the switch is not on; Global DHCP Server must be enabled;
- If DHCP Server is not enable in IP port, DHCP Server does not take effect on this IP port;
- When DHCP Server is on, DHCP Snooping cannot be started either on the switch;
- Make sure that the connection to DHCP Relay and DHCP server is correct. DHCP server must be ISCOM3000 serious products. The IP port address and the corresponding address pool range is correct;
- If the client connect DHCP server through DHCP Relay, DHCP server must be ISCOM3000 serial switches. Except making sure IP port address and address pool configuration correct, correct configuration to neighbor proxy address and DHCP Relay.

Configure global DHCP Server

By default, global DHCP Server is disabled. Only when global DHCP Server is enabled, the switch DHCP Server can take effect. User can follow the steps below to start global DHCP Server:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp server	Enable global DHCP Server
3	exit	Return to privileged EXEC mode
4	show ip dhcp server	Show DHCP Server configuration

Notice:

- If DHCP Snooping has been started on a switch, global DHCP Server can not be started any more.
- On the opposite, if global DHCP Server has been started, DHCP Snooping or DHCP Client cannot be started.

Use global configuration command **no ip dhcp server** to close global DHCP Server.

IP port DHCP Server

By default, IP port DHCP Server function is disabled as well, user can use IP port command **ip dhcp server** to start IP port DHCP Server function. To close IP port DHCP Server, use IP port command **no ip dhcp server**.

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 4	Enter IP port 4 configuration mode
3	ip dhcp server	Enable DHCP Server
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp server	Show DHCP Server configuration

Notice: When global DHCP Server is off, user can start DHCP Server beforehand on a certain IP interface, but only when global DHCP Server starts, can the DHCP Server started from the IP port take effect.

ip-pool

DHCP server selects and distributes IP address and other parameters from the address pool for the client. When the equipment that is selected as DHCP server receives a DHCP request from the client, it will select proper address pool by configuration, and then pick out a free IP address, which will sent out to the client together with other parameters (like DNS server address, address lease limit). Lots of standard configuration option is identified in RFC2132, where more detailed information can be got there. But most DHCP configurations use only a few options of the rules.

Following the steps below user can configure address pool:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp sever ip-pool WORD start-ip-address end-ip-address mask-address ip <0-14> [gateway ip-address] [dns ip-address] [secondary-dns ip-address]	Configure the address pool
3	exit	Return to privileged EXEC mode
4	show ip dhcp server ip-pool	Show DHCP Server address pool configuration

Notice:

- The command can configure one address pool to IP interface once. If IP interface does not exist

when configuring, still the address pool can be successfully configured, but it will not take effect until the IP port is created and the IP address is configured. If the IP port is changed or deleted, the configured address pool can still be kept. Once the IP port is re-created, the configured address pool will take effect again.

- If the client and the server is in the same subnet, when configuring IP address pool, the network section that the address pool is in should be the same with the network section that of IP port address's, that is to say, address pool's network address is the same with the port's network address; if the client connects the server through DHCP Relay, then the server's address and relay-ip should be within the same network section. Otherwise, DHCP Server will not distribute IP address for DHCP client.

Use global configuration command **no ip dhcp server ip-pool** ip-pool to delete the configured address pool. If the IP address pool that is to be deleted does not exist, returned value is fault.

Here, the maximum IP address pool number that can be configured for each IP port is 4, the maximum IP address number that the switch supports is 2500. Address pool take the name as the only mark.

Configuration example:

Raisecom#**config**

Raisecom(config)#**ip dhcp server ip-pool** pool1 192.168.1.100 192.168.1.200

255.255.255.0 **ip 4 gateway** 192.168.1.1 **dns** 192.168.1.1 **secondary-dns** 10.168.0.1

Raisecom(config)#**exit**

Raisecom#**show ip dhcp server ip-pool**

The result is shown below

```

-----
Name of ip pool table : pool1
Status of IP pool table: active
IP address range: 192.168.1.100 - 192.168.1.200
Mask: 255.255.255.0
Including IP Interface: 4
IP address of gateway: 192.168.1.1
IP address of DNS server: 192.168.1.1
IP address of secondary DNS server: 10.168.0.1
-----
Valid IP pool count : 1
Valid IP address count : 12
Allotted IP address count : 0

```

Gateway and dns is optical, if they are not used, default gateway and DNS will not be selected for the client.

lease table timeout

When distributing IP address for the client, it is needed to designate the lease time of the IP address. By default the system lease time is:

- Default lease time: 30 minutes (usually it will not be used);
- The maximum lease time: 10080 minutes (7days), when the lease time that the client requests is larger than this value, the larger value will be used.
- The least lease time: 30 minutes, when the lease time that the client requests is smaller than this value, least lease time will be used; otherwise, according to the request time, if the client does not designate lease time, use the least lease time for distribution.

If the administrator needs to modify the least lease time, manual configuration is needed.

The configuration step is as follows:

Step	Command	Description
1	config	Enter global configuration mode
2 (optional)	ip dhcp sever default-lease <i>timeout</i>	Configure the IP address pool default lease time for DHCP server
3 (optional)	ip dhcp sever max-lease <i>timeout</i>	Configure the IP address pool maximum lease time for DHCP serve
4 (optional)	ip dhcp sever min-lease <i>timeout</i>	Configure the IP address pool least lease time for DHCP serve
5	exit	Return to privileged EXEC mode
6	show ip dhcp server	Show DHCP server configuration

Notice: The lease time configured here is used for all the IP address of the address pool. At the same time, the maximum lease time cannot be shorter than least rent time, default lease time must be between maximum and least lease time.

Use global command **no ip dhcp server default**, **no dhcp-server max-lease**, **no dhcp-server min-lease** to cannel the current setting, and restore system default lease time setting.

Configuration example:

```
Raisecom#config
Raisecom(config)#ip dhcp server default-lease 60
Raisecom(config)#ip dhcp server max-lease 1440
Raisecom(config)#ip dhcp server min-lease 45
Raisecom(config)#exit
Raisecom#show ip dhcp server
```

The result is shown below:

```
DHCP Server: Enabled
IP Interface Enabled: 4
Total Number: 1
```


Max lease time: 1440 m

Min lease time: 40 m

Default lease time: 60 m

relay-ip

When the client is connected with the server by DHCP Relay, DHCP server must know the neighbor DHCP Relay IP address, which needs the administrator's manual configuration as well.

The configuration step is shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp sever relay-ip <i>ip-address</i> <i>ip-mask</i>	Configure neighbor proxy IP address
3	exit	Return to privileged EXEC mode
4	show ip dhcp server relay-ip	Show DHCP server configuration

Notice: Only ISCOM3000 serious switches support the command **ip dhcp server relay-op**. Here the configured neighbor proxy IP address is actually the port address that is connected with the client, as is shown in the typical example. The maximum number of neighbor proxy IP address is 8.

Use global configuration command **no ip dhcp server relay-ip** *ip-address* to delete neighbor proxy IP address configuration.

Configuration example:

Raisecom#**config**

Raisecom(config)#**ip dhcp server relay-ip** *192.168.1.1 255.255.255.0*

Raisecom(config)#**exit**

Raisecom#**show ip dhcp server relay-ip**

The result is shown below:

<i>index</i>	<i>IP address</i>	<i>IP Mask</i>	<i>Status</i>

<i>1</i>	<i>192.168.1.1</i>	<i>255.0.0.0</i>	<i>active</i>

6.3.3 Monitoring and maintaining

Use different **show** commands to show the switch DHCP Server running and configuration situation for monitoring and maintaining. All the show commands are listed below:

Command	Description
---------	-------------

show ip dhcp server	Show DHCP Server configuration and static information
show ip dhcp server ip-pool	Show DHCP Server address pool information
show ip dhcp server relay-ip	Show the configured neighbor DHCP proxy address information
show ip dhcp server lease	Show the designated IP address and the corresponding information

Notice:

- Only ISCOM3000 serial switches supports the command **show ip dhcp server relay-ip**
- Before using **show ip dhcp server lease**, the system time should better be configured accurately, because lease time limit is computed according to the system date absolute time.

Use **show ip dhcp server** command to look over the configuration information, like global or IP port configuration information, static information or so.

Raisecom#show ip dhcp server

DHCP Server: Enabled

IP Interface Enabled: 4

Total Number: 1

Max lease time: 1000 m

Min lease time: 32 m

Default lease time: 300 m

Statistics information:

Running time: 0 hours 7 minutes 33 seconds

Boots: 0

Discover: 0

Request: 0

Release: 0

Offer: 0

Ack: 0

Nack: 0

Decline: 0

Information: 0

Unknowns: 0

Total: 0

Use the command **show ip dhcp server ip-pool** to show the configured address pool information:

Raisecom#show ip dhcp server ip-pool

Name of IP pool table: dhcp

Status of IP pool table: active

IP address range: 11.1.1.33 - 11.1.1.44

Mask: 255.255.255.0

Including IP Interface: 4

IP address of gateway: 0.0.0.0

IP address of DNS server: 0.0.0.0
IP address of secondary DNS server: 0.0.0.0

Valid IP pool count: 1
Valid IP address count: 12
Allotted IP address count: 0

Use the command **show ip dhcp server relay-ip** to show the configured neighbour proxy address information:

Raisecom#**show ip dhcp server relay-ip**

In English:

<i>Index</i>	<i>IP Address</i>	<i>IP Mask</i>	<i>Status</i>

1	11.1.1.34	255.255.255.0	active

Use the command **show ip dhcp server lease** to show the configured neighbour proxy address information.

Raisecom#**show ip dhcp server lease**

<i>IP Address</i>	<i>Hardware Address</i>	<i>Lease Expiration</i>	<i>IP Interface</i>

172.16.1.11	00:a0:98:02:32:de	Feb-01-2006 11:40:00	1
172.16.3.254	02:c7:f8:00:04:22	Jul-01-2006 23:00:00	1

Character instruction:

- IP Address: the client IP address;
- Hardware Address: the client MAC address
- Lease Expiration: lease timeout limit
- IP Interface: IP interface number

Lease timeout limit is computed according to system date, format is mm-dd-yy hh:mm:ss

6.3.4 Typical configuration example

The typical DHCP Relay and Server configuration case is as below:

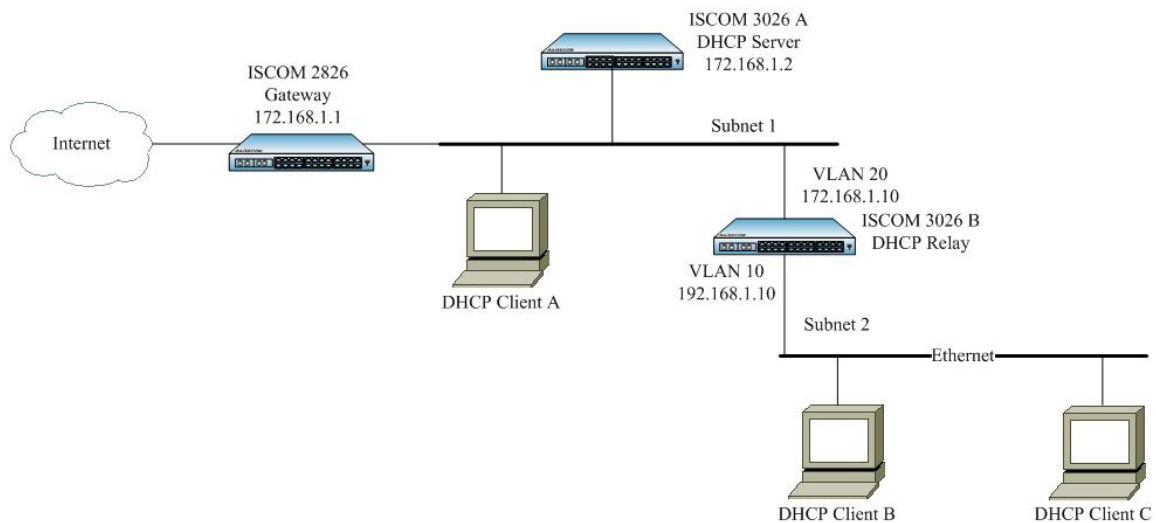
- Direct connection to the client for IP address
- The client get IP address through proxy

1) Configuration instruction

The example is simple and typical in realizing DHCP protocol. Specific connection state is shown as below. In the figure ISCOM3026, as DHCP Relay, divides the two VLAN: VLAN 10 and VLAN 20, the two corresponding subnet IP address are 192.168.1.10 and 172.168.1.10 respectively. The DHCP server is ISCOM3026A, IP address is 172.168.1.2, suppose the subnet NDS be 172.168.1.3, subnet 1 and subnet 2 needs to get connection to public network through gateway 172.168.1.1. To realize the

client accessing the resource of the public network, it is only needed to configure DHCP Server and DHCP Relay correctly.

2) Topology figure



Typical configuration example

3) Configuration steps

Configure DHCP Server:

➤ Configure VLAN and interfaces:

```
Raisecom(config)#create vlan 20 active
```

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

```
Raisecom(config-port)#switchport access vlan 20
```

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

```
Raisecom(config)#interface ip 2
```

```
Raisecom (config-ip)#ip address 172.168.1.2 255.255.0.0 20
```

➤ Configure address pool

Configuring a address pool for both subnet 1 and subnet 2 respectively.

```
Raisecom (config)#ip dhcp server ip-pool pool1 172.168.1.100 172.168.1.200 255.255.0.0 ip 2
gateway 172.168.1.1 dns 172.168.1.3
```

```
Raisecom(config)#ip dhcp server ip-pool pool2 192.168.1.100 192.168.1.200 255.255.255.0 ip 2
gateway 172.168.1.1 dns 172.168.1.3
```

```
Raisecom (config)#exit
```

```
Raisecom #show ip dhcp server ip-pool
```

➤ Start DHCP Server service

```
Raisecom (config)#ip dhcp server
```

```
Raisecom(config)#interface ip 2
```

Raisecom(config-ip)#**ip dhcp server**

Raisecom #**show ip dhcp server**

➤ **Configure neighbour proxy IP address**

Raisecom (config)#**ip dhcp server relay-ip** 192.168.1.10 255.255.255.0

Raisecom (config)#**exit**

Raisecom #**show ip dhcp server relay-ip**

➤ **Configure the router**

Raisecom (config)#**ip route** 192.168.1.0 255.255.255.0 172.168.1.10

➤ **Configure DHCP Relay**

Create VLAN and the interface

Raisecom (config)#**create vlan** 10 **active**

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

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

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

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

Raisecom(config-ip)#**ip address** 192.168.1.10 255.255.255.0 10

Raisecom (config)#**create vlan** 20 *active*

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

Raisecom(config-port)#**switchport access vlan** 20

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

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

Raisecom (config-ip)#**ip address** 172.168.1.10 255.255.0.0 20

➤ **Enable router function**

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

Raisecom(config)#**ip routing**

➤ **Configure DHCP server IP address**

Raisecom(config)#**ip dhcp relay ip-list** 2 **target-ip** 172.168.1.2

Raisecom (config)#**exit**

Raisecom #**show ip dhcp relay**

➤ **Start DHCP Relay**

Raisecom (config)#**ip dhcp relay**

Raisecom(config)#**exit**

Raisecom #**show ip dhcp relay**

The client will be configured as auto acquiring IP address through DHCP

4) Show the result

- Show DHCP configuration static information, address pool information and the configured IP address information.

On ISCOM3026A use the command **show ip dhcp server**、**show ip dhcp server ip-pool** and **show ip dhcp server lease**.

- Show DHCP Relay information

On switch device(OLT) use the command **show ip dhcp relay**.

➤ **Show client A**

c:\>ipconfig /all

Ethernet adapter: local connection:

Connection-specific DNS Suffix . :

Description : Realtek RTL8139/810x Family Fast Ethernet NIC

Physical Address. : 00-50-8D-4B-FD-27

DHCP Enabled. : Yes

Autoconfiguration Enable. . . :Yes

IP Address. : 172.168.1.100

Subnet Mask : 255.255.0.0

Default Gateway : 172.168.1.1

DHCP server. : 172.168.1.2

DNS Servers : 172.168.1.3

Lease Obtained. : 13:03:24

Lease Expires. : 13:33:24

➤ **Show client B**

c:\>ipconfig /all

Ethernet adapter: local connection:

Connection-specific DNS Suffix . :

Description : Realtek RTL8139/810x Family Fast Ethernet NIC

Physical Address. : 00-50-8D-4B-DE-46

DHCP Enabled. : Yes

Autoconfiguration Enable. . . :Yes

```

IP Address. .... : 192.168.1.100
Subnet Mask ..... : 255.255.255.0
Default Gateway ..... : 172.168.1.1
DHCP server. .... : 172.168.1.2
DNS Servers ..... : 172.168.1.3
Lease Obtained. .... : 13:03:24
Lease Expires. .... : 13:33:24

```

- Show client C:

Client C is the same with client B in content, the IP address is 192.168.1.101

6.3.5 DHCP Server trouble-shooting

- As per ISCOM3000 series switches, don't specify the IP address of the relay agent, the equipment can't accurately realize DHCP relay functions; ISCOM2800/2900 switches don't support the DHCP agent
- When setting neighbor agent, error is likely caused by: address is beyond the maximum limit(8); IP address is not correct;
- When setting IP-pool, error is likely caused by: ip-pool is above the maximum limit(4); IP address or other parameter is not correct;
- If delete ip-pool failed, the reason is probably that the input parameters are not correct; ip-pool does not exist.

If after above setting, the system still cannot work normally, check whether a DHCP server has the default gateway or routing, and check whether DHCP Relay opened the routing functions.

6.4 DHCP Relay Configuration

6.4.1 DHCP Relay principle overview

Early DHCP protocol is suitable for only the situation that the client and server are in the same subnet, which cannot go through network sections. Therefore, for dynamical host configuration, configuring a DHCP server on all the network sections is needed, which is obviously wasteful.

The introduction of DHCP Relay solves this problem: the local network client can communicate with the other subnet DHCP servers by DHCP Relay, and get the legal IP address finally. Thus, the DHCP client on several networks can use the same DHCP server, which decreases the cost and helps centralized management

DHCP Relay provides DHCP broadcast message transparent transmission function, which is able to transmit the broadcast message of DHCP client (or server) transparently to the other network section DHCP server (or client).

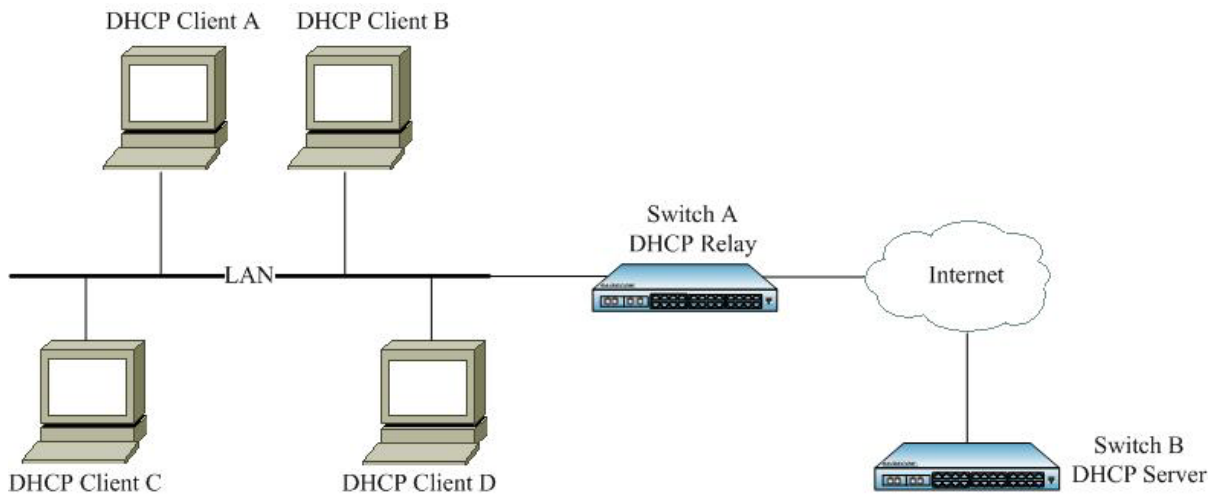
In the process that DHCP Relay completes dynamic configuration, the processing way that DHCP client and server takes is basically the same with that of not through DHCP Relay. The following steps are only about DHCP Relay transmission:

- (1) DHCP client transmits DHCP-DISCOVER message in broadcasting.
- (2) When the network equipment with DHCP Relay function receives the broadcast message, by configuration it will transmit the message to the specific DHCP server in unicast.

(3) DHCP server makes IP addresses distribution, and sends the configuration information to the client through DHCP Relay.

Usually, DHCP Relay can be host, two-layer switch, three-layer switch or router, if only DHCP Relay service program is enable.

The figure below is a typical DHCP Relay application:



DHCP Relay typical application

The mechanism of DHCP Relay support Option 82 is shown below:

- (1) DHCP client sends out request message in the form of broadcasting when initialized.
- (2) The DHCP Relay equipment that is connected with local network will receive the broadcast message, check out if there has been Option 82 in the message, and handles it in the corresponding way.
- (3) If there has been Option 82 in the message, the equipment will follow the configured strategy to handle the message (drop, replace the Option 82 in the message that has been there with the relay equipment's Option 82 or keep the Option 82 that has been there), and transmits the request message to DHCP server.
- (4) If there is no Option 82 in the request message, the Option 82 of DHCP equipment will be added into the message (located in the end of all the options) and be transmitted to DHCP server. At this time, the Option 82 of the request message contains the port number of the switch which is connected with DHCP client, the number of the VLAN that the port belongs to and the DHCP Relay equipment's own MAC address and so on.
- (5) When DHCP server receives the DHCP request message that is transmitted by DHCP Relay equipment, it will record the information from Option in the message, then transmit the message that contains DHCP configuration information and Option 82 information.
- (6) After DHCP Relay receives the response message of DHCP server it will peel off the message's Option 82 information, then transmit the message that contains DHCP configuration information to DHCP client.

Note: there are two sorts of request messages from DHCP client, DHCP-DISCOVER and DHCP-REQUEST message. Because of the different mechanisms that different manufacturers' DHCP server handle request messages, some equipments handle DHCP-DISCOVER message's Option 82 information, while some others handle DHCP-REQUEST message's Option 82

information, so DHCP Relay handles both the two messages in the strategy of Option 82.

Otherwise, if DHCP Relay receives the messages sent out from the two DHCP client DHCP-DECLINE and DHCP-INFORM, it will handle Option 82 uniformly according to the strategy, without affecting its basic function of supporting Option 82.

6.4.2 Configure DHCP Relay

Default DHCP Relay configuration

The following table is the default configuration steps of DHCP Relay:

Function	Default value
Global DHCP Relay state	Disabled
IP port DHCP Relay state	Enabled
IP port's destination IP address	N/A
DHCP Relay support Option 82	Disabled
The strategy of DHCP Relay handling option 82 request messages	Replace
Port DHCP Relay trust	Untrusted

DHCP Relay configuration guide

- Make sure the DHCP Snooping on the switch is not started; Global DHCP Relay must be started;
- If on a IP port DHCP Relay is not started, it cannot work on this IP port;
- When DHCP Relay is on, DHCP Snooping cannot be started either on the switch;
- Make sure the DHCP server that is connected with DHCP Relay has correct configuration and connection to the client. DHCP server must be ISCOM 3000 serious switches. Except making sure the correct configuration of IP port addresses and address pool, correct configuration to the neighbor proxy address and Relay addresses;
- If the client acquires IP address automatically from DHCP server through multiplex Relay, you must make sure the connection of each equipment and correct configuration. The DHCP Relay number between the client and server, cannot exceed 16 in RFC1542 rules, it is usually suggested not to exceed 8.

Configure global DHCP Relay

By default, global DHCP Relay is off. Only when global DHCP Relay is on can the switch DHCP Relay takes effect. User can take the following steps to start global DHCP Relay.

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp relay	Start global DHCP Relay

3	exit	Return to privileged EXEC mode
4	show ip dhcp relay	Show DHCP Relay configuration

Notice: If the switch starts DHCP Snooping, it cannot start global DHCP Relay. On the opposite, if the switch starts global DHCP Relay, it cannot start DHCP Snooping.

Use global command **no ip dhcp relay** to disable global DHCP Relay.

Configure IP port DHCP Relay

By default, IP port DHCP Relay function is on, user can use IP port command **no ip dhcp relay** to disable IP port DHCP Relay function. To start IP port DHCP Relay, use IP port command **ip dhcp relay**.

Step	Command	Description
1	config	Enter global configuration mode
2	interface ip 4	Enter IP port 4 configuration mode
3	ip dhcp relay	Start DHCP Relay
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp relay	Show DHCP Relay configuration

Notice: When global DHCP Relay is off, on a certain IP port DHCP Relay can be started in advance. But only when global DHCP Relay starts can the DHCP Relay started on this port takes effect.

Configure IP port destination IP address

When the client equipment and DHCP server is not in the same broadcasting domain, the relay equipment in the middle must be able to transmit the kind of broadcasting packet. Configuring the destination IP address of DHCP Relay points out the destination address of the DHCP broadcasting packet from DHCP client for the relay equipment.

When DHCP Relay is configuring destination IP address, use network port LIST for the convenience of user's configuration. That is to say, according to the actual need, one command can be used to configure the same IP address for parts of the network ports or all the ports.

When DHCP Relay is configuring destination IP address, except the configuration commands in config mode, you can also configure the port's corresponding destination IP address in IP port, which is flexible.

Take the following steps to configure the port's destination IP address.

Step	Command	Description
1	config	Enter global configuration mode

2	ip dhcp relay ip-list all target-ip 10.199.0.200	For all the IP ports configure the destination IP 10.199.0.200
3	ip dhcp relay ip-list 1-3 target-ip	For IP port 1-3 configure the destination IP 10.200.0.200
4	interface ip 3	Enter IP port 3 configuration mode
5	ip dhcp relay target-ip	Configure the destination IP 10.201.0.200
6	exit	Return to global configuration mode

Notice:

- Here, the configured maximum destination IP address number for each port is 4. At the same time, make sure that the destination IP address is correct.
- When it comes to configuring destination IP address for several IP ports in one command, if configuring the destination IP address in a certain port fails, the rest IP port destination IP address configuration should be continued and return the cue which specific port configuring destination IP address fails, the format is: IP interface %s set target IP address unsuccessfully. Use IP table to replace %s in actual use. If only one port is configured successfully, the command line will return 'configuration successful' finally.

Use global configuration command **no ip dhcp relay ip-list target-ip** to delete the configured destination IP address of the IP port, or IP interface configuration command **no ip dhcp relay target-ip** in the corresponding port configuration mode.

Configuration example:

Raisecom#**config**

Raisecom(config)# **ip dhcp relay ip-list all target-ip 10.199.0.200**

Raisecom(config)# **ip dhcp relay ip-list 1-3 target-ip 10.200.0.200**

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

Raisecom(config-ip)#**ip dhcp relay target-ip 10.201.0.200**

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

Raisecom(config)#**exit**

Raisecom#**show ip dhcp relay**

The result is shown below:

DHCP Relay: Enabled

<i>IP Interface</i>	<i>Enabled Status</i>	<i>Target IP Address</i>
0	enabled	10.199. 0.200
1	enabled	10.199. 0.200
10.200.0.200		
2	enabled	10.199. 0.200
10.200.0.200		
3	enabled	10.199. 0.200
10.200.0.200		

```

10.201.0.200
4          enabled          10.199.0.200
...        ...              ...
...        ...              ...

```

Configure DHCP Relay support option 82

By default, DHCP Relay do not support option 82, in global configuration mode use **ip dhcp relay information option** to start DHCP Relay support option 82.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp relay information	Start DHCP Relay support option 82
3	exit	Return to privileged EXEC mode
4	show ip dhcp relay information	Show DHCP Relay support Option 82 configuration information and port trust list

Notice: To active DHCP Relay support option 82, enable global DHCP Relay service first. To make option 82 function available, corresponding configuration on DHCP Server is needed.

Use global configuration command **no ip dhcp relay information option** to disable DHCP Relay support Option 82.

Configure DHCP Relay request message handling strategy

By default, DHCP Relay handling strategy to the client request messages is Replace, that is to fill Option 82 in the way of normal or verbose, replace the Option 82 contents that has been there and transmit it. In global configuration mode use the command **ip dhcp relay information policy {drop / keep / replace}** to configure the message handling strategy of DHCP Relay as drop, keep or replace.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp relay information policy {drop / keep / replace} [schedule-list list-no]	Configure DHCP Relay request message handling strategy
3	exit	Return to privileged EXEC mode
4	show ip dhcp relay information	Show DHCP Relay handling strategy to client request message

Notice: The command configured request message handling strategy can available only in DHCP Relay support Option 82.

Use global configuration command **no ip dhcp relay information policy {drop / keep / replace}**

[schedule-list list-no] to recover default DHCP Relay handling strategy to Option 82.

The configuration example:

Raisecom#**config**

Raisecom(config) **ip dhcp relay information policy keep**

Raisecom(config)#**exit**

Raisecom#**show ip dhcp relay information**

The result is shown below:

Option 82: Enabled

Policy: Keep

Port Trusted

... ..

Port DHCP Relay trust configuration

By default, if one DHCP message gateway address part is 0 and relay agent information option part (option 82) exists, then DHCP Relay will drop messages of this kind. If DHCP Relay is required to transmit messages of this kind, use the command to configure DHCP Relay port trust. After the specific port has configured DHCP Relay port trust command, these port can transmit this kind of DHCP messages normally. You can also use the key word all to set all the system port Relay Agent Information Option port trust.

When configuring port trust, except the configuration commands in config mode, you can configure the port trust state under the port directly as well, which is flexible.

The configuration steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp relay information trusted port-list 1-7	Set port 1-7 to trusted port
3	interface ip 8	Enter port 8 configuration mode
4	ip dhcp relay information trusted	Configure the destination IP 10.201.0.200
5	exit	Return to global configuration mode
6	exit	Return to privileged EXEC mode
7	show ip dhcp relay information	Show DHCP Relay support Option 82 configuration information and port trust table

Notice: Only when DHCP Relay support Option 82 can port trust take effect.

Use global configuration command **no ip dhcp relay information port-list** to set the port to distrust

port, in the corresponding port configuration mode use port configuration command **no ip dhcp relay information option** to realize it.

Configuration example:

```
Raisecom#config
```

```
Raisecom(config) ip dhcp relay information trusted port-list 1-7
```

```
Raisecom(config)#interface ip 8
```

```
Raisecom(config-port)# ip dhcp relay information trusted
```

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

```
Raisecom(config)#exit
```

```
Raisecom#show ip dhcp relay information
```

Option 82: Disabled

Policy: Replace

<i>Port</i>	<i>Trusted</i>

<i>1</i>	<i>yes</i>
<i>2</i>	<i>yes</i>
<i>3</i>	<i>yes</i>
<i>4</i>	<i>yes</i>
<i>5</i>	<i>yes</i>
<i>6</i>	<i>yes</i>
<i>7</i>	<i>yes</i>
<i>8</i>	<i>yes</i>
<i>...</i>	<i>...</i>
<i>...</i>	<i>...</i>

6.4.3 Monitoring and maintaining

Use different show commands to show switch DHCP Relay running state and configuration state for monitoring and maintaining. All the show commands are listed below:

Command	Description
show ip dhcp relay	Show DHCP Relay configuration.
show ip dhcp relay statistics	Show DHCP Relay static.
show ip dhcp relay information	Show the configured neighbor DHCP proxy address information.

Use the command **show ip dhcp relay** to show HDCP Relay basic configuration information, including DHCP Relay state, IP port DHCP Relay state and the corresponding DHCP proxy destination IP address.

```
Raisecom#show ip dhcp relay
```

DHCP Relay: Enabled

<i>IP Interface</i>	<i>Enabled Status</i>	<i>Target IP Address</i>

0	<i>enabled</i>	10.199. 0.200
1	<i>enabled</i>	10.199. 0.200
10.200.0.200		
2	<i>enabled</i>	10.199. 0.200
10.200.0.200		
3	<i>enabled</i>	10.199. 0.200
10.200.0.200		
10.201.0.200		
4	<i>enabled</i>	10.199. 0.200
...
...

Use the command **show ip dhcp relay statistics** to show DHCP Relay static, including DHCP Relay running time and received/sending messages number.

Raisecom#**show ip dhcp relay ip-pool**

Runtime: 0 hours 23 minutes 34 seconds

<i>Packet Type</i>	<i>Receive</i>	<i>Send</i>

<i>Bootp</i>	0	0
<i>Discover</i>	1	1
<i>Request</i>	1	1
<i>Decline</i>	0	0
<i>Offer</i>	0	0
<i>Ack</i>	0	0
<i>Nack</i>	0	0
<i>Decline</i>	0	0
<i>Inform</i>	0	0
<i>Unknowns</i>	0	0
 <i>Total</i>	 2	 2

Use the command **show ip dhcp relay information** to show DHCP Relay support Option 82 configuration information and port trust table:

Raisecom#**show ip dhcp relay information**

Option 82: Enabled

Policy: Replace

<i>Port</i>	<i>Trusted</i>

1	yes
2	no
3	yes
4	yes
...	...

Note:

DHCP Relay supporting Option 82 includes:

- Enabled
- Disabled

The strategy includes:

- Drop
- Keep
- Replace

6.4.4 Typical configuration example

DHCP Relay typical configuration example is like DHCP Server typical configuration example. The following is about a example that the client using DHCP Snooping connects to DHCP Relay and get IP address.

1) Configuration instruction

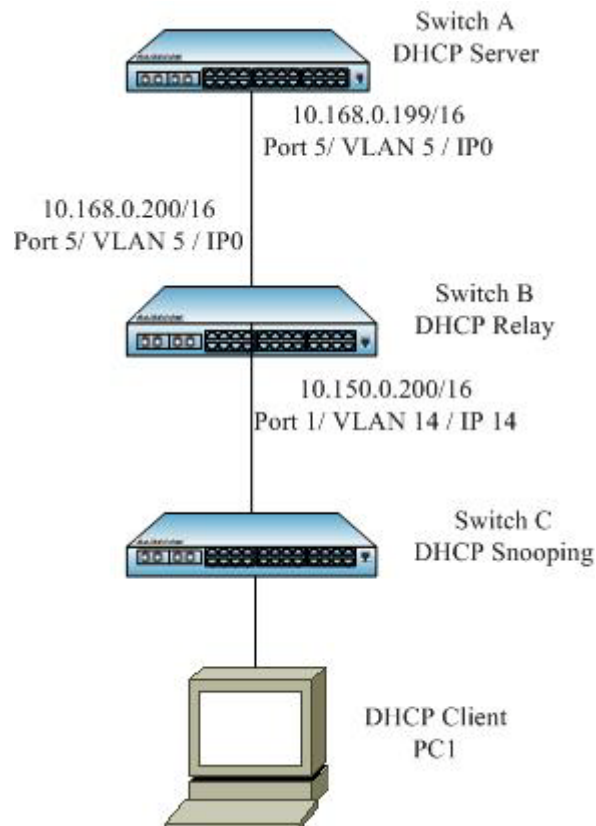
1: The connection of starting Snooping on DHCP Snooping equipment is as fig 3-2, start DHCP Snooping support option 82, and set port 2 to DHCP Snooping trust port.

2: DHCP Relay divides two subnets, the connection between it and the client and the server connection and configuration is as the figure below. Follow the figure to configure VLAN, IP port address and the VLAN that the port belongs to.

3: DHCP Server divides two subnets, establish correct address pool (10.150.0.2 – 10.150.0.100) on the subnet, start DHCP Server function at the same time and configure relay-ip shown in the figure (consult DHCP Server module configuration guide). Then follow the figure to configure VLAN, IP port address and VLAN the port belongs to, and configure it to the router belongs to 10.150 network segment.

4: Set PCI to auto acquiring IP address.

2) Topology figure



Typical configuration

3) Configuration steps:

Configure DHCP Relay:

- Start global DHCP Relay

Raisecom (config)#**ip dhcp relay**

- Prot 14 configure destination IP addresss

Raisecom (config)# **ip dhcp relay ip-list 14 target-ip 10.168.0.199**

- Start DHCP Realy support option 82

Raisecom (config) #**ip dhcp relay information option**

- Configure port 1 as DHCP Relay trust port

Raisecom (config) #**ip dhcp relay information trusted port-list 1**

- Open the router function

Raisecom (config)# **ip dhcp relay ip routing**

a) Show the result

- Show the client PC1

```
C:\>ipconfig /all
```

```
Ethernet adapter local connection
```

```
Connection-specific DNS Suffix . :
```

```
Description . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
```

```
Physical Address. . . . . : 00-50-8D-4B-FD-27
```

```

DHCP Enabled. . . . . : Yes
Autoconfiguration Enable. . . : Yes
IP Address. . . . . : 10.150.0.0
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
DHCP server. . . . . : 10.168.0.199
DNS Servers . . . . . :
Lease Obtained. . . . . : 13:03:24
Lease Expires. . . . . : 13:33:24

```

6.4.5 DHCP Relay trouble shooting

- If the correct destination IP address is not designated, DHCP Relay cannot transmit the message correctly.
- If the gateway address field of a DHCP message is 0 and relay agent information option field exists, DHCP Relay trusted port will drop messages of this kind.

If the configuration above still cannot help, please examine if DHCP Relay has started router function, and examine if DHCP server address is correctly configured, if the neighbor proxy default gateway or router is configured.

6.5 DHCP OPTION

6.5.1 DHCP OPTION principle

The DHCP request packet has a variety of options, including a special option exists in DHCP SNOOPING, DHCP RELAY, DHCP SERVER, to identify a client position. This option is OPTION82, which include circuit-id and remote - id. Through them, the SERVER can obtain client position for effectively management.

6.5.2 DHCP OPTION configuration

Default configuration

Function	Default value
global attach-string	None
global remote-id	switch-mac
port circuit-id	None

DHCP OPTION configuration guide

DHCP OPTION can be configured if DHCP SNOOPING and DHCP RELAY are available.

Global DHCP OPTION attach-string

By default, global DHCP OPTION attach-string is empty. OPTION82 format in DHCP OPTION is:
Port/VLAN/attach-string

Step	Command	Description
1	config	Enter global configuration mode
2	ip dhcp information option attach-string raisecom	Configure DHCP OPTION attach-string as raisecom
3	exit	Return to privileged EXEC mode
4	show ip dhcp information option	Show DHCP OPTION configuration

Port DHCP OPTION circuit-id

By default, port circuit-id is empty. OPTION82 format in DHCP OPTION is:
CIRCUIT_ID

Step	Command	Description
1	config	Enter global configuration mode
2	interface port 10	Enter port 10 configuration
3	ip dhcp information option circuit-id raisecom	Configure circuit-id on port 10 as raisecom
4	exit	Return to global EXEC mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp information option	Show DHCP OPTION configuration

Global DHCP OPTION remote-id

By default, remote-id mode is switch-mac. After the configuration, DHCP OPTION82 will be sent by the configured mode.

- switch – mac: remote - id is sent by switch MAC address in binary form;
- client-mac : remote - id is sent by client MAC address in binary form
- switch-mac-string: remote - id is sent by switch MAC address string
- client-mac-string: remote - id is sent by client MAC address string
- hostname: remote- id is sent by user-defined host name
- string STRING: remote- id is sent by user-defined string

Step	Command	Description
1	config	Enter global configuration mode

2	ip dhcp information option remote-id switch-mac-string	Set remote-id mode transmitted by switch-mac-string
3	exit	Return to privileged EXEC mode
4	show ip dhcp information option	Show DHCP OPTION configuration

6.5.3 Monitoring and maintaining

By show command, users can learn DHCP OPTION configuration, easy to monitoring and maintaining.

Command	Description
show ip dhcp information option	Show DHCP OPTION configuration

Through above command, users can see the information of global circuit-id, port circuit-id as well as remote-id.

Raisecom#**show ip dhcp information option**

Switch use attach string as circuit ID

attach-string: raisecom

remote ID use switch MAC-address as string mode

6.5.4 Typical configuration

1. If the carrier do not configure OPTION module

If the carrier do not configure DHCP OPTION, the switch will mark the client device position in default way:

Vlan \Port number\ switch-mac

2. If the carrier wants to mark the client device position

➤ If the carrier wants to mark the client device position in the way of attach-string

Configure attach-string in global configuration mode

Raisecom(config)#**ip dhcp information option attach-string** *STRING*

The client position information is as follows:

Port number\VLAN\STRING MAC address (the carrier can choose MAC address mode)

➤ If the carrier wants to mark client device position completely in its own way

In port configuration mode, the carrier is able to mark the client position in its own way, for example, one carrier needs the client mark shown as follows:

Option 1

<Access-Node-Identifier>/PON/<rack> / <shelf> / <slot> / <PON> : <ONT> . <ONT-slot> . <UNI>

Circuit-id can be configuring to the needed format in port mode, the steps are as follows:

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	interface port 10	Enter port 10 configuration mode
3	ip dhcp information option circuit-id <i>CHINA/PON/1/1/08/01:28.1.10</i>	Configure port 10 circuit-id to CHINA/PON/1/1/08/01:28.1.10
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ip dhcp information option	Show DHCP OPTION module configuration

6.5.5 DHCP OPTION trouble-shooting

N/A

Chapter 7 SNMP Configuration Guide

7.1 SNMP principle

7.1.1 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

7.1.2 SNMP V1/V2 interview

SNMPv1 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 cannot 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.

7.1.3 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.

7.2 SNMPv1/v2/v3 management configuration

7.2.1 Default SNMP configuration

Function	Default value
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

7.2.2 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 who's group name is not accorded will be dropped. The whole configuration steps are as follows:

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

4

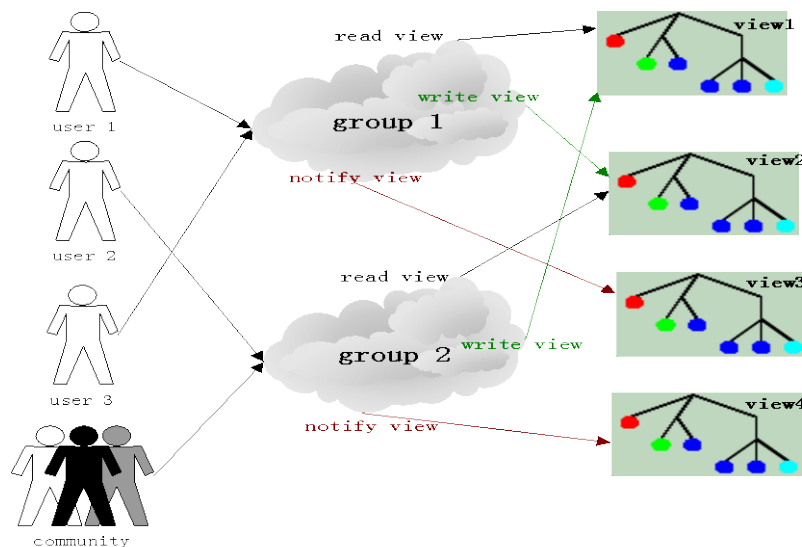
show snmp community

Show group information

Notice: Both SNMPv1 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.

7.2.3 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 like Get 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 <i>username</i> [remote <i>engineid</i>] [authentication { md5 sha } <i>authpassword</i>]	Add a user
3	snmp-server view <i>view-name</i> <i>oid-tree</i> [<i>mask</i>] { included excluded }	Define the view and its privilege of the MIB <i>view-name</i> : specify the configured name of view. <i>oid-tree</i> : specify OID tree <i>mask</i> : 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 <i>groupname</i> <i>user</i> <i>username</i> { v1sm v2csm usm }	Configure the group which the user belongs to

5	snmp-server access <i>groupname</i> [read <i>readview</i>] [write <i>writeview</i>] [notify <i>notifyview</i>] [context <i>contextname</i> [{ exact prefix }]] { v1sm v2csm usm } { noauthnopriv authnopriv }	Define the access privilege of the group <i>Groupname</i> : is the name of access group; <i>readview</i> : is the read view, default is internet; <i>writeview</i> : is the write view, default is empty; <i>notifyview</i> : is informational view, default is empty; <i>contextname</i> : is the name of context or its prefix; exact prefix stands for the match type of the <i>context name</i> : 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

7.2.4 SNMP v1/v2 TRAP configuration

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

7.2.5 SNMPv3 Trap configuration

Step	Command	Description
1	config	Enter global configuration mode.
2	interface ip 0	Enter IP port mode.
3	ip address <i>A.B.C.D</i> [<i>A.B.C.D</i>] <i>vlanID</i>	Configure the switch IP address.

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

7.2.6 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 <i>sysContact</i>	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.

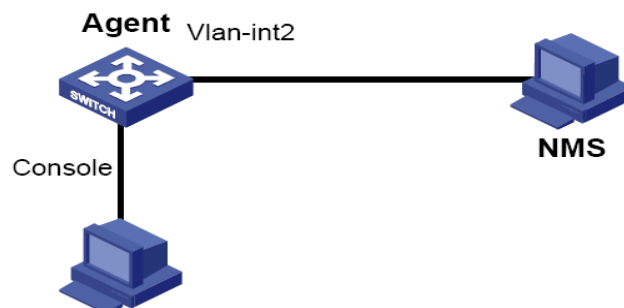
Step	Command	Description
1	config	Enter global configuration mode
2	snmp-server location <i>sysLocation</i>	Configure the switch position <i>sysLocation</i> specify the switch physical position, the type is character stream
3	exit	Return to privileged EXEC mode
4	show snmp config	Show the configuration

7.2.7 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

7.2.8 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

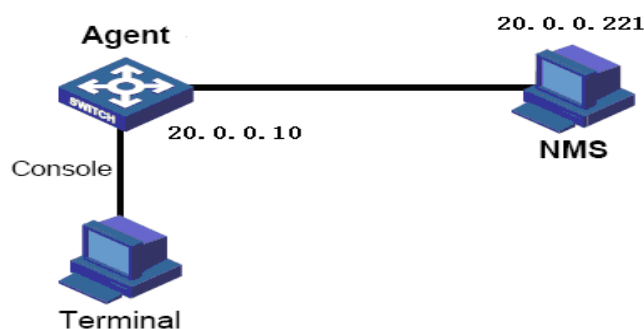
Context Prefix: --
 Context Match: exact
 Read View: system
 Write View: --
 Notify View: internet

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**

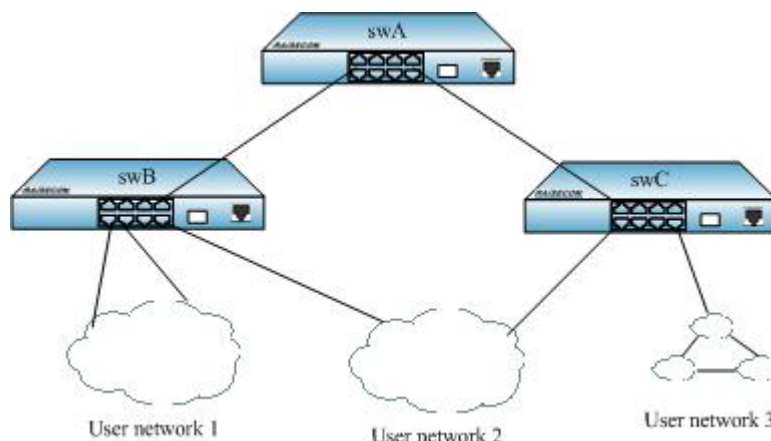
Raisecom(config)# **snmp-server host 20.0.0.221 version 3 authnopriv raisecom**

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 8 Loopback Detection Configuration Guide

8.1 Loopback detection introduction



Loopback detection is mainly used in edge port, as shown in Figure 1, swB and swC mouth. Open the loop detection function port and periodically send the loop detection message. As these ports are the edge port, so the switch under normal circumstances should not receive any message loop detection, if it receives, it means that there are Errors in configuration or loops. If a device receives its own message loop detection, it indicates that the ring appeared. In order to prevent the same time blocking several ports, the received message loop detection port will be blocked only in the case that the receiving package is not less than the sending port. If other devices received the message loop detection is considered an error configuration.

8.2 Loopback detection default configuration

Loopback detection function is disable.

8.3 Loopback detection function configuration

8.3.1 Open or close port loopback detection function

This configuration is used to open or close port loopback detection function.

Step	Command	Description
1	config	Enter global configuration mode
2	loopback-detection {enable disable} port-list portlist	Open/close port loopback detection function <i>portlist</i> : refers to port list
3	show loopback-detection port-list portlist	Show loopback detection status

8.3.2 Configure destination MAC address and VLAN Function

This configuration is used to configure loop detection of destination MAC address. It suggests that configuration within the topology is consistency, or may lead to fail to detect.

Step	Command	Description
1	config	Enter global configuration mode
2	[no] loopback-detection destination-address <i>HHHH.HHHH.HHHH</i>	Configure loopback detection message destinations MAC address. HHHH.HHHH.HHHH: configuration destination MAC address.
3	show loopback-detection port-list <i>portlist</i>	Show loopback detection status

This configuration is used to configure loop detection VLAN, as for specific topology and configuration, the different vlan will show different loop status. By configuring the value of this vlan, vlan can check whether there is a loop. It suggests that the configuration within topology is consistent, or may lead to fail to detect.

Step	Command	Description
1	config	Enter global configuration mode
2	[no] loopback-detection vlan <i>vlanid</i>	Configure loopback detection vlan. <i>vlanid</i> : requisite vlan
3	show loopback-detection port-list <i>portlist</i>	Show loopback detection status

8.3.3 Configure cycle loopback detection function

Circle detection is to detect the presence of loops by sending hello packets periodically; the cycle of sending periodic hello packets is loop detection cycle. It is not conducive to detect loop on time if cycle is too large, while it will make the hello packets increase in a certain period of time and increase the burden of network and equipment if cycle is too small. It suggests that the configuration in the topology is consistent, because the other parameters, such as blocking test time, need to refer to this cycle, if the cycle configuration is inconsistency that may lead to coordination errors between devices, the module does not work.

Step	Command	Description
1	config	Enter global configuration mode
2	loopback-detectionhello -time <i>hellotime</i>	Configure loopback detection cycle <i>hellotime</i> : the cycle value unit is second.
3	show loopback-detection port-list <i>portlist</i>	Show loopback detection status

8.3.4 Configure loop detection automatically release the blocked port time

The port after loop is blocked can be detected automatically after a certain period of time, if the loop has been eliminated then open the port, the time depends on the configuration and the actual situation. This configuration is a real time base configuration, not the actual block time. When the port is

blocked, after the configured time, the loop will be detected, if the loop is lifted, then release the port; if the loop is still there, then the next probe need to go through twice the time base, if there, Then three times ... the relationship was gradually increased, but the maximum of 65535s. It can also be configured to automatically restore said they did not infinite, and is configured to trap-only trap that only sent without closing the port.

Step	Command	Description
1	config	Enter global configuration mode
2	loopback-detection down-time { <i>infinite</i> / <i>trap-only</i> / <i>downtime</i> }	Configure loop detection automatically recover time Downtime is the base. The unit is second.
3	show loopback-detection port-list portlist	Show loopback detection status

8.3.5 Configure other receiving device loop detection the message approach

When an opened loop detection port received loop detection packet and MAC address the packet carrying is inconsistent with this device, the default approach is to send a trap. If the MAC address is smaller than the MAC address of the device, the port will make a suspension to send the loop detection packet 10 hellotime times. In addition, in the case of the presence of the loop, a packet may be flooded, leading repeatedly to receive the same packet, in order to prevent excessive trap against increasing the burden of network and network management, if within 20 hellotime Receive the same message will not send trap. When receiving other devices loop detection packet, it can also choose the method that deals with blocking. In order to avoid blocking multiple devices at the same time, only the receiving packets carried the MAC address is smaller than the device itself will be blocked.

Step	Command	Description
1	config	Enter global configuration mode
2	loopback-detection error-device { <i>discarding</i> / <i>trap-only</i> } port-list <i>portlist</i>	Configure loopback detection receiving other device approach <i>discarding</i> : sending trap and blocking <i>trap-only</i> : only sending <i>portlist</i> : the port list
3	show loopback-detection port-list portlist	Show loopback detection status

8.3.6 Manually open the port blocked

After the port is blocked by loop detection, it can be allowed to automatically recover; besides, you can also manually open ports. Before opening the port will conduct loop detection, if the loop is there, it will continue to obstruct.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port port_num	Enter port configuration mode <i>port_num</i> : port number It can use interface range portlist Into the batch configuration mode to

		configure multiple ports <i>portlist</i> : port list
3	no loopback-detection discarding	Release loop detection blocked port
4	show loopback-detection port-list <i>portlist</i>	Show loopback detection status

8.3.7 Clear loop detection statistics

Statistical information is recorded in units of the port, including the number of sent packets loop detection, the number of received packets loop detection, the number of blocked, error device records information. Clear statistics will make counting became zero.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>port_num</i>	Enter port configuration mode <i>port_num</i> : port list It can use interface range portlist Into the batch configuration mode to configure multiple ports <i>portlist</i> : port list
3	clear loopback-detection statistic	Clear loopback detection statistics information Portlist port list
4	show loopback-detection statistic port-list <i>portlist</i>	Show loopback detection statistics information

8.4 Monitoring and Maintenance

Command	Description
show loopback-detection port-list <i>portlist</i>	Show loopback detection statistics information <i>portlist</i> : port list
show loopback-detection statistic port-list <i>portlist</i>	Show loopback detection statistics information <i>portlist</i> : port list

8.5 Typical Configuration Examples

Example 1: enable port 1-5 loopback detection.

Raisecom#**config**

Raisecom(config)#**loopback-detection enable port-list 1-5**

Raisecom(config)#**show loopback-detection port-list 1-9**

Destination address: FFFF.FFFF.FFFF

VLAN:1

Period of loopback-detection:4s

Restore time:infinite

Port State Status exloop-act Last Last-Occur Open-Time vlan

					Loop-with	(ago)	(ago)

1	Ena	no	trap-only	--	--	--	--
2	Ena	no	trap-only	--	--	--	--
3	Ena	no	trap-only	--	--	--	--
4	Ena	no	trap-only	--	--	--	--
5	Ena	no	trap-only	--	--	--	--
6	Dis	no	trap-only	--	--	--	--
7	Dis	no	trap-only	--	--	--	--
8	Dis	no	trap-only	--	--	--	--
9	Dis	no	trap-only	--	--	--	--

Example 2: Configure destination MAC address as 0012.3456.7890, VLAN as 3, Cycle as 10s, automatically open port time is 60s, port 6-9 receive the other device approach is discarding.

Raisecom(config)#**loopback-detection destination-address 0012.3456.7890**

Raisecom(config)#**loopback-detection vlan 3**

Raisecom(config)#**loopback-detection hello-time 10**

Raisecom(config)#**loopback-detection down-time 60**

Raisecom(config)#**loopback-detection error-device discarding port-list 6-9**

Raisecom(config)#**show loopback-detection port-list 1-9**

Destination address: 0012.3456.7890

VLAN:3

Period of loopback-detection:10s

Restore time:60s

Port	State	Status	exloop-act	Last	Last-Occur	Open-Time	vlan
					Loop-with	(ago)	(ago)

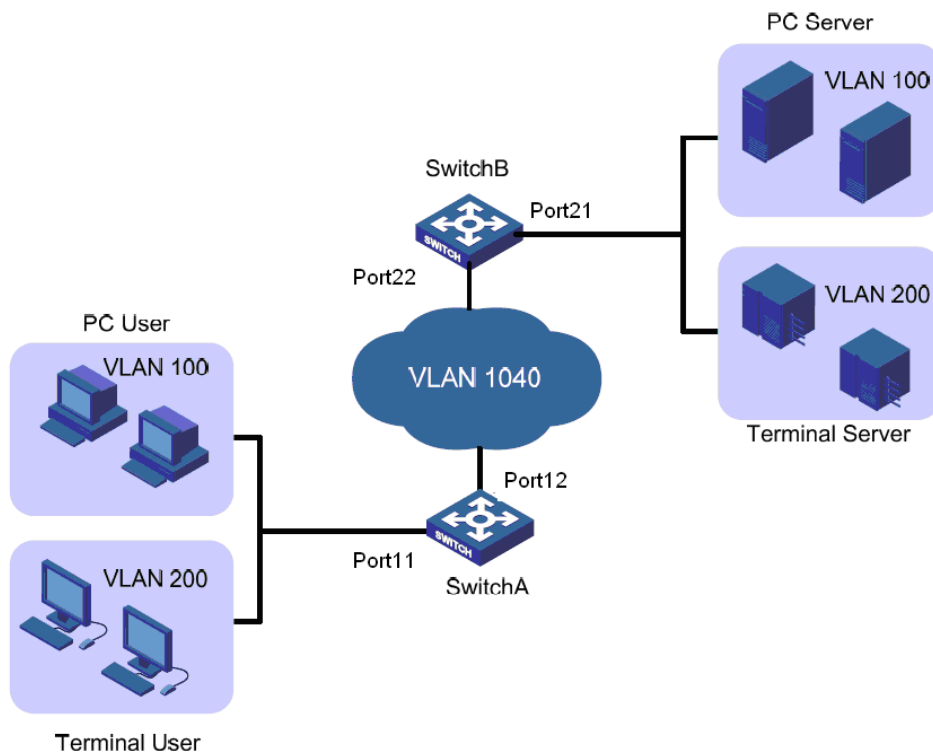
1	Ena	no	trap-only	--	--	--	--
2	Ena	no	trap-only	--	--	--	--
3	Ena	no	trap-only	--	--	--	--
4	Ena	no	trap-only	--	--	--	--
5	Ena	no	trap-only	--	--	--	--
6	Dis	no	discarding	--	--	--	--
7	Dis	no	discarding	--	--	--	--
8	Dis	no	discarding	--	--	--	--
9	Dis	no	discarding	--	--	--	--

Chapter 9 QinQ Configuration

9.1 QinQ principle overview

9.1.1 Basic QinQ

Basic QinQ is a kind of simple layer-two VPN channel technology, which makes message being able to go through the carriers' backbone network (public network) by encapsulating outer-layer VLAN Tag on the carrier access end for the private network messages. In public network, messages transmit according only to outer-layer VLAN Tag, while user private VLAN Tag can be transmitted as the data in the message. The technology helps relieving the public network VLAN ID resource that is becoming rare, while user can now his own private VLAN ID which wouldn't conflict with public network VLAN ID. The typical topology structure of basic QinQ is shown below:



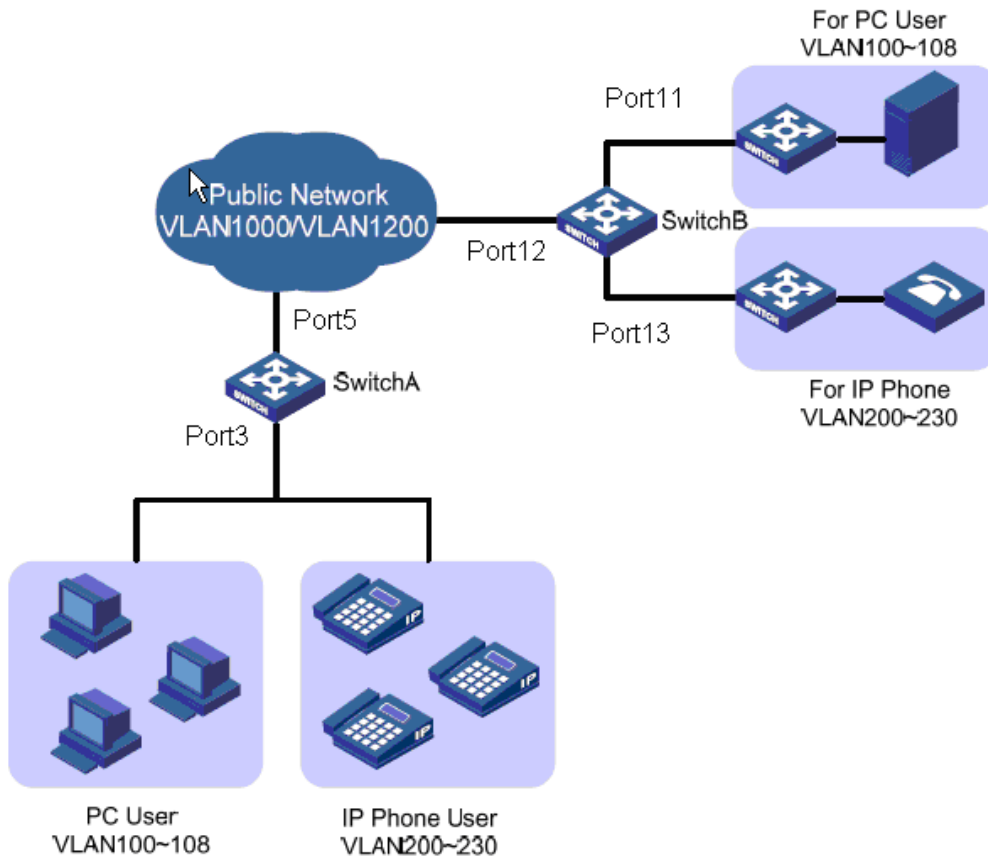
The typical topology of basic QinQ

With QinQ, the limitation of 4096 VLAN on metropolitan area Ethernet can be broken through. The technology extends the ability of establishing layer-two network with VLAN, and it realizes MAN layer-two VPN, which fits MAN and WAN services.

9.1.2 Flexible QinQ

Flexible QinQ is an enhanced application of basic QinQ, which is based on the combination of port and VLAN. Except all the function of basic QinQ, flexible QinQ can take different action according to different VLAN Tags for the messages received from the same port, and adds different outer-layer

VLAN ID for different inner-layer VLAN ID. With flexible QinQ, user can configure inner and outer layer Tag mapping rule, and encapsulate different outer-layer Tags for the messages with different inner-layer Tags according to the mapping rules. Flexible QinQ makes carriers network structure more elastic, and different terminal users can be sorted on the port that is connected with access devices according to VLAN Tag, while QoS strategy can be configured on public network according to outer-layer Tag, and configure the transmission priority flexibly, so that each user can acquire corresponding service. The typical topology structure of flexible QinQ is shown below:



A typical topology structure of flexible QinQ

9.1.3 VLAN conversion

VLAN conversion is mainly used to replace the private VLAN Tag of user message with the VLAN Tag of public network, so that the message can be transmitted as the network planning of the public network. When the messages are transmitted to user's private network, the VLAN Tag will be restored the previous user private network VLAN Tag, so that the messages can be sent to destination correctly.

When the switch receives a message with user private network VLAN Tag, user private network message will be matched following the configured VLAN conversion rules. If they match each other successfully, the private network VLAN Tag will be replaced following the VLAN conversion rules.

Different from QinQ, VLAN conversion function needs not multi-layer VLAN Tag encapsulation, and let the messages transmit in the network planning of public network. The typical topology of VLAN conversion is similar with typical flexible QinQ topology.

9.2 Basic QinQ configuration

9.2.1 Default configuration

Function	Default value
Outer-layer Tag TPID value	0x8100
Port basic QinQ	Disable
Port double Tag function	disable

9.2.2 Basic QinQ function configuration

Step	Command	Description
1	config	Enter global configuration
2	mls double-tagging tpid HHHH	Configure outer-layer Tag TPID (optical) HHHH: TPID value, range is 0x0000-0xFFFF
3	interface port portid	Enter port configuration mode
4	switchport qinq dot1q-tunnel	Enable port basic QinQ function qinq VLAN nesting dot1q-tunnel enable port TUNNEL function
5	exit	Return to global configuration mode
6	interface port portid	Enter port configuration mode (optical)
7	switchport qinq double-tagging	Enable port double Tag function qinq VLAN nesting double-tagging enable port double Tag function
8	exit	Return to global configuration mode

Use **no mls double-tagging tpid** to restore outer-layer Tag TPID to default value, that is 0x8100.

Use **no switchport qinq** to disable port basic qinq function.

Use **no switchport qinq** to disable port double Tag function.

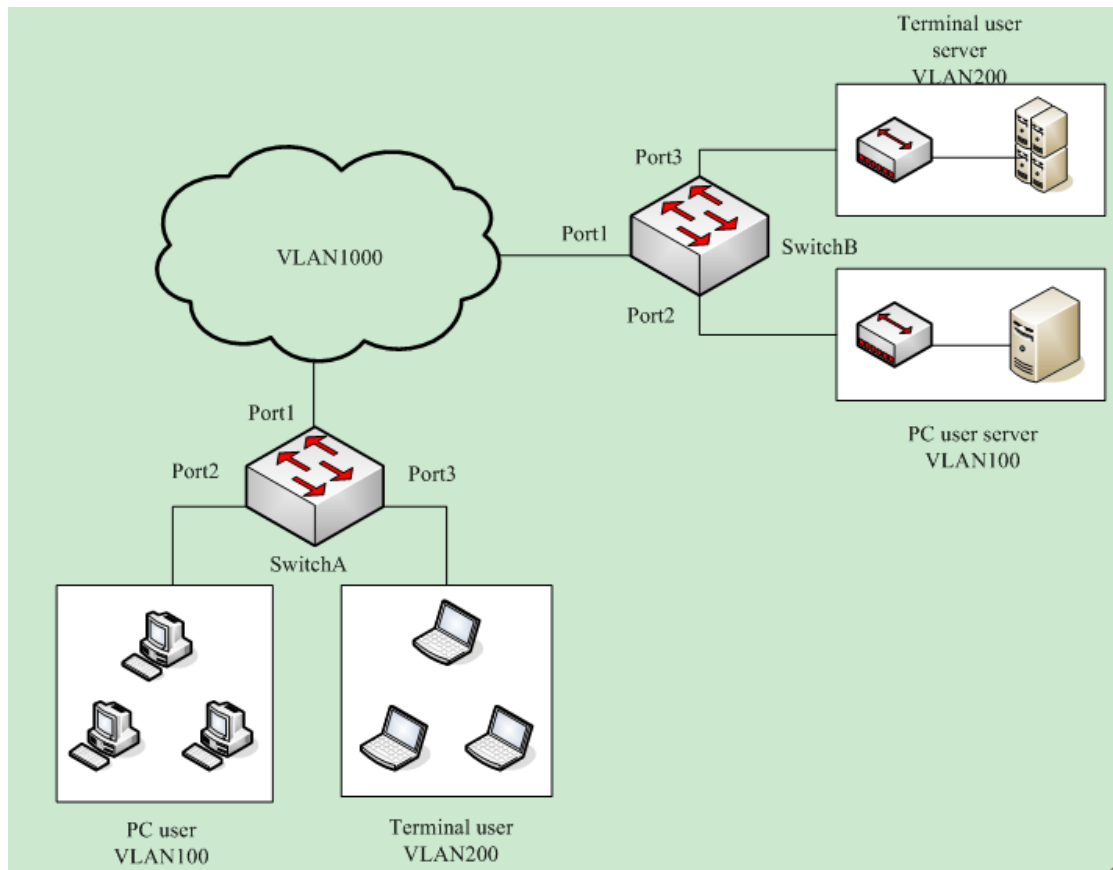
Note: Enable port double Tag function is optical configuration, only parts of the equipments supports the configuration.

9.2.3 Monitoring and maintenance

Command	Description
show switchport qinq	Show port basic QinQ related configuration

9.2.4 Typical configuration example

The topology is shown below:



Basic QinQ topology structure

As above, SwitchA Port2 and Port3 connect PC user in VLAN 100 and terminal user in VLAN 200 respectively, SwitchB port2 and Port3 connect PC user server in VLAN 100 and terminal user server in VLAN 200, VLAN 1000 is used in carrier network for transmission, and the carrier network TPID is 9100. Configure SwitchA and SwitchB to realize basic QinQ function.

The steps to configure SwitchA are shown below:

```
Raisecom#config
```

```
Raisecom(config)#mls double-tagging tpid 9100
```

```
Raisecom(config)#create vlan 100,200,1000 active
```

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

```
Raisecom(config-port)#switchport mode trunk
```

```
Raisecom(config-port)#switchport trunk allowed vlan 1000
```

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

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

```
Raisecom(config-port)#switchport mode access
```

```
Raisecom(config-port)#switchport access vlan 1000
```

```
Raisecom(config-port)#switchport qinq dot1q-tunnel
```

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

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

```
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchprot trunk native vlan 1000
Raisecom(config-port)#switchport qinq dot1q-tunnel
Raisecom(config-port)#exit
Raisecom(config)#show switchport qinq
```

Outer TPID: 0x9100

<i>Port</i>	<i>QinQ Status</i>

<i>1</i>	<i>Double-tagging</i>
<i>2</i>	<i>Dot1q-tunnel</i>
<i>3</i>	<i>Dot1q-tunnel</i>
<i>4</i>	<i>--</i>
<i>5</i>	<i>--</i>
<i>6</i>	<i>--</i>
<i>7</i>	<i>--</i>
<i>8</i>	<i>--</i>

SwitchB are shown below:

```
Raisecom#config
Raisecom(config)#mls double-tagging tpid 9100
Raisecom(config)#create vlan 100,200,1000 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 1000
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode access
Raisecom(config-port)#switchport access vlan 1000
Raisecom(config-port)#switchport qinq dot1q-tunnel
Raisecom(config-port)#exit
Raisecom(config)#interface port 3
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchprot trunk native vlan 1000
Raisecom(config-port)#switchport qinq dot1q-tunnel
Raisecom(config-port)#exit
Raisecom(config)#show switchport qinq
```

Outer TPID: 0x9100

Port	QinQ Status
1	Double-tagging
2	Dot1q-tunnel
3	Dot1q-tunnel
4	--
5	--
6	--
7	--
8	--

9.3 Configure flexible QinQ

9.3.1 Configure flexible QinQ function

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter port configuration mode
3	switchport vlan-mapping <i>vlanlist</i> add-outer <i>vlanid</i>	Add Tag VLAN mapping vlan-mapping: VLAN nesting <i>vlanlist:</i> user network inner layer VLAN IDs add-outer: add outer-layer Tag <i>vlanid</i> : outer-layer VLAN ID
4	exit	Return to global configuration mode

Use **no switchport vlan-mapping add-outer** *vlanid* to delete flexible QinQ adding Tag VLAN mapping rules.

Note:

- In the same port, if the VLAN list of the VLAN mapping rule conflicts with the existed VLAN mapping rules, then the system will return mapping rules confliction, and the configuration fails;
- In the same port, if the VLAN matched mapping rule that is designated by VLAN mapping rule has existed, delete the existed VLAN mapping rule, then the later configured VLAN mapping rule will cover the existed mapping rule.

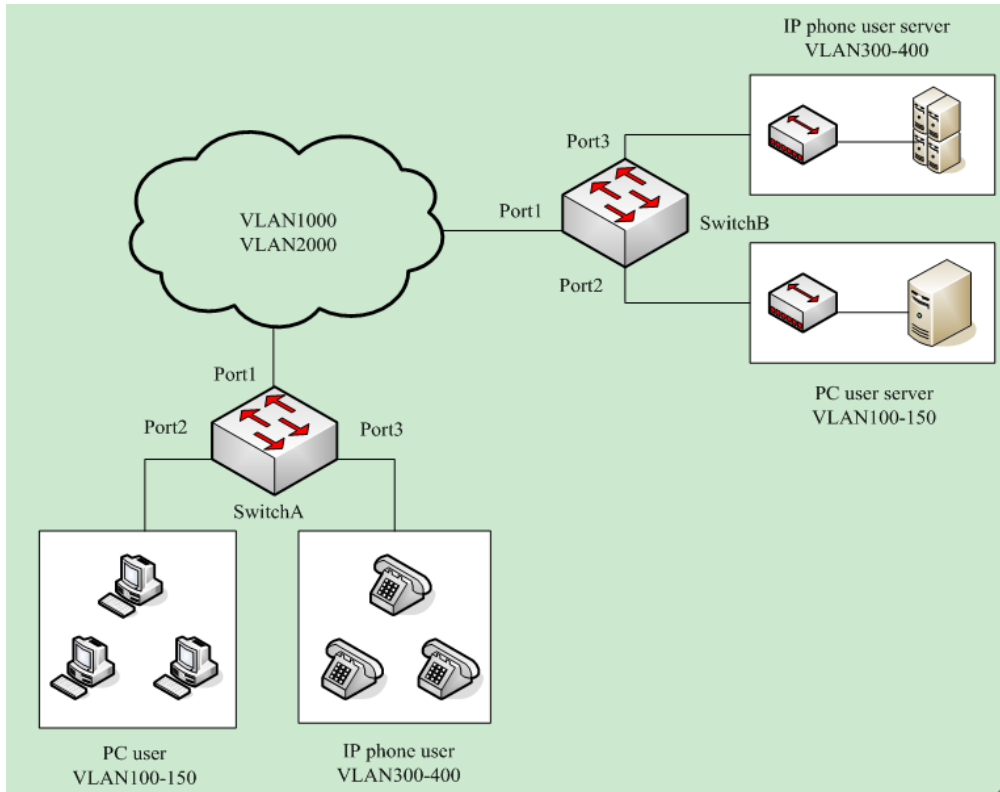
9.3.2 Monitoring and maintenance

Command	Description
show interface port [<i>portid</i>] vlan-mapping add-outer	Show port flexible QinQ adding Tag VLAN mapping rule
show interface line [<i>lineid</i>] vlan-mapping add-outer	Show line port flexible QinQ adding Tag VLAN mapping rule
show interface client [<i>clientid</i>] vlan-mapping add-outer	Show user port flexible QinQ adding Tag VLAN mapping rule

9.3.3 Typical configuration

The topology structure is as below:

SwitchA Port2 and Port3 connect PC user in VLAN 100 and terminal user in VLAN 200 respectively, SwitchB port2 and Port3 connect PC user server in VLAN 100-150 and IP phone user server using VLAN 300-400, VLAN 1000 is used in carrier network for transmission, and the carrier network TPID is 9100. Configure SwitchA and SwitchB flexible QinQ function to realize the normal communication between the server and PC/IP phone user.



Flexible QinQ topology structure

The steps to configure SwitchA are shown below:

```
Raisecom#config
```

```
Raisecom(config)#mls double-tagging tpid 9100
```

```
Raisecom(config)#create vlan 100-150,300-400,1000,2000 active
```

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

```
Raisecom(config-port)#switchport mode trunk
```

```
Raisecom(config-port)#switchport trunk allowed vlan 1000,2000
```

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

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

```
Raisecom(config-port)#switchport mode trunk
```

```
Raisecom(config-port)#switchport vlan-mapping 100-150 add-outer 1000
```

```
Raisecom(config-port)#switchport trunk untag vlan 1000,2000
```

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

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

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

Raisecom(config-port)#**switchprot vlan-mapping 300-400 add-outer 2000**

Raisecom(config-port)#**switchport trunk untag vlan 1000,2000**

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

Raisecom(config)#**show interface port 2 vlan-mapping add-outer**

Port	Original Inner VLAN List	Add-outer VLAN	Hw Status	Hw-ID
2	100-150	1000	Enable	1

Raisecom(config)#show interface port 3 vlan-mapping add-outer

Port	Original Inner VLAN List	Add-outer VLAN	Hw Status	Hw-ID
3	300-400	2000	Enable	2

SwitchB is configured as below:

Raisecom#**config**

Raisecom(config)#**mls double-tagging tpid 9100**

Raisecom(config)#**create vlan 100-150,300-400,1000,2000 active**

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

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

Raisecom(config-port)#**switchport trunk allowed vlan 1000,2000**

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

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

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

Raisecom(config-port)#**switchport vlan-mapping 100-150 add-outer 1000**

Raisecom(config-port)#**switchport trunk untag vlan 1000,2000**

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

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

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

Raisecom(config-port)#**switchport vlan-mapping 300-400 add-outer 2000**

Raisecom(config-port)#**switchport trunk untag vlan 1000,2000**

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

Raisecom(config)#**show interface port 2 vlan-mapping add-outer**

Port	Original Inner VLAN List	Add-outer VLAN	Hw Status	Hw-ID
2	100-150	1000	Enable	1

Raisecom(config)#show interface port 3 vlan-mapping add-outer

Port	Original Inner VLAN List	Add-outer VLAN	Hw Status	Hw-ID
3	300-400	2000	Enable	2

9.4 Configure VLAN conversion

9.4.1 Configure VLAN conversion

Configure VLAN conversion based on single Tag

The steps to configure 1:1 VLAN conversion are shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	vlan-mapping (<i>enable</i> / <i>disable</i>)	Enable or disable vlan-mapping
3	interface port <i>portid</i>	Enter port configuration mode
4	switchport vlan-mapping ingress <i>vlanlist translate vlanid</i>	Configure ingress VLAN conversion rule vlan-mapping : VLAN-mapping ingress : ingress <i>vlanlist</i> : user network inner layer VLAN IDs translate : translate vlanid : outer-layer VLAN ID
5	switchport vlan-mapping egress <i>vlanlist translate vlanid</i> switchport vlan-mapping egress outer (<i>all</i> <i>vlanlist</i>) [<i>inner vlanlist</i>] outer (translate <i>vlanid</i> remove tagged unchanged) [<i>inner</i> (translate <i>vlanid</i> remove tagged)]	Configure egress VLAN conversion rule vlan-mapping : VLAN-mapping egress : egress translate : translate <i>vlanid</i> : outer-layer VLAN ID remove : remove TAG tagged : add TAG <i>unchanged</i> : remain unchanged <i>id</i> : VLAN-mapping ID
6	exit	Return to global configuration mode

Use **no switchport vlan-mapping ingress translate** *vlanid* to delete ingress VLAN transmission rule configured under port.

Use **no switchport vlan-mapping egress translate** *vlanid* to delete egress VLAN transmission rule under port.

Note:

- To configure 1:1 VLAN transmission, it is needed to configure both ingress VLAN conversion and egress VLAN conversion.
- For some equipment, in port egress VLAN conversion outer VLAN can't be the same with TRUKE NATIVE VLAN on the port. Under ACCESS mode, configure TRUNK NATIVE alike outer vlan of VLAN conversion rule, then it will failure when configured to TRUNK. Modify or delete it, TRUNK mode can be successful again;

The steps to configure N:1 VLAN conversion are shown below:

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter port configuration mode
3	switchport vlan-mapping cvlan {1-4094} translate <1-4094>	Configure flexible QinQ adding Tag VLAN mapping rule vlan-mapping : VLAN-mapping cvlan : based on outer vlan conversion {1-4094}: user network inner layer VLAN IDs translate : translate <1-4094>: outer-layer VLAN ID
4	exit	Return to global configuration mode

Use **no switchport vlan-mapping cvlan translate** <1-4094> to delete VLAN conversion rule under port.

The steps to configure N:N VLAN conversion are shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	vlan-mapping (<i>enable</i> <i>disable</i>)	Enable or disable vlan-mapping
3	interface port <i>portid</i>	Enter port configuration mode
4	switchport vlan-mapping ingress vlanlist translate <i>vlanlist</i>	Configure ingress vlan-mapping <i>vlanlist</i> : outer VLAN IDs
5	switchport vlan-mapping egress <i>vlanlist</i> translate <i>vlanid</i> switchport vlan-mapping egress outer (<i>all</i> <i>vlanlist</i>) [<i>inner vlanlist</i>] outer (translate <i>vlanid</i> remove tagged unchanged) [<i>inner (translate</i> <i>vlanid</i> <i>remove</i> tagged)]	Configure egress VLAN conversion rule vlan-mapping : VLAN-mapping egress : egress translate : translate <i>vlanid</i> : outer-layer VLAN ID remove : remove TAG tagged : add TAG <i>unchanged</i> : remain unchanged <i>id</i> : VLAN-mapping ID
6	exit	Return to global configuration mode

The command of **no switchport vlan-mapping ingress translate** *vlanlist* can delete ingress vlan-mapping.

The command of **no switchport vlan-mapping egress translate** *vlanlist* can delete egress vlan-mapping.

Note:

- N: N VLAN conversion must have ingress and egress VLAN conversion on the port at the same time.
- The same number of the VLAN before or after the N: N VLAN conversion, and a VLAN list is according to the ascending or descending arrangement.
- For some equipment, outer VLAN in egress VLAN conversion can't be the same with TRUNK mode NATIVE VLAN. When under ACCESS mode, TRUNK NATIVE VLAN is alike outer VLAN in VLAN conversion, it will fail to configure the port for TRUNK.

The steps to configure acl-based VLAN conversion are shown below:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter port configuration mode
3	switchport vlan-mapping acl <i><0-399></i> translate [inner <i><1-4094></i>][outer <i><1-4094></i>][innercos <i><0-7></i>][outercos <i><0-7></i>]	Configure acl-based vlan conversion. <i>vlan-mapping</i> : VLAN mapping <i>acl</i> : acl-based vlan conversion <i><0-399></i> : acl number <i><1-4094></i> : inner VLAN ID <i><1-4094></i> : outerVLAN ID <i>innercos</i> : inner VLAN COS <i>outercos</i> : outer VLAN COS
4	exit	Return to global configuration mode

The command of **no switchport vlan-mapping acl** *<0-399>* **translate** can delete it,

Configure VLAN conversion based on two Tag

Step	Command	Description
1	config	Enter global configuration
2	interface port <i>portid</i>	Enter port configuration mode
3	switchport vlan-mapping ingress outer (all <i>vlanlist</i>) inner (all <i>vlanlist</i>) translate outer <i>vlanid</i>	Configure flexible QinQ adding Tag VLAN mapping rule vlan-mapping : VLAN-mapping ingress : ingress outer :outer-layer tag all : all VLAN IDs vlanlist :user network outer-layer VLAN ID inner : inner-layer tag all : all VLAN IDs vlanlist user network inner VLAN IDs translate : translate outer : outer-layer Tag <i><1-4094></i> :outer-layer VLAN ID
4	exit	Return to global configuration mode

Use **no switchport vlan-mapping ingress translate** *<1-4094>* to delete VLAN conversion rule configured under port.

Note:

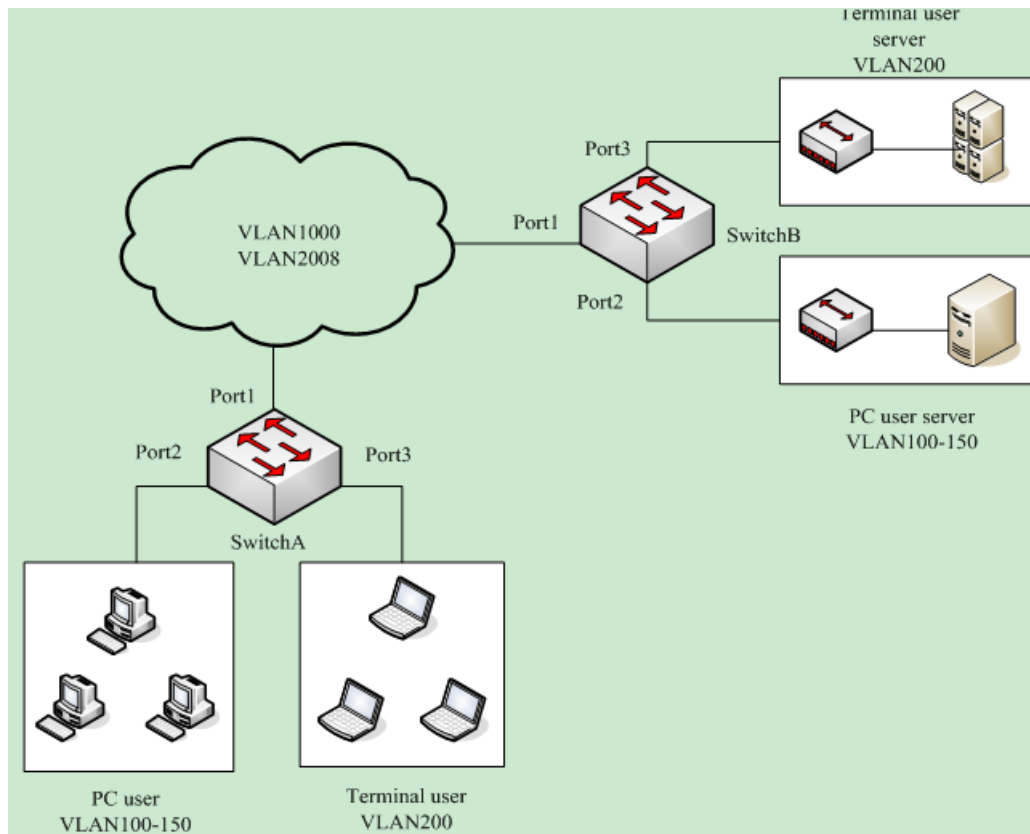
- In the same port, if the VLAN list of VLAN transmission rule conflicts with the existed VLAN conversion rule, then the system will return conversion rule confliction and configuration failure.
- In the same port, if the conversion rule that matches the VLAN designated with the VLAN conversion rules exists, then the existed VLAN conversion rule will be deleted, and the later configured VLAN conversion rule will cover the existed conversion rule.

9.4.2 Monitoring and maintenance

Command	Description
show interface port [<i>portid</i>] vlan-mapping (<i>ingress</i> / <i>egress</i> / <i>both</i>) translate	Show port VLAN conversion rule
show interface line [<i>lineid</i>] vlan-mapping (<i>ingress</i> / <i>egress</i> / <i>both</i>) translate	Show line port VLAN conversion rule
show interface client [<i>clientid</i>] vlan-mapping (<i>ingress</i> / <i>egress</i> / <i>both</i>) translate	Show user port VLAN conversion rule
show interface port [<1-MAX_PORT_STR>] vlan-mapping acl translate	Show ACL-based vlan conversion

9.4.3 Typical configuration example

The typical configuration example based on single Tag VLAN



VLAN conversion topology structure based on single TAG

As above, SwitchA Port2 and Port3 connects PC user in VLAN100-150, SwitchB Port2 and Port3 connects PC user server using VLAN100-150 and terminal user server using VLAN200. In the carrier network VLAN1000 will be designated to PC user for transmission, while VLAN2008 will be designated to terminal user for transmission. By configuring 1:1 and N:1 VLAN conversion on SwitchA and SwitchB to realize the communication between the servers and PC/terminal user.

The configuration:

SwitchA configuration:

Raisecom#**config**

Raisecom(config)#**create vlan 100-150,200,1000,2008 active**

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

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

Raisecom(config-port)#**switchport trunk allowed vlan 1000,2008**

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

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

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

Raisecom(config-port)#**switchport vlan-mapping cvlan 100-150 translate 1000**

Raisecom(config-port)#**switchport trunk allowed vlan 100-150**

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

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

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

Raisecom(config-port)#**switchport vlan-mapping ingress 200 translate 2008**

Raisecom(config-port)#**switchport vlan-mapping egress 2008 translate 200**

Raisecom(config-port)#**switchport trunk allowed vlan 200**

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

Raisecom(config)#**show interface port 2 vlan-mapping both translate**

Direction: Both

<i>Port</i>	<i>Outer VLAN</i>	<i>Customer VLAN List</i>	<i>Provider VLAN List</i>
2	1000	n/a	100-150

Raisecom(config)#**show interface port 3 vlan-mapping ingress translate**

Direction: Ingress

<i>Port</i>	<i>Original Inner VLANs</i>	<i>Original Outer VLANs</i>	<i>Outer-tag Mode</i>	<i>New Outer-VID Mode</i>	<i>Inner-tag Mode</i>	<i>New Inner-VID Hw-ID</i>
3	n/a	200	Translate	2008	--	1

Raisecom(config)#**show interface port 3 vlan-mapping egress translate**

Direction: Egress

<i>Port</i>	<i>Original Inner VLANs</i>	<i>Original Outer VLANs</i>	<i>Outer-tag Mode</i>	<i>New Outer-VID Mode</i>	<i>Inner-tag Mode</i>	<i>New Inner-VID Hw-ID</i>
3	n/a	2008	Translate	200	--	2

SwitchB is configured as below:

Raisecom#**config**


```

Raisecom(config)#create vlan 100-150,200,1000,2008 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 1000,2008
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport vlan-mapping both 100-150 translate 1000
Raisecom(config-port)#switchport trunk allowed vlan 100-150
Raisecom(config-port)#exit
Raisecom(config)#interface port 3
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport vlan-mapping ingress 200 translate 2008
Raisecom(config-port)#switchport vlan-mapping egress 2008 translate 200
Raisecom(config-port)#switchport trunk allowed vlan 200
Raisecom(config-port)#exit
Raisecom(config)#show interface port 2 vlan-mapping both translate

```

Direction: Both

<i>Port</i>	<i>Outer VLAN</i>	<i>Customer VLAN List</i>	<i>Provider VLAN List</i>
2	1000	n/a	100-150

```

Raisecom(config)#show interface port 3 vlan-mapping ingress translate

```

Direction: Ingress

<i>Port</i>	<i>Original Inner VLANs</i>	<i>Original Outer VLANs</i>	<i>Outer-tag Mode</i>	<i>New Outer-VID</i>	<i>Inner-tag Mode</i>	<i>New Inner-VID</i>	<i>Hw-ID</i>
3	n/a	200	Translate	2008	--	--	1

```

Raisecom(config)#show interface port 3 vlan-mapping egress translate

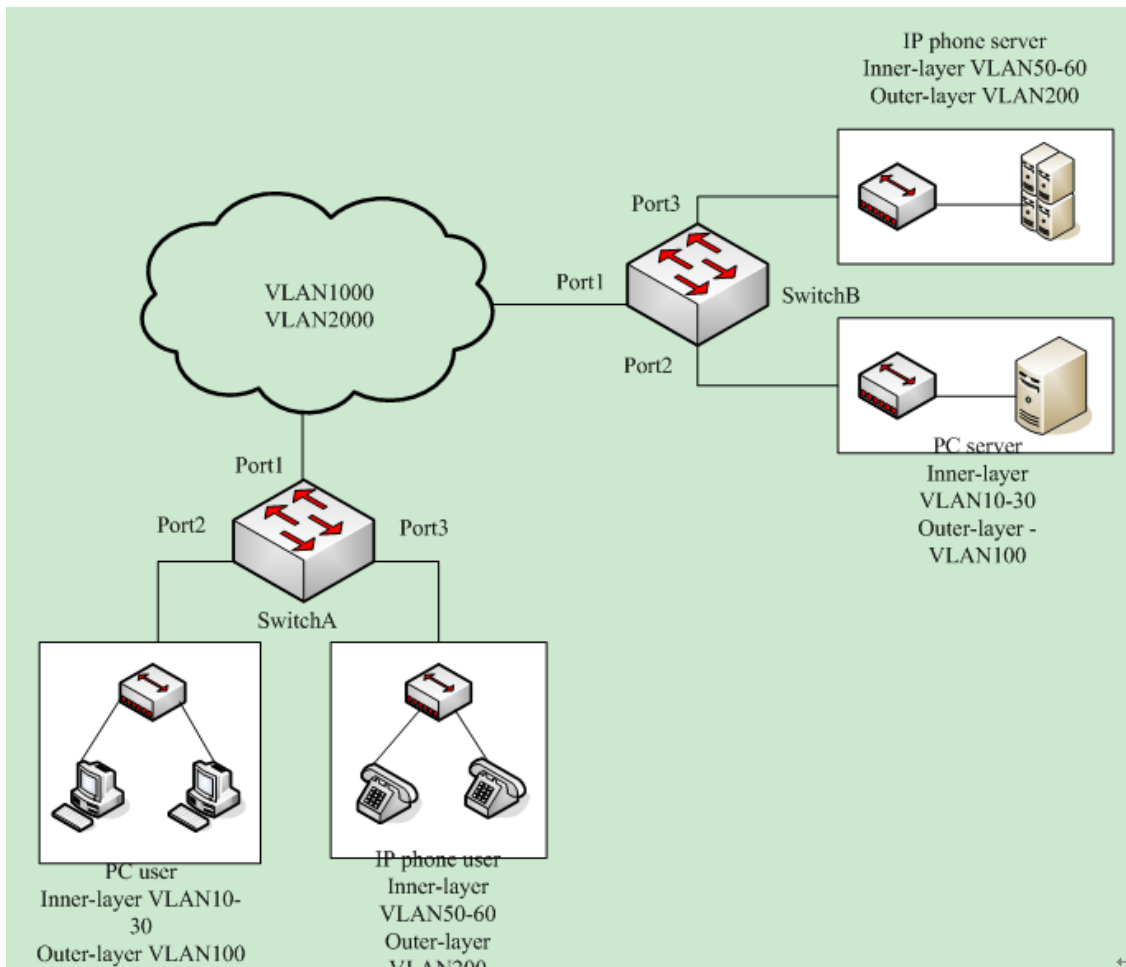
```

Direction: Egress

<i>Port</i>	<i>Original Inner VLANs</i>	<i>Original Outer VLANs</i>	<i>Outer-tag Mode</i>	<i>New Outer-VID</i>	<i>Inner-tag Mode</i>	<i>New Inner-VID</i>	<i>Hw-ID</i>
3	n/a	2008	Translate	200	--	--	2

The typical configuration example of VLAN conversion based on two Tag

The topology is shown below:



The topology of VLAN conversion based on two Tag

SwitchA Port2 and Port3 connect PC user that uses outer-layer VLAN100 and inner-layer10-30 and IP phone user that uses outer-layer VLAN200 and inner-layer VLAN50-60 respectively, SwitchB Port2 and Port3 uses PC server that uses outer-layer VLAN100 and inner-layer10-30 and IP phone server that uses outer-layer VLAN200 and inner-layer VLAN50-60. In carrier network VLAN1000 is used for PC user service, while VLAN2000 is used for IP phone service. By configuring VLAN conversion function based on two Tag on SwitchA and SwitchB, the communication between the server and PC/IP user can be realized, the configuration is as follows:

Switch configuration:

Raisecom#config

Raisecom(config)#**create vlan** 10-30,50-60,100,200,1000,2000 active

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

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

Raisecom(config-port)#**switchport trunk allowed vlan** 100,200,1000,2000

Raisecom(config-port)#**switchport vlan-mapping** ingress outer 1000 inner 10-30 translate outer 100

Raisecom(config-port)#**switchport vlan-mapping** ingress outer 2000 inner 50-60 translate outer 200

Raisecom(config-port)#**mac-address-table** vlan-copy from 1000 to 100

Raisecom(config-port)#**mac-address-table vlan-copy** *from 2000 to 200*

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

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

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

Raisecom(config-port)#**switchport vlan-mapping** *ingress outer 100 inner 10-30 translate outer 1000*

Raisecom(config-port)#**switchport trunk allowed vlan 100**

Raisecom(config-port)#**mac-address-table vlan-copy** *from 100 to 1000*

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

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

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

Raisecom(config-port)#**switchport vlan-mapping** *ingress outer 200 inner 50-60 translate outer 2000*

Raisecom(config-port)#**mac-address-table vlan-copy** *from 200 to 2000*

Raisecom(config-port)#switchport trunk allowed vlan 200

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

Raisecom(config)#**show interface port 1 vlan-mapping** *ingress translate*

Direction: Ingress

	<i>Original</i>	<i>Original</i>	<i>Outer-tag</i>	<i>New</i>	<i>Inner-tag</i>	<i>New</i>	
<i>Port</i>	<i>Inner VLANs</i>	<i>Outer VLANs</i>	<i>Mode</i>	<i>Outer-VID</i>	<i>Mode</i>	<i>Inner-VID</i>	<i>Hw-ID</i>

1	10-30	1000	Translate	100	--	--	1
1	50-60	2000	Translate	200	--	--	2

Raisecom(config)#**show interface port 2 vlan-mapping** *ingress translate*

Direction: Ingress

	<i>Original</i>	<i>Original</i>	<i>Outer-tag</i>	<i>New</i>	<i>Inner-tag</i>	<i>New</i>	
<i>Port</i>	<i>Inner VLANs</i>	<i>Outer VLANs</i>	<i>Mode</i>	<i>Outer-VID</i>	<i>Mode</i>	<i>Inner-VID</i>	<i>Hw-ID</i>

2	10-30	100	Translate	1000	--	--	3

Raisecom(config)#**show interface port 3 vlan-mapping** *ingress translate*

Direction: Ingress

	<i>Original</i>	<i>Original</i>	<i>Outer-tag</i>	<i>New</i>	<i>Inner-tag</i>	<i>New</i>	
<i>Port</i>	<i>Inner VLANs</i>	<i>Outer VLANs</i>	<i>Mode</i>	<i>Outer-VID</i>	<i>Mode</i>	<i>Inner-VID</i>	<i>Hw-ID</i>

3	50-60	200	Translate	2000	--	--	4

SwitchB is configured as below:

Raisecom#**config**

Raisecom(config)#**create vlan** 10-30,50-60,100,200,1000,2000 *active*

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

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

Raisecom(config-port)#**switchport trunk allowed vlan** 100,200,1000,2000

Raisecom(config-port)#**switchport vlan-mapping** *ingress* *outer* 1000 *inner* 10-30 *translate* *outer* 100

Raisecom(config-port)#**switchport vlan-mapping** *ingress* *outer* 2000 *inner* 50-60 *translate* *outer* 200

Raisecom(config-port)#**mac-address-table vlan-copy** *from* 1000 *to* 100

Raisecom(config-port)#**mac-address-table vlan-copy** *from* 2000 *to* 200

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

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

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

Raisecom(config-port)#**switchport vlan-mapping** *ingress* *outer* 100 *inner* 10-30 *translate* *outer* 1000

Raisecom(config-port)#**switchport trunk allowed vlan** 100

Raisecom(config-port)#**mac-address-table vlan-copy** *from* 100 *to* 1000

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

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

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

Raisecom(config-port)#**switchport vlan-mapping** *ingress* *outer* 200 *inner* 50-60 *translate* *outer* 2000

Raisecom(config-port)#**mac-address-table vlan-copy** *from* 200 *to* 2000

Raisecom(config-port)#**switchport trunk allowed vlan** 200

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

Raisecom(config)#**show interface port** 1 **vlan-mapping** *ingress* *translate*

Direction: Ingress

	<i>Original</i>	<i>Original</i>	<i>Outer-tag</i>	<i>New</i>	<i>Inner-tag</i>	<i>New</i>	
<i>Port</i>	<i>Inner VLANs</i>	<i>Outer VLANs</i>	<i>Mode</i>	<i>Outer-VID</i>	<i>Mode</i>	<i>Inner-VID</i>	<i>Hw-ID</i>
1	10-30	1000	Translate	100	--	--	1
1	50-60	2000	Transalte	200	--	--	2

Raisecom(config)#**show interface port** 2 **vlan-mapping** *ingress* *translate*

Direction: Ingress

	<i>Original</i>	<i>Original</i>	<i>Outer-tag</i>	<i>New</i>	<i>Inner-tag</i>	<i>New</i>	
<i>Port</i>	<i>Inner VLANs</i>	<i>Outer VLANs</i>	<i>Mode</i>	<i>Outer-VID</i>	<i>Mode</i>	<i>Inner-VID</i>	<i>Hw-ID</i>
2	10-30	100	Translate	1000	--	--	3

Raisecom(config)#**show interface port 3 vlan-mapping ingress translate**

Direction: Ingress

	<i>Original</i>	<i>Original</i>	<i>Outer-tag</i>	<i>New</i>	<i>Inner-tag</i>	<i>New</i>
<i>Port</i>	<i>Inner VLANs</i>	<i>Outer VLANs</i>	<i>Mode</i>	<i>Outer-VID</i>	<i>Mode</i>	<i>Inner-VID Hw-ID</i>

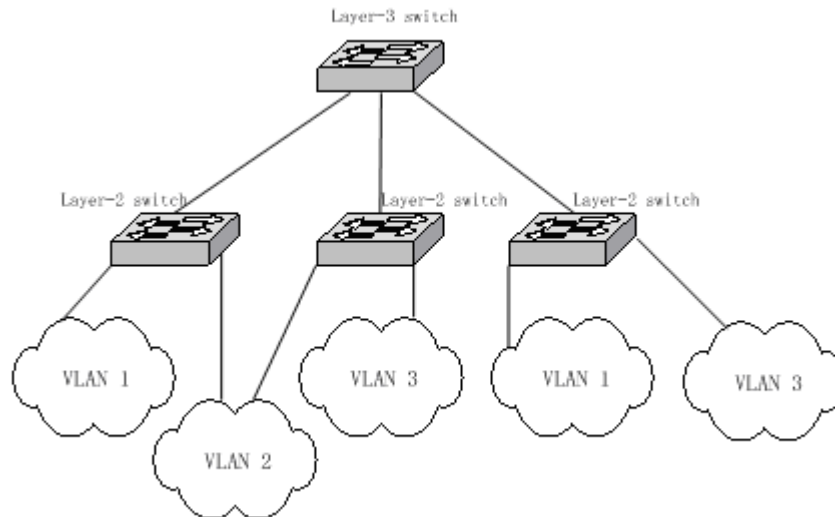
3	50-60	200	Translate	2000	--	-- 4

Chapter 10 VLAN Configuration Guide

10.1 VLAN Configuration Principles

10.1.1 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.

10.1.2 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.

10.1.3 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.

10.2 Switch VLAN Function Configuration

10.2.1 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.

VLAN port mode interview

Port 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 <i>allowed vlans</i>
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)

Default VLAN configuration

Function	Default value
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

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} (active suspend) priority {0-7}	Create VLAN and make sure the state: 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.

Use **no name** to delete VLAN name and recover to default name.

Note:

- 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 activated. 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.

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 valid	Configure VLAN priority Enter static VLAN mode
3	priority <0-7>	Configure the priority of VALN <0-7> VLAN priority
4	exit	Return to privileged EXEC mode
5	show vlan	Shown VLAN configuraion

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

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 port <i>portid</i>	Enter the corresponding physical port configuration mode <i>portid</i> : port number
3	switchport mode { <i>access</i> / <i>hybrid</i> [<i>double-tagging</i>] / <i>trunk</i> [<i>double-tagging</i>] / [<i>hybrid</i>] <i>dot1q-tunnel</i> }	Configure port VLAN mode access ACCESS mode, that is port exists in the unique VLAN in the form of UNTAG; 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)
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface port [<i>port-list</i>] 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 port <i>portid</i>	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 port [<i>port-list</i>] 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 port <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 port [[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.

When the user is configured the HYBRID mode 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.

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 port 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 port [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.

When the user is configured the HYBRID mode 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.

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 port 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 port [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.

Configure port protection

The configuration steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port 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 port protected** Show physical port protection attribute

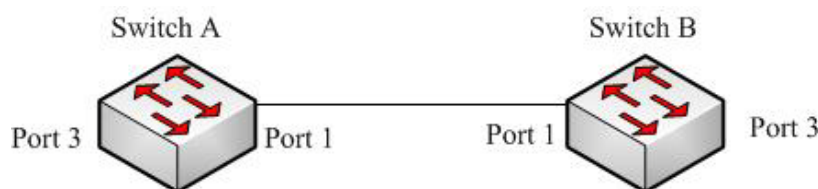
Use **no switchport protect** to cancel port protection configuration.

Monitoring and maintenance

Command	Description
show interface port [port-list] switchport	Show port VLAN attribute configuration
show interface port protected	Show physical port protection attribute
show vlan	Show port VLAN attribute configuration

Typical configuration example

The topology structure is shown below:



topology structure

As is shown in figure 1, the SwitchA and SwitchB use Port1(SwitchA) and Port1(SwitchB) to connect each other, configure Port1 of the two equipments to Trunk port, allow VLAN1-VLAN100 to pass, Port3(SwitchA) and Port3(SwitchB) 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 port 1
```

```
Raisecom(config-port)#switchport mode trunk
```

```
Raisecom(config-port)#switchport trunk allowed vlan 1-100
```

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

```
Raisecom(config)#interface port 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

<i>VLAN</i>	<i>Name</i>	<i>Status</i>	<i>VLAN-Priority</i>	<i>Ports</i>
---	-----	-----	-----	-----
1	Default	active	N/A	1,2,4-26
6	VLAN0006	active	0	3

Raisecom#**show interface port 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 port 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

10.2.2 Basic Q-IN-Q function

Default Q-IN-IN configuration

Function	Default value
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.

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; <i>HHHH</i> : hex outer layer Tag TPID value, it is 1~4 figures hex number, range is 0x0-0xFFFF.
3	interface port portid	Enter port mode
4	switchport mode {access trunk }	Configure port VLAN mode access ACCESS mode, port exists in the form of UNTAG in the only VLAN; trunk TRUNK mode, the port exists in several VLAN in TAG mode, and exists in Native Vlan in UNTAG mode;
4	switchport access vlan <1-4094>	Configure the port ACCESS VLAN ID. <i><1-4094></i> 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 port [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.

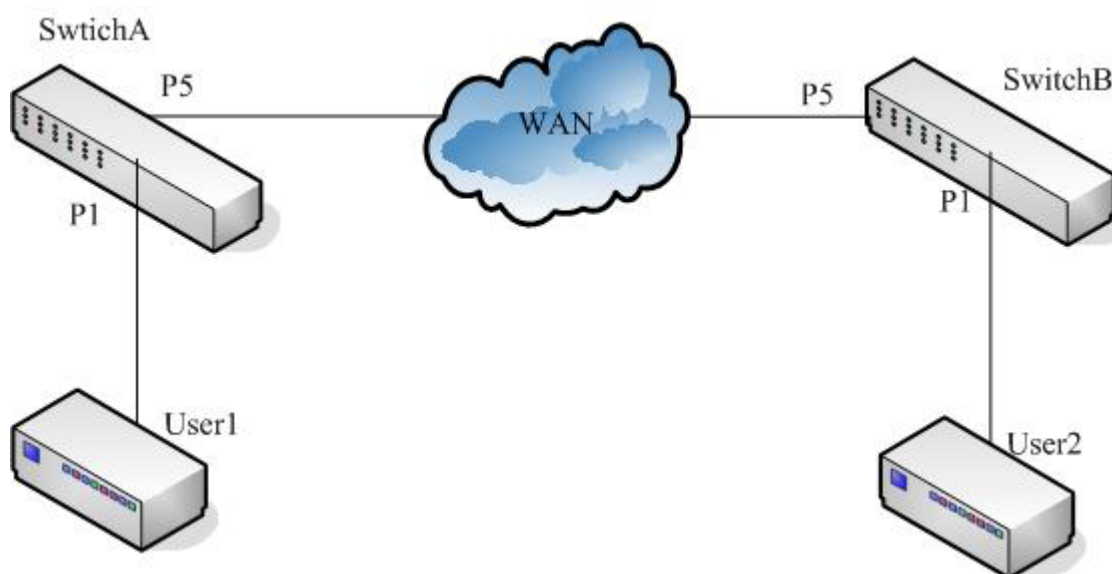
Use **no switchport access vlan** mode to restore Access VLAN to default value, that is, port Access VLAN is VLAN 1.

Monitoring and maintenance

Command	Command parameter instruction
show vlan [{1-4094}]	Show stable VLAN configuration
show interface port [port-list] switchport	Show port VLAN attribute configuration

Typical configuration example

The topology structure is shown in figure below:



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, SwitchB use P5 to connect to MAN. P1 connect to User2. MAN TPID is 0x8600. Configure SwitchA and SwitchB to realize QinQ function.

SwitchA configuration is shown below:

```
Raisecom#config
```

```
Raisecom(config)#mls double-tagging tpid 8600
```

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

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

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

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

```
Raisecom(config)#interface port 5
```

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

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

```
Raisecom(config)#exit
```


Raisecom#show interface port 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 port 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 port 1****Raisecom(config-port)#switchport mode dot1q-tunnel**

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

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

Raisecom(config)#**interface port 5**

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

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

Raisecom(config)#**exit**

Raisecom#**show interface port 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 port 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

10.2.3 Flexible Q-IN-Q function

Default flexible Q-IN-Q configuration

Function	Default value
Configure port flexible Q-IN-Q VLAN mapping relationship	None

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 port <i>portid</i>	Enter corresponding physical port configuration mode
3	switchport vlan mapping <i>vlan-list add-outer</i> <i>outer-vlan-list</i>	Configure the VLAN mapping relationship of port flexible Q-in-Q <i>vlan-list</i> inner: layer VLAN ID from client network <i>outer-vlan-list</i> : 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 port [<i>port-list</i>] 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.

Note:

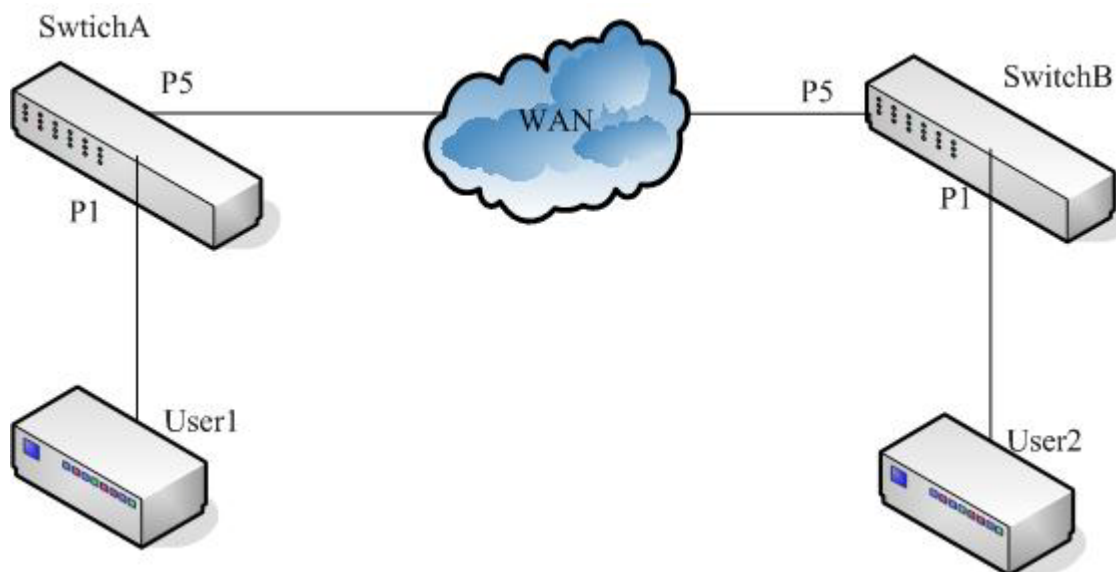
- To ISCOM2924GF/2926, 768 VLAN mapping can be configured at the most.
- The VLAN mapping relationship of flexible Q-in-Q function configure by this command takes effect only on TUNNEL port, that is, only when the interface mode is TUNNEL, can flexible Q-in-Q function takes effect. The port enters command 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.

Monitoring and maintenance

Command	Command parameter instruction
show interface port [<i>port-list</i>] switchport	Show port VLAN attribute configuration

Typical configuration example

The topology structure is shown below:



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, SwitchB 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 realize flexible Q-in-Q function.

SwitchA configure is shown below:

```
Raisecom#config
```

```
Raisecom(config)#mls double-tagging tpid 8600
```

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

SwitchB configuration is shown below:

Raisecom#config**Raisecom(config)#mls double-tagging tpid 8600****Raisecom(config)#interface port 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 port 5**

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

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

Raisecom(config)#**exit**

Raisecom#**show vlan mapping**

<i>Port</i>	<i>Inner VLAN</i>	<i>Outer VLAN</i>	<i>Hardware</i>

<i>1</i>	<i>20</i>	<i>200</i>	<i>Yes</i>

Raisecom#**show interface port 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 port 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

10.3 VLAN Function Configuration

10.3.1 VLAN Configuration

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.

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

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

Note:

- 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:
- 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.

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>	Create VLAN <2-4094>: VLAN ID.
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:

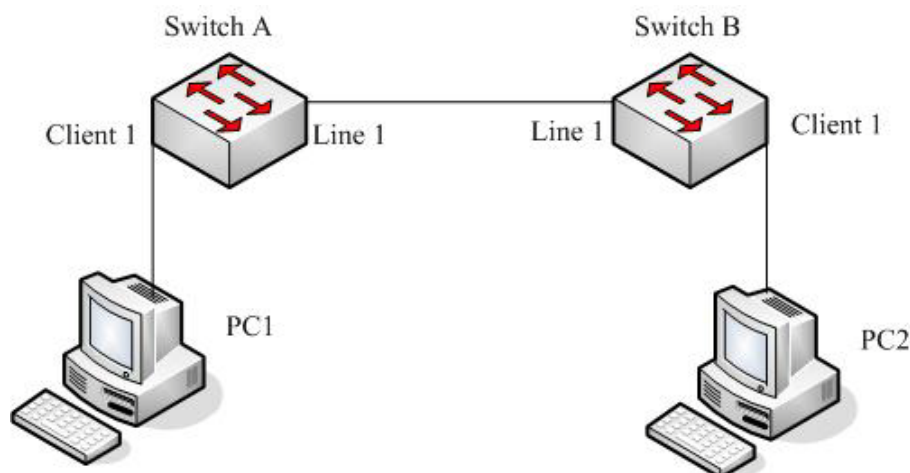
Step	Command	Description
1	config	Enter global configuration mode
2	no vlan {all <2-4094>}	Delete VLAN <2-4094>: VLAN ID; All: all the stable VLAN except default VLAN (VLAN ID is 1)
3	exit	Return to global configuration mode
4	show vlan	Show VLAN configuration

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

Typical configuration example

Topology structure is shown as figure below:



Topology structure

As is shown in figure 5, Line1 of SwitchB connects with Line1 of SwitchA, 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

<i>VLAN</i>	<i>Ports</i>	<i>Untag Ports</i>	<i>Priority</i>
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

10.3.2 Basic Q-in-Q function

Basic Q-in-Q default configuration

Function	Default value
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

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 { <i>transparent/</i> <i>dot1q-vlan/double-tagged-vlan</i> }	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 <i>HHHH</i>	Configure outer layer Tag TPID value to HHHH <i>HHHH:</i> hex outer layer Tag TPID value, which is 1~4 figures hex number, range is 0x0-0xFFFF
4	exit	Return to privileged EXEC mode
5	show vlan	Show stable VLAN configuration
6	show interface { client <i>client-list</i> line <i>line-list</i> } switchport	Show VLAN configuration

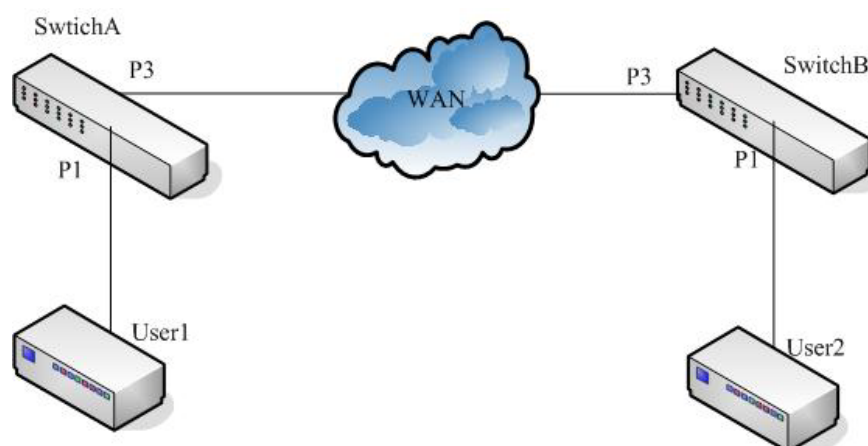
Use **no mls double-tagging tpid HHHH** to restore outer layer Tag TPID to default value, 0x9100.

Monitoring and maintenance

Command	Description
show vlan [{ <i>1-4094</i> }]	Show stable VLAN configuration
show interface client [<i>client-list</i>] switchport	Show user port VLAN configuration
show interface line [<i>line-list</i>] switchport	Show line port VLAN configuration

Typical configuration example

Topology structure:



Topology structure

As is shown in the topology structure, SwitchA and SwitchB 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

<i>VLAN</i>	<i>Ports</i>	<i>Untag Ports</i>	<i>Priority</i>

<i>1</i>	<i>L:1;C:1-4</i>	<i>L:1;C:1-4</i>	<i>--</i>
<i>3</i>	<i>C:3</i>	<i>n/a</i>	<i>--</i>
<i>5</i>	<i>L:1</i>	<i>n/a</i>	<i>--</i>

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

10.4 VLAN Function Configuration

10.4.1 VLAN based on port

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.

VLAN 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

Default VLAN configuration

Function	Default value
Device switch mode	transparent
Create static VLAN	Default VLAN and cluster VLAN exist in the system, which 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

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

Note: 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.

Configure 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.

The command of **no name** can restore it to the default name.

Note:

- 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 3 is '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.

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 <i>valid</i>	Configure VLAN priority Enter static VLAN mode
3	priority <0-7>	Configure the priority of VALN <0-7> VLAN priority
4	exit	Return to privileged EXEC mode
5	show vlan	Shown VLAN configuraion

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

Configure 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 port <i>portid</i>	Enter corresponding physical interface configuration mode
3	switchport mode {<i>access</i> / <i>trunk</i>}	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 <i>vlan-list</i> add <i>add-vlan-list</i> remove <i>remove-vlan-list</i> }	Configure the VLAN that Access port allows to pass All , all the VLAN are allowed to pass; <i>Vlan-list</i> , VLAN that is allowed to pass, the existed configuration will be covered directly Add <i>add-vlan-list</i> , add allowed VLAN on the base of existed allowed VLAN Remove <i>remove-vlan-list</i> , 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 <i>vlan-list</i> add <i>add-vlan-list</i> remove <i>remove-vlan-list</i> }	Configure the VLAN that is allowed to pass Trunk port All allow all the VLAN to pass <i>Vlan-list</i> , allow the passed VLAN ,cover the existed configuration directly; Add <i>add-vlan-list</i> , add allowed VLAN on the base of the existed allowed VLAN Remote <i>remote-vlan-list</i> , delete allowed VLAN

		on the base of the existed allowed VLAN
8	switchport trunk untagged vlan { all <i>vlan-list</i> add <i>add-vlan-list</i> remove <i>remove-vlan-list</i> }	Configure the Untagged VLAN that is allowed to pass Trunk port, All , all the VLAN are allowed to pass; <i>Vlan-list</i> , 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 port [<i>port-list</i>] 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.

Note:

- 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.

Configure port protection

The steps are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>portid</i>	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 port protected	Show physical port protection attribution

Use **no switchport protection** to cancel port protection configuration.

Configure 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 port <i>portid</i>	Enter port mode
3	switchport forwarding allowed portlist <i>port-list</i>	Configure port forwarding list
4	exit	Quit from port mode
5	exit	Quit from global mode
6	show interface port [<i>port-list</i>] 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.

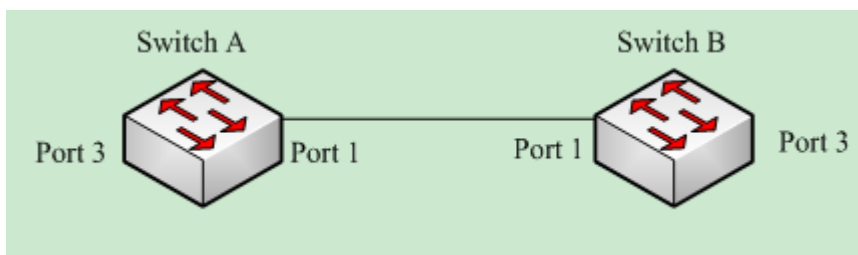
Monitoring and maintenance

Command	Description
show interface port [<i>port-list</i>] 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 port protected	Show the protected port attribution of the physical port
show vlan	Show port VLAN attribution

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 port 1
```

```
Raisecom(config-port)#switchport mode trunk
```

```
Raisecom(conifg-port)#switchport trunk allowed vlan 1-100
```

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

```
Raisecom(config)#interface port 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 port 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 port 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 11 ACL Function Configuration

11.1 Configuration Description

This chapter is suit to configuration ACL function on the following devices: ISCOM2812f/2826/2826e/2828f/2852, ISCOM2926/2924gf, ISCOM3012f/3026/3026e/3028f/3052, ISCOM2250.

11.2 ACL Introduction

In order to filter packets, network equipment needs to set a series of matching rules to identify the filtered objects. Only after this, user can allow or prohibit relative packets to pass through according to the designated strategy in advance. ACL (Access Control list) is used to realize these operations. ACL can be applied to VLAN, Layer-2 physical port and Layer-3 management interface. ACL makes classification to packets according to a series of matching conditions; these conditions can be packet source address, destination address and port number etc. It is combined with a series of judgment sentences. After activating a ACL, switch will check each received packet according to the judgment conditions, packets will be forwarded or dropped then according to these conditions. User can specify *permit* or *deny* while configuring ACLs. When it is set as *deny*, packets that are in accord with the rules will be dropped, the others will be forwarded; when it is set as *permit*, packets that are in accord with the rules will be forwarded, the others will be dropped.

11.3 IPACL Configuration

Switch supports 400 IP access control lists at most with corresponding series number 0~399. It specifies classification rules according to the source IP address, destination IP address in the IP packet header, used TCP or UDP protocol port number and etc. packet attributes information, and then processes related operations to the packets according these rules. The construction of IP packet header can be referred to RFC791 and other related documents.

11.3.1 IPACL Default Configuration

N/A

11.3.2 IPACL Configuration

Steps	Command	Description
1	config	Entry into global configuration mode
2	ip-access-list <i>list-number</i> { <i>deny</i> / <i>permit</i> } <i>protocol</i> [<i>source-address mask</i> any] [<i>source-protocol-port</i>] [<i>destination-address mask</i>]	ip-access-list configuration IP address access control list <i>list-number</i> IP address access control listserial number, range from 0-399

	any } [<i>destination-protocol-port</i>]	deny permit represents reject/accept access. <i>protocol</i> binding protocol type. <i>source-address mask</i> any is source IP address with its mask, format is dotted decimal in the form of A.B.C.D, any indicates arbitrary address. <i>source-protocol-port</i> is source port for TCP/UDP protocol <i>destination -address mask</i> any is the destination address and its mask, the format is dotted decimal as A.B.C.D; any indicates arbitrary address. <i>destination -protocol-port</i> is the destination port of TCP/UDP.
3	exit	Exit global configuration mode and enter privileged EXEC mode
4	show ip-access-list <i>list-number</i>	Show IP access control list relevant information <i>list-number</i> is the series number for the IP access control list to be shown, rang is 0-399.
5	No ip-access-list <i>list-number</i>	Delete IP access control list <i>list-number</i> : the list series number to be deleted

11.3.3 Monitoring and Maintenance

Check and display indicated IP ACL command:

Command	Description
show ip-access-list [{0-399}]	Show IP Access Control List

11.3.4 Specific Configuration Example

➤ Destination

Configure source IP address as 192.168.1.0 segment, destination IP address as random address , protocol type as IP and access type as deny IP access rule;

Configure source IP address is 10.168.1.19; mask is 255.255.255.255; source protocol port is 80; destination address is random port; protocol type is TCP; visit type is deny IP access rule.

Configure source IP address is 10.168.1.19; mask is 255.255.255.255; destination address is 10.168.0.0 segment; protocol type is TCP; access type is permit's IP access rule.

➤ Set up Steps

Raisecom#**config**

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

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

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

```
Raisecom(config)#exit
```

```
Raisecom#show ip-access-list
```

Src Ip: Source Ip Address

Dest Ip: Destination Ip Address

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

11.4 MAC ACL Function

Switch supports 400 digital-identified Layer-2 (MAC) access control lists at most with corresponding series number 0~399. Layer-2 access control list in conjunction with filter can process relevant operations to packets according to the source MAC address carried in Layer-2 frame, destination MAC address, source VLAN ID, Layer-2 protocol types and other Layer-2 information rules.

11.4.1 MAC ACL Default Configuration

11.4.2 MAC ACL Configuration

Steps	Command	Description
1	config	Entry into global configuration mode
2	mac-access-list <i>list-number</i> { deny permit } [<i>protocol</i> / any] { <i>source-MAC-address</i> any } { <i>destination-MAC-address</i> / any }	MAC access control list configuration <i>list-number</i> access control list series number, range 0-399. <i>deny/permit</i> indicates deny/permit access [<i>protocol</i> any] indicates bonded protocol type, any indicates unrestricted protocol type. <i>source-MAC-address</i> indicates the source MAC address to be configured, format is hexadecimal string as "HHHH.HHHH.HHHH", dotted every 4 characters; any indicates arbitrary source MAC address. <i>destination-MAC-address</i> is the destination MAC address to be configured, format is hexadecimal string as "HHHH.HHHH.HHHH", dotted every 4 characters; any indicates arbitrary destination MAC address.
3	exit	Exit global configuration mode and enter privileged EXEC mode
4	show mac-access-list <i>list-number</i>	Show MAC access control list <i>list-number</i> is the series number for the MAC access control list to be shown, rang is 0-399.
5	no mac-access-list <i>list-number</i>	Delete configured MAC access control list <i>list-number</i> is the list series number to be deleted

11.4.3 Monitoring and Maintenance

Check and display indicated MAC ACL command:

Command	Description
show mac-access-list <i>[[0-399]]</i>	Display MAC access control list

11.4.4 Specific Configuration Examples

➤ Destination

Configure source MAC address as 1234.1234.1234; destination MAC address as 5678.5678.5678; protocol as IP; access type as deny's MAC access rule;

Configuration source MAC address as 1111.2222.3333; destination MAC address as 4444.5555.6666; protocol as ARP; access type as permit's MAC access rule.

➤ Set up Steps

Raisecom#**config**

Raisecom#**config**

Raisecom(config)# **mac-access-list 0 deny ip 1234.1234.1234 5678.5678.5678**

Raisecom(config)# **mac-access-list 1 permit arp 1111.2222.3333 4444.5555.6666**

Raisecom(config)#**exit**

Raisecom#**show mac-access-list**

Src Mac: Source MAC Address

Dest Mac: Destination MAC Address

List	Access	Protocol	Ref.	Src Mac	Dest Mac
0	deny	ip	0	1234.1234.1234	5678.5678.5678
1	permit	arp	0	1111.2222.3333	4444.5555.6666

11.5 MAPACL Function

Switch supports 400 digital-identified access list maps at most with corresponding series number 0~399. Access list map can define more protocols and more detailed protocol character fields than IP access list and MAC access list, also can implement matching to any bytes in the first 64 bytes of Layer-2 frame according to user's definition before corresponding processing to the data packets from matched results. User needs to be familiar with Layer-2 data frame before using user-defined access list map.

Access list map uses command *match* to set the expected matching character field, no conflicts can exist in the same access list map when setting matching character field. Character fields that can be matched are shown below:

- Mac destination address
- Mac source address
- Ethernet protocol type

- CoS
- ARP protocol type
- Hardware address of ARP protocol sender
- Hardware address of ARP protocol receiver
- IP address of ARP protocol sender
- IP address of ARP protocol receiver
- IP protocol destination address
- IP protocol source address
- IP protocol priority
- IP protocol ToS
- IP protocol dscp
- IP protocol segmentation bit
- IP protocol type
- TCP protocol destination port
- TCP protocol source port
- TCP protocol bit
- UDP protocol destination port
- UDP protocol source port
- ICMP protocol information type
- ICMP protocol information code
- IGMP protocol information type

User can also use regular mask and offset to define any byte in the first 64 bytes in data frame, and then compare them with the user-defined rules to obtain the matched data frame, after this user can implement relevant operations. User-defined rules can be certain data fixed attributes, such as that in order to obtain all the TCP packets, user can define the rules as “06”, mask as “FF”, offset as “27”, by using such a method, regular rules and offsets can work together to pick up the segment of TCP protocol number in data frame, then compare it with defined rules to obtain all matched TCP packets.

Attention: Rules should be even hexadecimal, offset includes segment of 802.1Q VLAN TAG even if what the switch receives is untagged packet.

11.5.1 MAPACL Default Configuration

11.5.2 MAPACL Configuration

Steps	Command	Description
1	config	Entry into global configuration mode
2	access-list-map <i>list-number</i> { deny permit }	<i>list-number</i> : list serial number, from 0-399 <i>deny</i> / <i>permit</i> deny or permit data packets to go through when matching.
3	match mac { destination source } <i>HHHH.HHHH.HHHH</i>	<i>destination</i> / <i>source</i> match source mac or destination mac <i>HHHH.HHHH.HHHH</i> mac address
4	match cos <0-7>	<0-7> match cos value
5	match ethertype <i>HHHH</i> [<i>HHHH</i>]	<i>HHHH</i> [<i>HHHH</i>] match Ethernet type [mask]
6	match { <i>arp</i> <i>eapol</i> <i>flowcontrol</i> <i>ip</i> <i>ipv6</i> <i>loopback</i> <i>mpls</i> <i>mpls-mcast</i> <i>pppoe</i> <i>pppoedisc</i> <i>x25</i> <i>x75</i> }	<i>arp</i> : match ARP protocol <i>eapol</i> : match eapol protocol <i>flowcontrol</i> : match flow control protocol <i>ip</i> : match ip protocol <i>ipv6</i> : match ipv6 protocol <i>loopback</i> : match loopback protocol <i>mpls</i> : matchmpls single cast protocol <i>mpls-mcast</i> : matchmpls group cast protocol <i>pppoe</i> : match pppoe protocol

		<i>pppoedisc</i> : match pppoe discover protocol
		<i>x25</i> : match x25 protocol
		<i>x75</i> : match x75 protocol
7	no match mac { <i>destination</i> / <i>source</i> }	Do not match MAC address
		<i>destination</i> / <i>source</i> : match source mac or destination mac
8	no match cos	Do not match CoS value
9	no match ethertype	Do not match Ethernet type
10	match arp opcode { <i>request</i> / <i>reply</i> }	Match arp protocol type
		<i>request</i> / <i>reply</i> arpprotocol reply /request packet
11	match arp { <i>sender-mac</i> / <i>target-mac</i> } <i>HHHH.HHHH.HHHH</i>	Match arp protocol hardware address
		<i>sender-mac</i> / <i>target-mac</i> : match arp sender/target mac address
		<i>HHHH.HHHH.HHHH</i> : MAC address
12	match arp { <i>sender-ip</i> / <i>target-ip</i> } <i>A.B.C.D</i> [<i>A.B.C.D</i>]	Match arp protocol IP address
		<i>sender-ip</i> / <i>target-ip</i> sender/target: IPaddress
		<i>A.B.C.D</i> [<i>A.B.C.D</i>]: Ip address [mask]
13	no match arp opcode	do not match arpprotocoltype
14	no match arp { <i>sender-mac</i> / <i>target-mac</i> }	do not match arp protocol hardware address
15	no match arp { <i>sender-ip</i> / <i>target-ip</i> }	do not match arpprotocolIPaddress
		<i>sender-ip</i> / <i>target-ip</i> sender/target IP address
16	match ip { <i>destination-address</i> / <i>source-address</i> } <i>A.B.C.D</i> [<i>A.B.C.D</i>]	Match IP protocol address
		<i>destination-address</i> / <i>source-address</i> Ip protocol destination/source address
		<i>A.B.C.D</i> [<i>A.B.C.D</i>] IP address [mask]
17	match ip precedence {<0-7>/ <i>routine</i> / <i>priority</i> / <i>immediate</i> / <i>flash</i> / <i>flash-override</i> / <i>critical</i> / <i>internet</i> / <i>network</i> }	Match IP priority
		<0-7>: IP priority value
		<i>routine</i> : IP priority value 0
		<i>priority</i> : IP priority value 1
		<i>immediate</i> : IP priority value 2
		<i>flash</i> : IP priority value 3
		<i>flash-override</i> : IP priority value 4
		<i>critical</i> : IP priority value 5
		<i>internet</i> : IP priority value 6
		<i>network</i> : IP priority value 7
18	match ip ToS {<0-15> / <i>normal</i> / <i>min-monetary-cost</i> / <i>min-delay</i> / <i>max-reliability</i> / <i>max-throughput</i> }	Match IP priority ToS value
		<0-15>: ToS value
		<i>normal</i> : normal ToS value (0)
		<i>min-monetary-cost</i> : Min monetary cost ToS value(1)
		<i>min-delay</i> : Min delay ToS value(8)
		<i>max-reliability</i> : Max reliability ToS value(2)
		<i>max-throughput</i> : Max throughput ToS value(4)
19	match ip dscp {<0-63> / <i>af11</i> / <i>af12</i> / <i>af13</i> / <i>af21</i> / <i>af22</i> / <i>af23</i> / <i>af31</i> / <i>af32</i> / <i>af33</i> / <i>af41</i> / <i>af42</i> / <i>af43</i> / <i>cs1</i> / <i>cs2</i> / <i>cs3</i> / <i>cs4</i> / <i>cs5</i> / <i>cs6</i> / <i>cs7</i> / <i>ef</i> / <i>default</i> }	Match IP DSCP value
		<0-63>: IP DSCP value
		<i>af11</i> : AF11 DSCP value(001010)
		<i>af12</i> : AF12 DSCP value(001100)
		<i>af13</i> : AF13 DSCP value(001110)
		<i>af21</i> : AF21 DSCP value(010010)
		<i>af22</i> : AF22 DSCP value(010100)
		<i>af23</i> : AF23 DSCP value(010110)
		<i>af31</i> : AF31 DSCP value(011010)
		<i>af32</i> : AF32 DSCP value(011100)
		<i>af33</i> : AF33 DSCP value(011110)
		<i>af41</i> : AF41 DSCP value(100010)
		<i>af42</i> : AF42 DSCP value(100100)

		<i>af43</i> : AF43 DSCP value(100110)
		<i>cs1</i> : CS1(priority 1) DSCP value(001000)
		<i>cs2</i> : CS2(priority 2) DSCP value(010000)
		<i>cs3</i> : CS3(priority 3) DSCP value(011000)
		<i>cs4</i> : CS4(priority 4) DSCP value(100000)
		<i>cs5</i> : CS5(priority 5) DSCP value(101000)
		<i>cs6</i> : CS6(priority 6) DSCP value(110000)
		<i>cs7</i> : CS7(priority 7) DSCP value(111000)
		default: Default DSCP value(000000)
		<i>ef</i> : EF DSCP value(101110)
20	match ip no-fragments	Match no-fragment IP packet
21	match ip protocol <0-255>	Match IP protocol value <0-255>: IP protocol type value
22	match ip { ahp /esp/gre/icmp/igmp/igrp /ipinip/ospf/pcp/pim/tcp/udp}	Match IP protocol value <i>ahp</i> : authorize header protocol <i>esp</i> : encapsulation security payload protocol <i>gre</i> : General routing encapsulation protocol <i>icmp</i> : Internet control message protocol <i>igmp</i> : Internet group message protocol <i>igrp</i> : Interior gateway routing protocol <i>ipinip</i> : IP-in-IP tunnel <i>ospf</i> : Open shortest path first <i>pcp</i> : Payload compression protocol <i>pim</i> : protocol independent multicast protocol <i>tcp</i> : Transmission control protocol <i>udp</i> : user datagram protocol
23	no match ip {destination-address / source-address}	Do not match IP protocol address <i>destination-address / source-address</i> : IP protocol destination/source address
24	no match ip precedence	do not match IP priority
25	no match ip ToS	do not match IP ToS value
26	no match ip dscp	do not match IP DSCP value
27	no match ip no-fragments	do not match IP no-fragment
28	no match ip protocol	do not match IP protocol value
29	match ip tcp { destination-port / source-port} {<0-65535> bgp / domain echo exec finger ftp / ftp-data gopher hostname ident / irc klogin kshell login lpd nntp / pim-auto-rp pop2 pop3 smtp / sunrpc syslog tacacs talk telnet / time uucp whois www}	Match Tcp protocol port number <i>destination-port / source-port</i> : TCP protocol destination/source port <0-65535>: tcp port number <i>bgp</i> : border gateway protocol (179) <i>domain</i> : domain name service protocol (53) <i>echo</i> : echo protocol (7) <i>exec</i> : Exec (rsh, 512) <i>finger</i> : Finger (79) <i>ftp</i> : File transfer protocol (21) <i>ftp-data</i> : FTP data connections (20) <i>gopher</i> : Gopher (70) <i>hostname</i> : NIC hostname server (101) <i>ident</i> : identify protocol (113) <i>irc</i> : Internet Relay Chat protocol (194) <i>klogin</i> : Kerberos login (543) <i>kshell</i> : Kerberos shell (544) <i>login</i> : Login (rlogin, 513) <i>lpd</i> : Printer Service protocol(515) <i>nntp</i> : network news transport protocol <i>pim-auto-rp</i> : PIM Auto-RP (496) <i>pop2</i> : post office protocol v2 (109)

		<i>pop3</i> : post office protocol v3 (110) <i>smtp</i> : simple mail transport protocol (25) <i>sunrpc</i> : Sun Remote Procedure Call (111) <i>syslog</i> : System log (514) <i>tacacs</i> : TAC access control system (49) <i>talk</i> : Talk (517) <i>telnet</i> : Telnet (23) <i>time</i> : Time (37) <i>uucp</i> : Unix-to-Unix Copy program (540) <i>whois</i> : Nicname(43) <i>www</i> : World Wide Web (HTTP, 80)
30	match ip tcp { <i>ack</i> / <i>fin</i> / <i>psh</i> / <i>rst</i> / <i>syn</i> / <i>urg</i> }	Match TCP protocol bit <i>ack</i> : match ACK bit <i>fin</i> : matchFIN bit <i>psh</i> : matchPSH bit <i>rst</i> : matchRST bit <i>syn</i> : matchSYN bit <i>urg</i> : matchURG bit
31	no match ip tcp { <i>destination-port</i> / <i>source-port</i> }	do not match Tcp protocol port number <i>destination-port</i> / <i>source-port</i> : TCP protocol destination/source port
32	no match ip tcp { <i>ack</i> / <i>fin</i> / <i>psh</i> / <i>rst</i> / <i>syn</i> / <i>urg</i> }	do not match TCP protocol bit <i>ack</i> : match ACK bit <i>fin</i> : match FIN bit <i>psh</i> : match PSH bit <i>rst</i> : match RST bit <i>syn</i> : match SYN bit <i>urg</i> : match URG bit
33	match ip udp { <i>destination-port</i> / <i>source-port</i> } { <0-65535> / <i>biff</i> / <i>bootpc</i> / <i>bootps</i> / <i>domain</i> / <i>echo</i> / <i>mobile-ip</i> / <i>netbios-dgm</i> / <i>netbios-ns</i> / <i>netbios-ss</i> / <i>ntp</i> / <i>pim-auto-rp</i> / <i>rip</i> / <i>snmp</i> / <i>snmptrap</i> / <i>sunrpc</i> / <i>syslog</i> / <i>tacacs</i> / <i>talk</i> / <i>tftp</i> / <i>time</i> / <i>who</i> }	Match udp protocol port number <i>destination-port</i> / <i>source-port</i> : TCP protocol destination/source port <0-65535>: udp port number <i>biff</i> : Biff (mail notification, comsat, 512) <i>bootpc</i> : bootstrap protocol (BOOTP) client (68) <i>bootps</i> : bootstrap protocol(BOOTP) server (67) <i>domain</i> : domain name service protocol (53) <i>echo</i> : echo protocol (7) <i>mobile-ip</i> : mobile IP registration (434) <i>netbios-dgm</i> : NetBios datagram eservic (138) <i>netbios-ns</i> : NetBios name service (137) <i>netbios-ss</i> : NetBios session service (139) <i>ntp</i> : network time protocol(123) <i>pim-auto-rp</i> : PIM Auto-RP (496) <i>rip</i> : routing information protocol(520) <i>snmp</i> : simple network magagement protocol(161) <i>snmptrap</i> : SNMP Traps (162) <i>sunrpc</i> : Sun remote procedure call (111) <i>syslog</i> : system log (514) <i>tacacs</i> : TAC access control system (49) <i>talk</i> : talk (517) <i>tftp</i> : trivial file transfer protocol(69) <i>time</i> : Time (37) <i>who</i> : Who service (rwho, 513)
34	no match ip udp { <i>destination-port</i> / <i>source-port</i> }	do not match udp protocol port number <i>destination-port</i> / <i>source-port</i> : TCP protocol destination/sourceport
35	match ip icmp <0-255> [<i><0-255></i>]	Match icmp protocol information type

		<0-255> [<i><0-255></i>]:	information type[information code]
36	match ip igmp {<0-255> <i>dvmrp</i> / <i>query</i> / <i>leave-v2</i> / <i>report-v1</i> / <i>report-v2</i> / <i>report-v3</i> / <i>pim-v1</i> }		Match igmp protocol information type <0-255>: IGMP information type <i>dvmrp</i> : Distance Vector Multicast Routing Protocol <i>leave-v2</i> : IGMPv2 leave group <i>pim-v1</i> : protocol Independent Multicast version 1 <i>query</i> : IGMP member query <i>report-v1</i> : IGMPv1 member report <i>report-v2</i> : IGMPv2 member report <i>report-v3</i> : IGMPv3 member report
37	match user-define <i>rule-string</i> <i>rule-mask</i> <0-64>		Match user-defined segment <i>rule-string</i> : user-defined regular string, must be combined of hexadecimal, no more than 64 bytes. <i>rule-mask</i> : mask rule, used to implement “or” operation with data packet <0-64>: offset, based on dataframe header, and implement “or” operation from the beginning of specified bytes
38	no match user-define		do not match user-defined segment
39	exit		Exit global configuration mode and enter privileged EXEC mode
40	show access-list-map [<i>list-number</i>]		Show port <i>access-list-map</i> <i>list-number</i> is the port access-list-map series number to show, range is 0-399
41	no access-list-map <i>list-number</i>		Delete user-defined access-list-map <i>list-number</i> is the list number to delete

11.5.3 Monitoring and Maintenance

Check and display indicated access control list command:

Command	Description
show access-list-map [<i>{0-399}</i>]	Display access control list map list

11.5.4 Specific Configuration Example

➤ Destination

To filter bytes 123456 from the 40th bytes in the data frame, access type is “deny”. ARP protocol request packet is filtered.

➤ Set up Steps

Raisecom#**config**

Raisecom(config)#**access-list-map** 0 **deny**

Raisecom(config-aclmap)#**match user-define** 123456 ffffff 40

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

Raisecom(config)#**access-list-map** 1 **permit**

```
Raisecom(config-aclmap)# match arp opcode request
```

```
Raisecom(config-aclmap)#exit
```

```
Raisecom(config)#exit
```

```
Raisecom#show access-list-map
```

```
access-list-map 0 deny
```

```
Match user-define 123456 ffffff 40
```

```
access-list-map 1 permit
```

```
Match arp Opcode request
```

11.6 Application Configuration Based on Hardware ACL

3 steps for using ACL on Layer-2 physical port or VLAN are as follows::

1. Define ACL

Described in section 1.4.

2. Configuration Filter

After setting up ACL, you need to set the filter. Whether the filter is configured successfully depends on if the global status is enabled or not. You can use specific commands to make ACLs effective or to delete the filters that are already take effects. You can user command **no filter** to disable the related rules, if rules have been written in hardware, they will be deleted from the hardware and configurations.

In a physical port or VLAN filter rule can be composed by multi “permit/deny” statements and every statement indicated different size range of data packet. There is a problem of match order while a data packet and access control rule are matching. The match order of access control rule depends on configuration filter rule’s order. The later the order, the higher the priority. If there is conflicts in the rules, high priority will be followed.

There are four kinds of configurations: one is based on switch, one is based on port, on is based from ingress port to egress port, one is based on VLAN. For the filtering rules based on port, you have two options, one of which is based on flow ingress with the other one based on flow egress.

3. Simulate Filter

Use filter command to make the access control rule effect or no effect. Default status is no effect. Once command is configured as effect, not only the earlier configuration filter rules will be effect, but also the later configuration filter rule will effect as well.

11.6.1 Application Default Configuration Based on Hardware ACL

11.6.2 Application Configuration Based on Hardware ACL

1. Application based on switch

Steps	Command	Description
1	config	Entry into global configuration mode

2	[no] filter (<i>ip-access-list / mac-access-list / access-list-map</i>) { <i>acllist / all</i> }	Set filter based on switch ip-access-list indicates that the filter uses IP access list mac-access-list indicates that the filter uses MAC access list access-list-map indicates that the filter uses user-defined access list map <i>acllist</i> / all access control list series number, all means all the configured access control lists
3	filter (<i>enable / disable</i>)	enable : filter function effect enable disable : filter function effect disable
4	exit	Exit global configuration mode and enter privileged EXEC mode
5	show filter	Show all filter status

2. Application based on port

Steps	Command	Description
1	config	Entry into global configuration mode
2	[no] filter (ip-access-list mac-access-list access-list-map) { <i>acllist / all</i> } { ingress / egress } port-list { <i>portlist</i> }	Set filter based on port ip-access-list indicates that the filter uses IP access list mac-access-list indicates that the filter uses MAC access list access-list-map indicates that the filter uses user-defined access list map acllist all access control list series number, all means all the configured access control lists ingress egress means to carry out the filtering on ingress egress port-list the filter is applied to port portlist Physical port list range
3	filter (<i>enable / disable</i>)	enable filter function effect enable disable filter function effect disable
4	exit	Exit global configuration mode and enter privileged EXEC mode
5	show filter	Show all filter status

3. Based from ingress port to egress port

Steps	Command	Description
1	config	Entry into global configuration mode
2	[no] filter (ip-access-list mac-access-list access-list-map) { <i>all/ acllist</i> } from ingress-port to egress-port	Set the filter based from ingress port to egress port ip-access-list indicates that the filter uses IP access list mac-access-list indicates that the filter uses MAC access list access-list-map indicates that the filter uses user-defined access list map <i>acllist</i> all access control list series number, all means all the configured access control lists

		from to directions
		ingress-port : ingress port
		egress-port : egress port
3	filter (enable disable)	enable : filter function effect enable disable : filter function effect disable
4	exit	Exit global configuration mode and enter privileged EXEC mode
5	show filter	Show all filter status

4. Application based on VLAN

Steps	Command	Description
1	config	Entry into global configuration mode
2	[no] filter (ip-access-list mac-access-list access-list-map) {all/ acllist} vlan <i>vlanid</i>	Set the filter based on VLAN ip-access-list indicates that the filter uses IP access list mac-access-list indicates that the filter uses MAC access list access-list-map indicates that the filter uses user-defined access list map acllist all access control list series number, all means all the configured access control lists Vlan the filter is applied to VLAN vlanid VLAN ID
3	filter (enable disable)	enable filter fuction effect enable disable filter fuction effect disable
4	exit	Exit global configuration mode and enter privileged EXEC mode
5	show filter	Show all filter status

11.6.3 Monitoring and Maintenance

Check and display all configuration filter status command:

Command	Description
show filter	Display all configuration filter status

11.6.4 Specific Configuration Examples

Example 1:

- Destination

The switch does not allow TCP packet to pass through with destination port 80

- Set up steps

Raisecom#**config**

Raisecom(config)# **ip-access-list 0 deny tcp any any 80**

Raisecom(config)# **filter ip-access-list 0**


```
Raisecom(config)#filter enable
```

```
Raisecom(config)#exit
```

Example 2:

➤ Destination

The switch does not allow ARP packets with the MAC address 000e.3842.34ea to pass through on port 2 to 8.

➤ Set up Steps

```
Raisecom#config
```

```
Raisecom(config)# mac-access-list 2 deny arp any 000e.3842.34ea
```

```
Raisecom(config)# filter mac-access-list 2 ingress portlist 2-8
```

```
Raisecom(config)#filter enable
```

```
Raisecom(config)#exit
```

Example 3:

➤ Destination

The switch allows IP packets with the source address in network segment 10.0.0.0/8 to pass through in VLAN 3

➤ Set up Steps

```
Raisecom#config
```

```
Raisecom(config)# ip-access-list 2 deny ip any any
```

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

```
Raisecom(config)# filter ip-access-list 2,3 vlan 3
```

```
Raisecom(config)#filter enable
```

```
Raisecom(config)#exit
```

11.7 Configuration Function Based on Software IP ACL

The steps below show how to use software IP ACL on Layer-3 interface:

1) Define access control list

Show in section 1.2

2) ACL Configuration

Filtering rules on a Layer-3 interface can be combined of one or multiple “permit | deny” sentences, every sentence has different specified packet ranges, so matching order problem may happen when matching one packet and ACL rule. The matching order depends on the orders of configured filtering rules, as the order closer to the back, the higher the priority will be. When conflict happens, high priority will be the benchmark.

11.7.1 Layer-3 Interface Protect Configuration Based on IP ACL

Steps	Command	Description
1	config	Entry into global configuration mode
2	interface ip <0-14>	Enter Layer-3 interface configuration mode
3	[no] ip ip-access-list {all/ acllist}	Set Layer-3 interface filter ip-access-list indicates that the filter uses IP access list acllist all access control list series number, all means all the configured access control lists
4	exit	Exit Ethernet Layer-3 interface configuration mode and enter global configuration mode
5	exit	Exit global configuration mode and enter privileged EXEC mode
6	show interface ip ip-access-list	Show filters status for all interfaces

11.7.2 Monitoring and Maintenance

Check and display configuration filter status command:

Command	Description
show interface ip ip-access-list	Show all filters status for Layer-3 interface

11.7.3 Specific Configuration Example

Example 1:

- Destination

Switch only allow IP packet with 10.0.0.0/8 access

- Set up steps

Raisecom#**config**

Raisecom(config)# **ip-access-list 2 deny ip any any**

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

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

Raisecom(config-ip)# **ip ip-access-list 2,3**

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

Raisecom(config)#**exit**

Chapter 12 QoS Configuration

This chapter describes the function of ISCOM series of switches and how to configure QoS. By using the QoS features, it can achieve on a particular type of flow control, it provides service guarantee quality for the business and user.

12.1 Configuration Description

To guide the user to configuration QoS function except for Policy and class function; To guide the user to configuration most QoS function on the most Switch device. User can look up the QoS function command one to the QoS function command nine to see the details.

12.2 QoS Introduction

12.2.1 Introduction

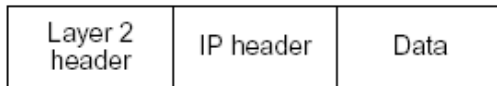
Generally speaking, Internet (IPv4 standard) provides users only “best effort” service, cannot guarantee a real-time and complete packets transmission, and the quality of services either. Since user always has different requirements for the transmission quality of separate multi-media applications, network 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

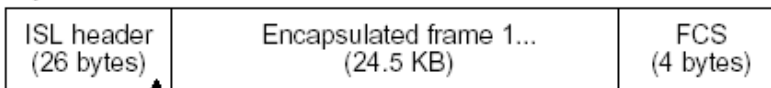
ISCOM2800 mechanism realizes layer-2 packets classification based on 802.1P and 802.1Q standards. 802.1Q defines VLAN, though QoS is not defined in this standard, the given mechanism which mention that the frame precedence can be modified configures a strong groundwork to realize QoS. 802.1P standard 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:

Encapsulated Packet

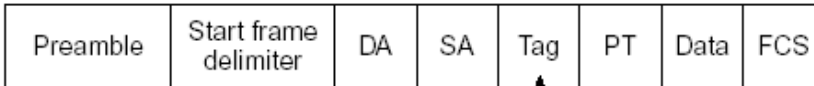


Layer 2 ISL Frame



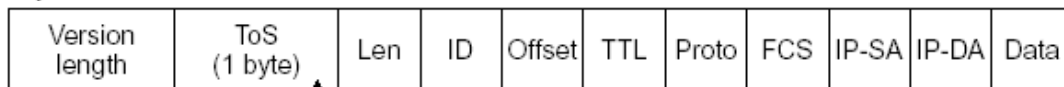
↑ 3 bits used for CoS

Layer 2 802.1Q/P Frame



↑ 3 bits used for CoS (user priority)

Layer 3 IPv4 Packet



↑ IP precedence or DSCP

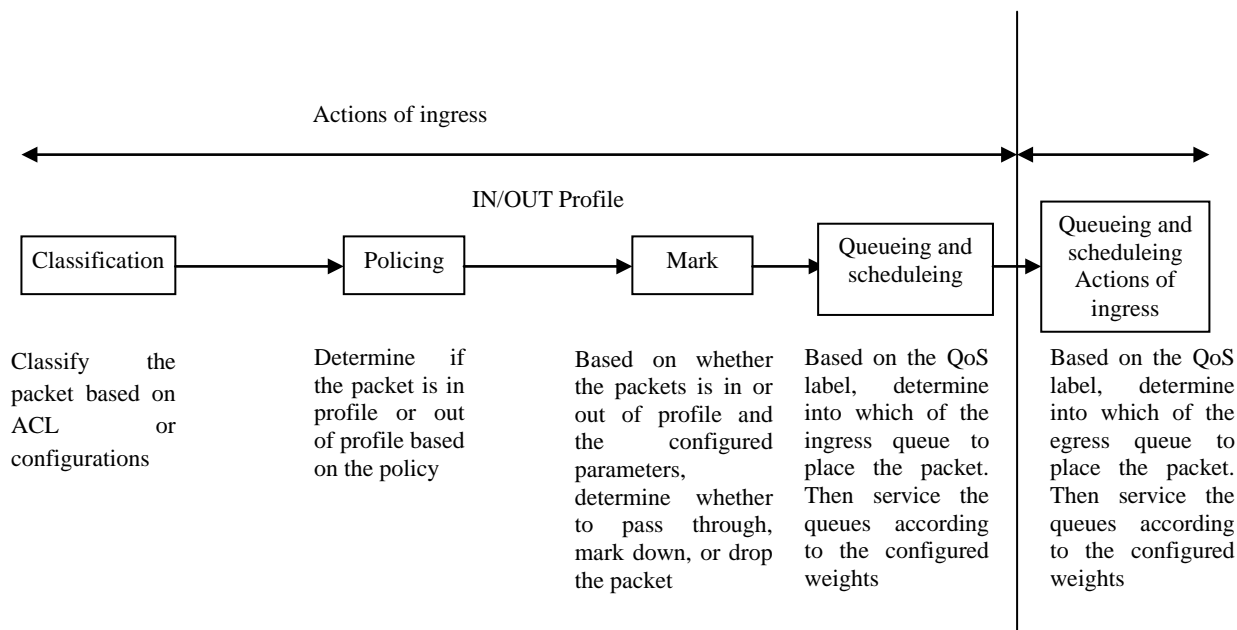
The 8 priority defined by CoS can be considered as the following 8 kinds of packets: Priority	Message type	Application
000	Routine	Level 0 corresponds to the default of the best efforts of the information delivery
001	Priority	Level 1 ~ 4 are corresponds for the definition of multi-media data or important 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 selection

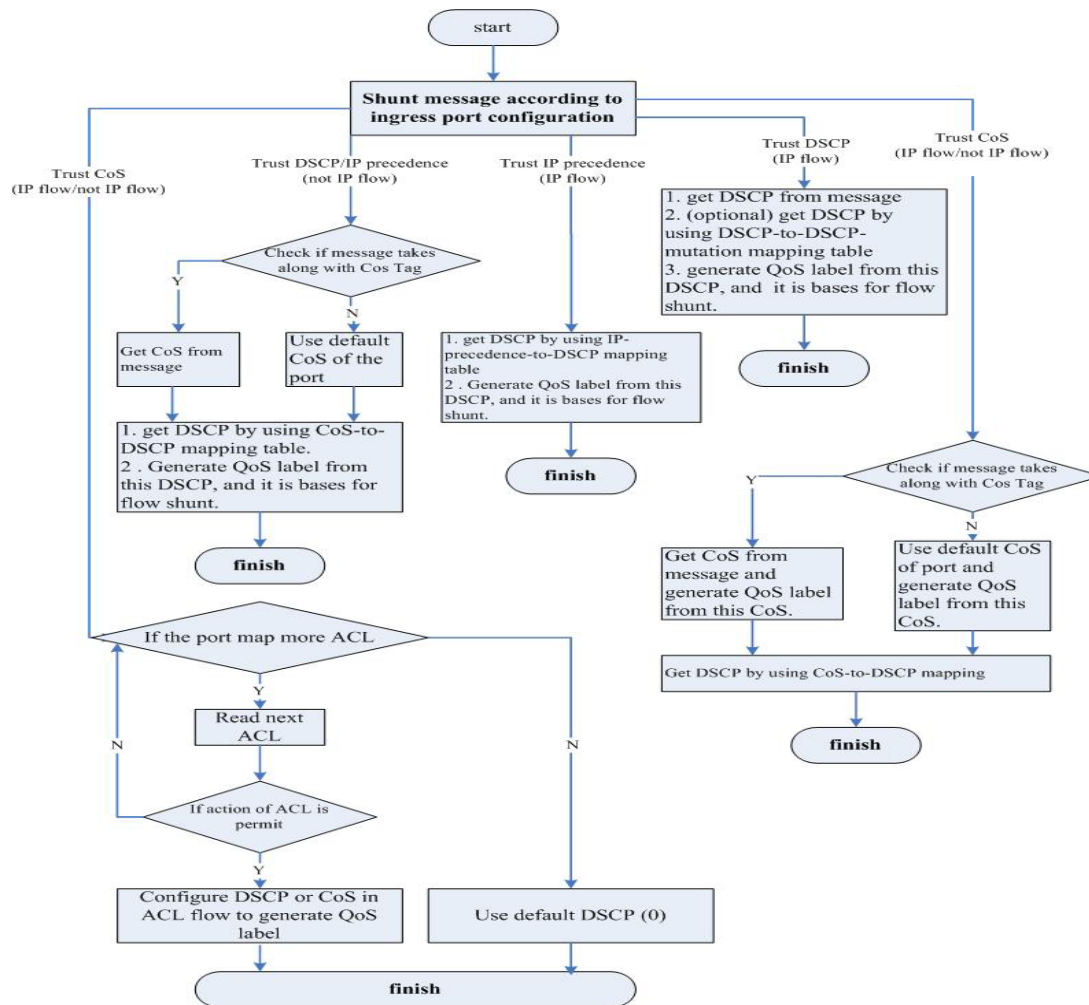
- of an output queue.
- Scheduling: based on configured WRR (Weighted round robin) and threshold to provide service for output queue.

➤ The figure below shows the QoS basic model:



12.2.2 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 mutually 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 classification, 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.

12.2.3 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.

12.2.4 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 switch 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.

12.2.5 Mapping Table

During QoS processing, switch describes the inner DSCP precedence for all traffics:

- 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.
- 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.
- 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.

12.2.6 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:

- Regenerate packet COS value according to the defined rules while maintaining the packet's native COS value
- 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 series 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.

12.2.7 QoS Default Configuration

Step	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

12.3 QoS Enable and Disable

12.3.1 QoS Start and Stop Default Configuration

	Attributes	Default configuration
1	QoS start	Disable

12.3.2 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.

12.3.3 Monitoring and Maintenance

Command	Description
show mls qos	Show QoS switch status

12.3.4 Configuration Examples

Open QoS function:

Raisecom#**config**

Raisecom(config)#**mls qos**

Raisecom#**show mls qos**

Show as below:

QoS is enabled.

12.4 Classification Function Configuration

12.4.1 Classification Default Configuration

Function	Default Value
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

12.4.2 Flow Classification Configuration Based on Port TRUST Status

Attention:

- Port TRUST status and ACL/Class-map flow classification 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 equipment.
- QoS TRUST status configuration and TRUST policy status configuration are mutually exclusive, and later configuration will take effects.

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 [<i>cos / dscp / port-priority</i>]	All QoS TRUST status ports configuration cos: configuration the switch as TRUST CoS status dscp: configuration the switch as TRUST DSCP status port-priority: 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

.....

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 port <i>portid</i>	Entry to port configuration mode
3	mls qos TRUST [<i>cos / dscp</i>]	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 <i>portid</i>	Show QoS port configuration

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 port <i>portid</i>	Entry to port configuration mode
3	mls qos default-cos override	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 <i>portid</i>	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

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.

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 <i>portid</i>	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 <i>portid</i>	Show QoS port configuration

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 port <i>portid</i>	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 <i>portid</i>	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

12.4.3 Configuring Flow Classification on ACL/class-map

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 <i>class-map-name</i> [<i>match-all/match-any</i>]	Create name as aaa, class-map and entry into config-cmap mode. <i>class-map-name</i> : class-map name, Max 16 characters match-all: satisfy all rules in class match-any: satisfy only one rule in class
3	description <i>WORD</i>	Description of information <i>WORD</i> : 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 [<i>WORD</i>]	Show CLASS MAP <i>WORD</i> : 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 because the matching message may have conflicts.
- When a ACL is matched, ACL must be identified and its type must be permit.

- When a class-map is matched, sub class-map must be match-all type.

Configuring match statements

Steps	Command	Description
1	config	Entry into global configuration mode
2	class-map <i>class-map-name</i>	Entry into config-cmap mode <i>class-map-name</i> : class-map name, max 16 characters
3	match { <i>ip-access-list</i> / <i>mac-access-list</i> / <i>access-list-map</i> } <i>acl-index</i>	Match ACL <i>ip-access-list</i> : match IP access list <i>mac-access-list</i> : match MAC access list <i>access-list-map</i> : match access control list map table <i>acl-index</i> : access 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 <i>WORD</i>	Match class map <i>WORD</i> : match class-map name, max 16 characters
8	exit	Return to global configuration mode
9	exit	Return to privilege mode
10	show class-map [<i>WORD</i>]	Show CLASS MAP <i>WORD</i> : 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 <i>class-map-name</i>	Entry into config-cmap mode <i>class-map-name</i> : class-map name, max 16 characters
3	no match { <i>ip-access-list</i> / <i>mac-access-list</i> / <i>access-list-map</i> } <i>acl-index</i>	Match ACL <i>ip-access-list</i> : match IP access list <i>mac-access-list</i> : match MAC access list <i>access-list-map</i> : match access control list map table <i>acl-index</i> : 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 <i>WORD</i>	Match class map <i>WORD</i> : 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.

12.4.4 Monitoring 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 equipments. 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

```

12.4.5 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

```

12.5 Policy and Marking Function Configuration

12.5.1 Policy and Marking Default Configuration

Function	Default value
Policy TRUST status	DSCP

12.5.2 Policy and Marking Configuration

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 <i>policy-map-name</i>	Create name as bbb, policy-map and entry into config-pmap mode. policy-map-name: policy map name, max 16 characters
3	description <i>WORD</i>	Description information 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 <i>WORD</i> : policy map name, max 16 characters
----------	-------------------------------	---

Configuration examples:

Raisecom#**config**

Raisecom(config)# **policy-map** *bbb*

Raisecom(config)# **exit**

To check whether 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.

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 <i>policy-map-name</i>	Entry into config-pmap mode policy-map-name: policy map name, max 16 characters
3	class-map <i>class-map-name</i>	Encapsulate cuclass-map aaa into policy aaa, and entry into config-pmap-c mode <i>class-map-name</i> : 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 policies.

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 whether 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 <i>policy-map-name</i>	Entry into config-pmap mode policy-map-name: policy map name, max 16 characters
3	no class-map <i>class-map-name</i>	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.

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 <i>policy-name</i>	Entry into config-pmap mode policy-name: policy map name, max 16 characters
3	Class-map <i>class-name</i>	Encapsulate class-map into policy, and entry into config-pmap-c mode class-name: class-map name, max 16 characters
4	police <i>policer-name</i>	Use policer for the policy data flow for bit-rate limiting and reshaping, check the link for more information: bit-Rate Limitation and reshaping function configuration policer-name: policer name, max 16 characters
5	TRUST [<i>cos</i> / <i>dscp</i> <i>ip-precedence</i>]	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 <i>new-dscp</i> ip precedence <i>new-precedence</i> cos <i>new-cos</i> }	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 <i>to-port</i>	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 <i>policy-name</i>	Entry into config-pmap mode <i>policy-name</i> : policy map name,max 16 characters
3	class-map <i>class-name</i>	Encapsulate class-map aaa into policy aaa, and entry into config-pmap-c mode <i>class-name</i> : class-map name, max 16 characters
4	no police <i>policer-name</i>	Apply policer in this policy data flow <i>policer-name</i> : policer name, max 16 characters Data flow TRUST status, default use DSCP <i>cos</i> : set switch as TRUST CoS status <i>dscp</i> : set switch as TRUST DSCP status <i>ip-precedence</i> : set switch as TRUST IP priority status
5	no TRUST [<i>cos</i> / <i>dscp</i> / <i>ip-precedence</i>]	Set new value for data flow <i>new-dscp</i> : DSCP value, 0-63; <i>new-precedence</i> : IP priority value, 0-7 <i>new-cos</i> : set CoS value, 0-7
6	no set { <i>ip dscp</i> / <i>ip precedence</i> / <i>cos</i> }	
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

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 <i>policy-name</i> ingress <i>portid</i> [egress <i>portlist</i>]	Apply policy on in/out port. <i>policy-name</i> : policy map name, max 16 characters <i>portid</i> : in port number <i>portlist</i> : out port list
3	exit	Return to privilege mode
4	show policy-map port [<i>portlist</i>]	Display port policy application information <i>portlist</i> : port number

Attention:

- QoS must start before applying 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:

Egress:1-5

Class Map :aaa (match-all)

port 1 on egress:

Policy Map bbb:

12.5.3 Monitoring and Maintenance

Command	Description
show policy-map [WORD]	Display POLICY MAP information <i>WORD</i> : policy map name, max 16 characters
show policy-map class {WORD}	Display some classified information of POLICY MAP <i>WORD</i> : class-map name, max 16 characters
show policy-map port [portlist]	Display port policy application information <i>portlist</i> : 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 specific 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)
```

12.5.4 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
```

12.6 Bit-Rate Limitation and Reshaping Function Configuration

12.6.1 Bit-Rate Limitation and Reshaping Default Configuration

None

12.6.2 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 <i>policer-name</i>	Create policer in type of single

	<i>rate burst exceed-action {drop policed-dscp-transmit marked-dscp }</i>	<i>policer-name</i> : set policer name <i>rate</i> : bit-rate value (Kbps), 8—2000000 <i>burst</i> : Burst value (KBps), 8—512000 <i>drop</i> : dropped packets once it is over bit-rate value <i>policed-dscp-transmit</i> : modified DSCP value once it is over bit-rate value <i>marked-dscp</i> : modified DSCP value once it is over bit-rate value Create policer as type of class
3	mls qos class-policer <i>policer-name</i> <i>rate burst exceed-action {drop policed-dscp-transmit marked-dscp }</i>	<i>policer-name</i> : set policer name <i>rate</i> : bit-rate value(Kbps), 8—2000000kbps <i>burst</i> : burst value (KBps), 8—512000 <i>drop</i> : dropped packets once it is over bit-rate value <i>policed-dscp-transmit</i> : modify DSCP once it is over bit-rate value <i>marked-dscp</i> : modified DSCP value once over bit-rate value Create policer as type of aggregate
4	mls qos aggregate-policer <i>policer-name rate burst exceed-action {drop policed-dscp-transmit marked-dscp }</i>	<i>policer-name</i> : set policer name <i>rate</i> : bit-rate value(Kbps), 8—2000000kbps <i>burst</i> : burst value (KBps), 8—512000 <i>drop</i> : dropped packets once it is over bit-rate value <i>policed-dscp-transmit</i> : modify DSCP once it is over bit-rate value <i>marked-dscp</i> : modified DSCP value once over bit-rate value
5	exit	Return to global configuration mode
6	show mls qos policer [<i>single-policer class-policer aggregate-policer</i>]	Display policer information <i>single-policer</i> : display single policer <i>class-policer</i> : display class policer <i>aggregate-policer</i> : display aggregate policer

To delete a policer, use command of 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.

12.6.3 Monitoring and Maintenance

Command	Description
show mls qos policer [<i>single-policer class-policer aggregate-policer</i>]	Display policer information <i>single-policer</i> : Display single policer <i>class-policer</i> : Display class policer <i>aggregate-policer</i> : 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

policy map name: aaa

policer type: Single, *name*: aaa

rate: 44 kbps, *burst*: 44 kbyte, *exceed action*: *policed-dscp-transmit*, *dscp*:4

12.6.4 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

policy map name: aaa

policer type: Single, name: aaa

rate: 44 kbps, burst: 44 kbyte, exceed action: policed-dscp-transmit, dscp: 4

12.7 Map Function Configuration

12.7.1 Map Default Configuration

COS-localpriority default configuration relationship as:

CoS value	0	1	2	3	4	5	6	7
Localpriority value	0	1	2	3	4	5	6	7

DSCP - localpriority default map relation as:

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

TOS- localpriority default map relation as:

ToS value	0	1	2	3	4	5	6	7
localpriority	0	1	2	3	4	5	6	7

12.7.2 CoS-localpriority map List Configuration

CoS-localpriority map list maps incoming packet COS value as a localpriority value. QoS is used to describe data flow priority. It default map relation as:

CoS value	0	1	2	3	4	5	6	7
Localpriority value	0	1	2	3	4	5	6	7

To modify the map relations, the following steps are set:

Steps	Command	Description
1	config	Entry into global configuration mode
2	mls qos mapping cos <cosVal> to localpriority <localPrioVal>	Set new map relation <i>cosVal</i> : COSvslur, range 0-7 <i>localPrioVal</i> : local priority, range 0-7
3	exit	Return to privilege mode
4	show mls qos mapping cos	Show cos-localpritoiry map inforamtion

Configuration examples:

Configuration cos as **5localpritoiry**

Raisecom#config

Raisecom(config)# **mls qos mapping cos 5 to localpriority 3**

Raisecom(config)#**exit**

Raisecom# **show mls qos mapping cos**

Show results as:

CoS-LocalPriority Mapping:

CoS: 0 1 2 3 4 5 6 7

LocalPriority: 0 1 2 3 4 5 6 7

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 localPriority map list

Raisecom#**show mls qos maps cos-dscp**

Cos-dscp map:

cos: 0 1 2 3 4 5 6 7

LocalPriority: 0 1 2 3 4 5 6 7

12.7.3 DHCP-localpriorityMap List Configuration

DHCP-localpriority map-list configuration maps incoming packet into a localpriority value. QoS is used to describe the data flow priority. Its default map relation as show below:

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

To modify that map relation, set as the following steps:

Steps	Command	Description
1	config	Entry global configuration mode
2	mls qos mapping dscp <dscpVal> to localpriority <localPrioVal>	Set new map relationship <i>dscpVal</i> :dscp value,range 0-63 <i>localPrioVal</i> : local priority value, range 0-7
3	exit	Return to privilege mode
4	show mls qos mapping dscp	Display dscp-localprioitry map information

Configuration example:

Configure dscp map as **5 localpriority**:

Raisecom#**config**

Raisecom(config)# **mls qos mapping dscp 5 to localpriority 3**

Raisecom(config)#**exit**

Raisecom# **show mls qos mapping dscp**

Show results as:

DSCP-LocalPriority Mapping:

```

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

0:      0  0  0  0  0  0  0  0  0  1  1
1:      2  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

```

Backing up dscp-localpriority map list to default map relation, use command **no**.

Steps	Command	Description
1	config	Entry into global configuration mode
2	no mls qos mapping dscp	Backup to default map relation
3	exit	Return to privilege mode
4	show mls qos mapping dscp	Show dscp-localpriority map list

DSCP-LocalPriority Mapping:

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

```

0:    0 0 0 0 0 0 0 0 0 1 1
1:    2 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

```

12.7.4 tos-localpriority List Configuration

Tos-localpriority list maps the incoming packet DSCP value into a localpriority value. QoS use its description data flow priority.

To modify that map relation, follows the steps below:

Steps	Command	Description
1	Config	Entry into global configuration mode
2	mls qos mapping tos <tosVal> to localpriority <localPrioVal>	set new map relation <i>tosVal</i> :TOS value, range 0-7 <i>localPrioVal</i> : local priority value, range 0-7
3	Exit	Return to privilege mode
4	show mls qos maps dscp-cos	Show tos map information

Configuration examples:

Configure **cos** map as **5 localpriority**

Raisecom#**config**

Raisecom(config)# **mls qos mapping tos 5 to localpriority 3**

Raisecom(config)#**exit**

Raisecom# **show mls qos mapping tos**

show results as:

ToS-LocalPriority Mapping:

ToS: 0 1 2 3 4 5 6 7

LocalPriority: 0 1 2 3 4 5 6 7

To delete tos-localpriority map list to default mapping relation, use command **no**:

steps	command	description
1	config	Entry into global configuration mode
2	no mls qos mapping tos	Back to the default mapping relation
3	exit	Return to privilege mode
4	show mls qos mapping tos	Show tos-localpriority map list

Raisecom#**show mls qos maps dscp-cos**

ToS-LocalPriority Mapping:

ToS: 0 1 2 3 4 5 6 7

LocalPriority: 0 1 2 3 4 5 6 7

12.7.5 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 frame priority and queue priority override.

Configuration steps as below:

Steps	Command	Description
1	config	Entry into global configuration mode
2	interface { port-list } <i><1-MAX_PORT_NUM></i>	Entry into Ethernet physic interface mode <i>1-MAX_PORT_NUM</i> equipment port numbers
3	mls qos {smac dmac} <i>{priority-set/cos-override}</i>	set up ports based on smac, dmac's frame priority or queue priority override function Smac: source MAC Dmac: destination MAC <i>cos-override</i> : frame priority <i>priority-set</i> : queue priority
4	mls qos {smac/dmac} <i>priority-set cos-override</i>	set up ports based on smac, dmac's frame priority and queue priority override function Smac: source MAC Dmac: destination MAC <i>cos-override</i> : frame priority <i>priority-set</i> : queue priority
5	mls qos vlan <i>{priority-set/cos-override}</i>	set up ports based on vlan's frame priority or queue priority override function <i>cos-override</i> : frame priority <i>priority-set</i> : queue priority

6	mls qos vlan <i>priority-set</i> <i>cos-override</i>	set up ports based on vlan's frame priority and queue priority override function <i>cos-override</i> : frame priority <i>priority-set</i> : queue priority
7	exit	Exit
8	show mls qos port-list {1- <i>MAX_PORT_NUM</i> }	Display QoS configuration information 1- <i>MAX_PORT_NUM</i> equipment port numbers

To use command no Renew all priority override based on smac、dmac、vlanto default configuration(even both of them are not override).

12.7.6 Monitoring and Maintenance

Command	Description
show mls qos mapping [cos dscp tos localpriority]	Display all map list's configuration content. <i>cos</i> : show cos map configuration information <i>dscp</i> : show cos map configuration information <i>tos</i> : show cos map configuration information <i>localpriority</i> : show local priority queue map configuration information
show mls qos queue	Display QoS queue map list
show mls qos port [<i>portid</i>]	Display QoS configuration information <i>Portid</i> : portID

Map list information maps

Raisecom#**show mls qos mapping cos**

CoS-LocalPriority Mapping:

```

CoS:      0  1  2  3  4  5  6  7
-----
LocalPriority:  0  1  2  3  4  5  6  7

```

Raisecom# **show mls qos mapping dscp**

DSCP-LocalPriority Mapping:

```

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

```

Raisecom#show mls qos mapping cos

ToS-LocalPriority Mapping:

ToS:	0	1	2	3	4	5	6	7

LocalPriority:	0	1	2	3	4	5	6	7

Raisecom#show mls qos mapping localpriority

LocalPriority-Queue Mapping:

LocalPriority:	0	1	2	3	4	5	6	7

Queue:	1	2	3	4	5	6	7	8

Queue map list information queueing

Raisecom(config)#show mls qos queue port 1

Port:1

Queue	Weight(WRR)

1	1
2	1
3	1
4	1
5	1
6	1
7	1

Display QoS configuration information

Raisecom#show mls qos port 1

Port	Priority	Scheduler

1	0	SP

12.7.7 Specific Configuration Examples

See the sections for details.

12.8 Queue and Adjust Function Mode

So far, the equipments 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.

12.8.1 Queue and Adjust Default Configuration

Function	Default value
Queue adjust policy	Strict priority adjust SP

12.8.2 SP Configuration

Configuration steps as:

Steps	Command	Description
1	config	Entry into global configuration mode
2	mls qos queue scheduler sp	Configuration is strict priority
3	exit	Return to privilege mode
4	show mls qos que	display QoS queuing information

12.8.3 WRR Configuration

Configuration steps as:

Steps	Command	Description
1	config	Entry into global configuration mode
2	mls qos queue scheduler wrr <weightVal1> <weightVal2> <weightVal3> <weightVal4> [<weightVal5> <weightVal6> <weightVal7> <weightVal8>]	Set ports' adjust mode as WRRmode Weight 1-8: set queue 1-8 weight value
3	exit	Return to privilege mode
4	show mls qos que	display QoS queuing information

12.8.4 DRR Configuration

Configuration steps as:

Steps	Command	Description
1	config	Entry into global configuration mode
2	mls qos queue scheduler drr <weightVal1> <weightVal2> <weightVal3> <weightVal4> [<weightVal5> <weightVal6> <weightVal7> <weightVal8>]	Set ports' adjust mode as DRR mode Weight 1-8: set queue 1-8 weight value
3	exit	Return to privilege mode

4	show mls qos queue	display QoS queuing information
----------	---------------------------	---------------------------------

12.8.5 WFQ Configuration

Configuration steps as:

Steps	Command	Description
1	config	entry into global configuration mode
2	mls qos queue scheduler wfq <weightVal1> <weightVal2> <weightVal3> <weightVal4> [<weightVal5> <weightVal6> <weightVal7> <weightVal8>]	Set ports' adjust mode as WFQ mode Weight 1-8: set queue 1-8 weight value
3	exit	Return to privilege mode
4	show mls qos queue	display QoS queuing information

12.8.6 Monitoring and Maintenance

Command	Description
show mls qos queue	Display QoS's queuemap list

Queue map list information queueing

Raisecom(config)#**show mls qos queue port 1**

Port:1

Queue	Weight(WRR)
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1

12.8.7 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:*

Queue	Weight(WRR)
1	1
2	2
3	4
4	8

12.9 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.

12.10 QoS Command Reference

Command	Description
class-map <i>class-map-name</i> [match-any match-all]	Create class-map
no class-map <i>class-map-name</i>	Delete class-map
[no] policy-map <i>policy-map-name</i>	Create delete policy map
description <i>WORD</i>	Set policy map and class-map description information
[no] class <i>class-map-name</i>	apply class map on policy
match { ip-access-list <i>acl-index</i> mac-access-list <i>acl-index</i> access-list-map <i>acl-index</i> ip dscp <i>dscp-list</i> ip precedence <i>ip-precedence-list</i> class <i>calss-name</i> vlan <i>vlanlist</i> }	Set match statements
no match { ip-access-list <i>acl-index</i> mac-access-list <i>acl-index</i> access-list-map <i>acl-index</i> ip dscp ip precedence class <i>calss-name</i> vlan <i>vlanlist</i> }	Delete match statements
[no] trust [cos dscp]	Set data flow TRUST status
set { ip dscp <i>new-dscp</i> ip precedence	Set actions

<i>new-precedence</i> cos <i>new-cos</i> }	
no set { ip dscp ip precedence cos }	Delete set value
mls qos { aggregate-policer class-policer single-policer } <i>policer-name</i> <i>rate</i> <i>burst</i> [exceed-action { drop policed-dscp-transmit <i>dscp</i> }]	Create policer
no mls qos { aggregate-policer class-policer single-policer } <i>policer-name</i>	Delete policer
[no] police <i>policer-name</i>	Apply policer
service-policy <i>policy-map-name</i> ingress <i>portid</i> [egress <i>portlist</i>]	Apply policy
no service-policy <i>policy-map-name</i> ingress <i>portid</i>	Decline apply policy
mls qos map cos-dscp <i>dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8</i>	configuration CoS to DSCP map
no mls qos map cos-dscp	Renew CoS to DSCP map
mls qos map ip-prec-dscp <i>dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8</i>	Configuration ToS to DSCP map
no mls qos map ip-prec-dscp	Renew ToS to DSCP map
mls qos map dscp-cos <i>dscp-list</i> to <i>cos</i>	Configuration DSCP to switch internal priority map
no mls qos map dscp-cos	Renew DSCP to switch internal priority map
queue cos-map <i>queue-id</i> <i>cos-list</i>	Configuration switch internal priority to queue map
no queue cos-map	Renew switch internal priority to queue map
queue wrr-weight <i>weight0 weight1 weight2 weight3</i>	Configuration switch queue adjust mode as WRR
queue bounded-delay <i>weight0 weight1 weight2 weight3</i> <i>delaytime</i>	Set port adjust mode as BOUNDDelay mode
queue preemp-wrr <i>weight1 weight2 weight3</i>	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 [<i>policename</i> <i>aggregate-policer</i> <i>class-policer</i> <i>single-policer</i>]	Display policer information
show mls qos maps [<i>cos-dscp</i> <i>dscp-cos</i> <i>dscp-mutation</i> <i>ip-prec-dscp</i>]	Display every map list configuration content
show mls qos queueing	Display in/out queue configuration information
show mls qos port <i>portid</i> [<i>policers</i>]	Display port strategy configuration, policer, etc information
show class-map [<i>class-map-name</i>]	Display class-map information
show policy-map [<i>policy-map-name</i> [<i>port</i> <i>portid</i>]] [<i>class</i> <i>class-name</i>]	Display policy information

Chapter 13 802.3ah OAM Function Configuration

13.1 802.3ah OAM Principle Introduction

IEEE802.3ah OAM (Operation Administration Maintenance) is used to provide more efficient Ethernet link operation, management and maintenance. As the efficient complementarity of the high managing tool, OAM enhances the Ethernet management and monitoring.

13.1.1 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.

13.1.2 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.

13.1.3 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 switches. 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 frame 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.)

13.1.4 OAM mib

Devices can gain opposite device link configuration/ statistics value through OAM and then get link status/ data.

13.2 802.3ah 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 variable 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 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
```

13.3 802.3ah OAM Active Mode Function

13.3.1 OAM default configuration

Function	Default Value
OAM Enable\Disable	Enable
Opposite OAM event alarm	Disable

13.3.2 OAM enable/disable configuration function

✧ OAM Enable\Disable

OAM is Ethernet point to point link protocol. 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 port <i>port_number</i>	Entry Ethernet physical interface mode <i>port_number</i> : physical interface number
3	oam { <i>disable</i> / <i>enable</i> }	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 port 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

13.3.3 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 port <i>port_number</i>	Entry Ethernet physical interface mode, <i>port_number</i> 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 port 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 port <i>port_number</i>	Entry Ethernet physical interface mode <i>port_number</i> 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 port 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.

- Except for OAM packets, all other packets are loopbacked.
- In loopback port, it only allows OAM packets to hand CPU
- Loopback port is prohibited forwarding packets to other ports
- The other ports are prohibited forwarding packets to loopback port

13.3.4 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 port <i>port_number</i>	Entry Ethernet physical interface mode <i>port_number</i> is physical interface number
3	oam peer event trap <i>{disable enable}</i>	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 port 2
```

```
Raisecom(config-port)# oam peer event trap enable
```

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

```
Raisecom(config)#exit
```

```
Raisecom#show oam trap
```

13.3.5 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 particularly 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 several attribute. Attribute is variable's smallest unit. OAM variable gain uses Clause 30 to state object/package/attribute's branch described 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 } <i>port_number</i>	Gain opposite device OAM information or port statistics variable value <i>port_number</i> : 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.

13.3.6 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 port <i>port_number</i>	Entry Ethernet physical interface mode <i>port_number</i> : 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 port 2**

Raisecom(config-port)#**oam clear statistics**

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

Raisecom(config)#**exit**

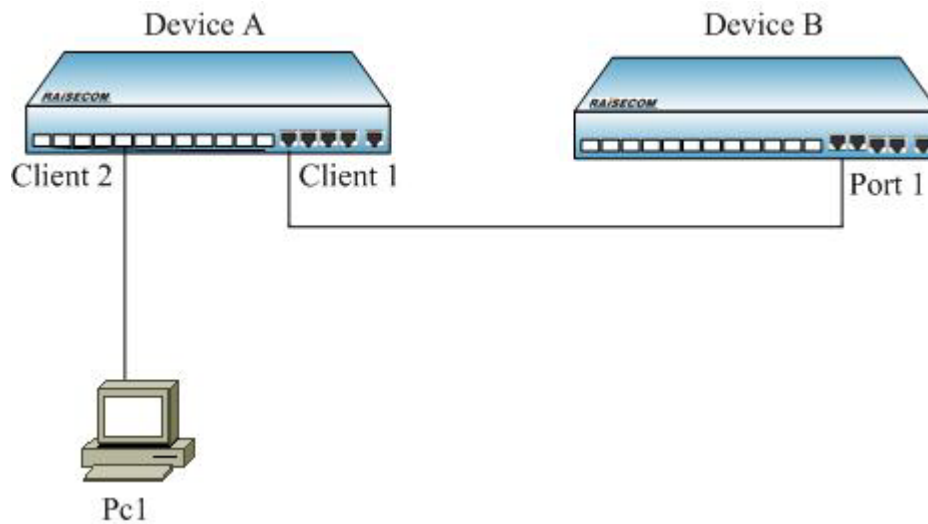
Raisecom#**show oam statistics**

13.3.7 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

13.3.8 Configuration example



As figure above, to set remote loop-back as following configuration:

```
Raisecom#config
```

```
Raisecom (config)#interface port 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 port 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

13.4 802.3ah OAM Passive Function

13.4.1 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 1 (s) Threshold 1 (unit)
Error frame event window and threshold	Window 1 (s) Threshold 1 (unit)
Error frame second statistics event window and threshold	Window 60 (s) Threshold 1 (unit)
Symbol error event window and the threshold	Window 1 (s) Threshold 1 (unit)

13.4.2 OAM enable/disable configuration

✧ OAM Enable\Disable

OAM is Ethernet point to point link protocol, 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 <i>port_number</i> : 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 port 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

13.4.3 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: 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 port 2
```

```
Raisecom(config-port)#oam loopback ignore
```

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

```
Raisecom(config)#exit
```

```
Raisecom#show oam loopback
```

13.4.4 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 periodically error frames over threshold, device will have that event.

Error frame periodical event: lately N frames' error is over threshold, N is indicated value; once lately N frames' error over threshold is detected, and device will release that event.

Error frame second statistics event: lately M seconds, the error frames' 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} <i>port_number</i>	Enter Ethernet physical interface mode <i>port_number</i> : physical interface number
3	oam errored-frame window <1-60> threshold <0-65535>	Config error frame monitoring window and threshold <1-60> : monitoring window, unit is second. <0-65535> : threshold.
4	oam errored-frame-period window <100-60000> threshold <0-65535>	Config error frame periodical event monitoring window and threshold <100-60000> : monitoring window, unit is second. <0-65535> : threshold.
5	oam errored-frame-seconds window <10-900> threshold <0-65536>	Config error frame statistics monitoring window and threshold <10-900> : monitoring window, unit is second. <0-65536> : threshold.
6	oam errored-symbol-period window <1-60> threshold <0-65535>	Set the error code statistics event monitoring window and threshold <1-60> : monitoring window, unit is second <0-65535> : threshold, unit is one
7	exit	Return to global configuration mode
8	exit	Return to privileged EXEC mode
9	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 port 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 frame event monitoring window and threshold as Default Value.

13.4.5 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 <i>port_number</i> 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 configuration situation

Disable port 3 critical-event fault indication:

```
Raisecom#config
```

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

```
Raisecom(config-port)# oam notify critical-event disable
```

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

```
Raisecom(config)#exit
```

```
Raisecom#show oam notify
```

13.4.6 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 <i>port_number</i> :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 port 2**

Raisecom(config-port)# **oam event trap enable**

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

Raisecom(config)#**exit**

Raisecom#**show oam trap**

13.4.7 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 information or port statistics variable value <i>port_number</i> : physical interface number

Gain port 2 opposite device OAM information value:

Raisecom(debug)#**show oam peer oam-info port-list 2**

13.4.8 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 information. 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 <i>port_number</i> : 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 port 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 <i>port_number</i> : 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 port 2**

```
Raisecom(config-port)# clear oam event
```

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

```
Raisecom(config)#exit
```

```
Raisecom#show oam event
```

```
Raisecom#show oam peer event
```

13.4.9 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

13.4.10 Configuration example

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 14 Optical Module Digital Diagnoses Configuration

14.1 Optical Module Digital diagnoses principle

SFP (Small Form Pluggable) is a kind of optical module in media converter. The fault diagnoses function provides the system a way of performance monitoring. Using the data monitoring function provided by this module, network administrator can forecast the lasting time of the module, insulate the system fault and validate the module compatibility when fixing equipments.

Each SFP module provides five performance parameters: the media converter temperature, inner power supply voltage, sending electronic current, sending optical power and receiving optical power.

The digital diagnoses module polls all the SFP ports every 5 seconds, and gives three datasheet according to the performance parameter getting from the poll: the real-time monitoring table of the optical module, the period performance monitoring table of the optical module, the current period performance monitoring table. When the parameter exceeds the threshold, it will send trap and offer its global switch control.

The index of optical module real-time monitoring table is SFP port number and parameter type. Inside the software the table has stable number of rows, but when you look over it in the command lines only the information of the ports that are active (the row mark is valid) can be shown. Seen from the network management software, the table has stable number of rows, when SFP is not active it means the row mark of the table is invalid. The table restores the parameter value, threshold value, the time and value that the last time the threshold value is exceeded of each parameter for each SFP module. The initialized value of last threshold exceeding is -1000000, the left values are all 0. When the digital diagnose module polls SFP port every 5 seconds, if SFP is active, read SFP's 5 parameter value, adjusting measure, adjusting parameter and threshold value, refresh the parameter value and threshold value of the optical module real-time monitoring table, if it exceeds the threshold value, update the time and value of the exceeding Digital diagnoses configuration. Configure real-time monitoring table that the row mark is invalid. Each row of the table contains 2 variables, which stands for how many 15 minutes' cycle records and 24 hours' cycle records are restored in the parameters of SFP ports. Now digital diagnoses module supports 96 15 minutes' cycle record and 1 24 hours' cycle record at the most.

The index of optical module current period performance monitoring table is SFP port number, period type and parameter type. The table records the maximum value, least value and the average value of the parameters that are within a recording cycle. The table has stable row number, and all the initialized parameter values are 0. When the equipment is started, the digital diagnoses module polls all the SFP ports every 5 seconds, and the value that read first will be evaluated to the maximum, least and average value. Then, if the polling value is larger than the maximum value, refresh it to the larger value; if it is smaller than the least value, refresh the recorded least value, and compute the summation, add 1 on the digit. If SFP is not active when polling, no data record will be refreshed. After 180 polling (15 minutes later), add a row in the period performance monitoring table, and configure the maximum, least and average value of the row's parameter according to current period monitoring table record, cycle type is 15 minutes, then reset all the data in the current period row, and start recording the next cycle. It is the same to record the data of 24 hour cycle. When it reaches

24 hours, add a row in period monitoring table, then reset all the data in the current period row, and start recording the next cycle.

The index of period performance monitoring table of the optical module is port number, cycle type, cycle recording number and parameter type. The monitoring table restores data of two cycles, that is 15 minutes data and 24 hours data. The table is empty originally. Every 15 minutes, a 15 minutes cycle record will be added to the table. The record number of the newest one is 1, larger recording number means older recording. The table keeps at most 96 fifteen minutes record. When it reaches 96 records, the oldest one will be deleted when a new one is added. Every time it reaches 24 hours, a 24 hour cycle record will be added to the table. The newest recording number is 1, at most 1 twenty-four hour cycle record will be restored in the table, and the old record will be covered every 24 hours.

14.2 Optical module digital diagnostic configuration

14.2.1 Optical module digital diagnostic default configuration

Function	Default
Enable/disable digital diagnostic function	Disable digital diagnostic function
Trap Enable / disable send optical module parameters abnormal trap	Allow to send optical module parameters abnormal trap

14.2.2 Optical module digital diagnostic enable/disable configuration

Step	Command	Description
1	config	Enter global configuration mode
2	transceiver digitaldiagnostic <i>{enable/disable}</i>	Enable/disable digital diagnostic function. enable: enable disable: disable
3	exit	Back to privileged mode
4	show interface port <i>[port-list] transceiver detail</i>	Show digital diagnostic information

Note:

When the digital diagnostic functions are configured to disable, the optical module real-time monitoring watch signs is invalid, the table more than the previous threshold parameter value is -1000000, and the rest of parameter values are all 0; the current cycle of performance monitoring for all parameter values in the table is 0; periodic performance monitoring records in the table is cleared, the table is empty.

If the digital diagnostic function is disabled, optical module parameter status is not unusual to send trap.

14.2.3 Optical module parameter abnormal alarm configuration

Step	Command	Description
1	config	Enter global configuration mode
2	snmp trap transceiver <i>{enable/disable}</i>	Enable/disable to send optical module parameter status abnormal trap. <i>enable</i> : enable. <i>disable</i> : disable
3	exit	Back to privileged mode
4	show interface {client/line} transceiver	Show digital diagnostic information

Note:

Configure allowed sending optical module parameters state exception trap, and properly configure the device IP address and SNMP Server circumstances, when the transceiver temperature, the internal supply voltage, bias current, transmit, transmit optical power, received optical power beyond the threshold parameter values To send trap. If digital diagnostic function is disabled, it will not sent trap.

14.2.4 Optical module digital diagnostic parameters monitoring and maintenance

Command	Description
show interface port [port-list] transceiver [threshold-violations] [detail]	Show digital diagnostic information

Chapter 15 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

15.1 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.

15.1.1 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.

15.1.2 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

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.

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.

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.

15.2 CFM Default Configuration List

No.	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.

15.3 CFM Configuration Guide and Limitation

- 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.
- 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.
- To state maintenance domain (MD), the domain name's character string length is 1-16 byte, maintaining level are level 0-7.
- As configure customer service instance s, service instance ID's character string length is 1-16 bytes. Vlan ID is in the range of 1-4094 and Vlan list is also in the range of 1-4094.
- MEP CCM Database's wrong CCM messages archive time is in the range of 1-65535.
- Configure Linktrace Database data archive time is in the range of 1-65535, saved data entries could be in 1-4095.

15.4 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

15.4.1 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 <i>domain-name</i> level <i>level-id</i>	Configure CFM maintain domain, state MD name and level. <i>domain-name</i> : domain name character string in 1-16 bytes; <i>level-id</i> : 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**

15.4.2 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 <i>domain-name level level-id</i>	Configure CFM MD, states MD name and MD level. <i>domain-name</i> : domain name character string length 1-16 bytes; <i>level-id</i> : MD level 0-7
3	service <i>csi-id</i> vlan <i>vlan-id</i>	Configure service illustration name and related VLAN. <i>csi-id</i> : service illustration ID character string, length 1-16 bytes; <i>vlan-id</i> : VLAN ID 1-4094
4	Exit	Return to GLOBAL configure mode.
5	Exit	Return to Privileged EXEC mode.
6	show ethernet cfm domain	Show specific maintenance field 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**

15.4.3 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 <i>port-num</i>	Enter related port. <i>port-num</i> : port number

3	ethernet cfm mip level <i>level-id</i>	In indicated MD, configure MIP, same level as MD. <i>level-id: MD level: 0-7</i>
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)

Raisecom#**config**

Raisecom(config)#**interface port 5**

Raisecom(config-port)#**ethernet cfm mip level 5**

15.4.4 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 <i>port-num</i>	Enter related port <i>port-num</i> : port number
3	ethernet cfm mep level <i>level-id [up] mpid mep-id</i> vlan {all/vlanlist}	In related MD, configure MEP. <i>level-id</i> : MD level: 0-7 <i>mep-id</i> : 1-8191; <i>vlanlist</i> : 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
```

15.4.5 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 <i>{enable/disable} level</i> <i>{all levellist} vlan {all vlanlist}</i>	Enable/disable cc protocol. <i>all</i> : all configure levels; <i>levellist</i> : maintenance domain level list; <i>all</i> : all configured VLAN; <i>vlanlist</i> : 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
```

15.4.6 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 {<i>all</i> <i>levellist</i>} vlan {<i>all</i> <i>vlanlist</i>} interval {<i>1</i> <i>10</i> <i>60</i> <i>600</i>}	Set CCM messages sending interval, can configure <i>all</i> : some indicated level from all service level <i>list</i> : some indicated service instance or indicated level in indicated service with instance CCM messages sending interval. <i>levellist</i> : 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 instance.

```
Raisecom#config
```

```
Raisecom(config)#ethernet cfm cc level 3 vlan 4 interval 60
```

```
Raisecom(config)#exit
```

15.4.7 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 <i>minutes</i>	Configure CCM messages error archive time. <i>minutes</i> : 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.

```
Raisecom#config
```

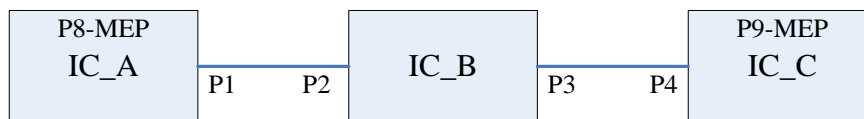
```
Raisecom(config)#ethernet cfm mep archive-hold-time 50
```

Raisecom(config)#exit

15.4.8 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. <i>mac-address</i> : remote MP MAC address, format is HHHH.HHHH.HHH, <i>mep-id</i> : remote MEP ID number(1-8191) . <i>level-id</i> : maintenance domain level: 0-7 <i>vlan-id</i> : VLAN ID1-4094 <i>domain-name</i> : domain name string length 1-16 bytes; <i>Mpid</i> : 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:

- On IC_A, enable CFM protocol: IC_A(config)#**ethernet cfm enable**
- 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**

- On IC_A, enable CC protocol: IC_A(config)#**ethernet cfm cc enable level 3 vlan 4**
- On IC_A port1, configure mode: IC_A(config-port)#**switchport access vlan 4**

- On IC_B, enable CFM protocol: `IC_B(config)#ethernet cfm enable`
- 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`

- On IC_B port 2, 3 configure mode: `IC_B(config-port)#switchport access vlan 4`
- On IC_C, enable CFM protocol: `IC_C(config)#ethernet cfm enable`
- On IC_C enable CC protocol: `IC_C(config)#ethernet cfm cc enable`
- 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`

- 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`

- On C_C port4, configure mode: `IC_C(config-port)#switchport access vlan 4`
- 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.

15.4.9 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 <i>mac-address {domain</i> <i>domain-name / level</i> <i>level-id} vlan vlan-id</i> <i>[source mpid]</i>	Launch Linktrace protocols configure. <i>mac-address</i> : Remote MP's MAC address, format as HHHH.HHHH.HHH; <i>domain-name</i> : domain name character string 1-16 bytes; <i>level-id</i> : maintenance domain <i>level</i> : 0-7 <i>vlan-id</i> : VLAN ID 1-4094 <i>mpid</i> : MEPID

Examples: Topology structure and configurations are same as last section; launch Traceroute Commands in two MEPs which have same MD and MA.

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>
```

15.4.10 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. <i>traceroute</i> : 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
```

15.4.11 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 <i>minutes</i> : database archive time, unit is minute, range in 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
```

15.4.12 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. <i>Entries</i> : 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
```

15.4.13 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 send Macstatus, 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
```

15.4.14 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. <i>enable</i> : enable CFM protocol in GLOBAL mode; <i>disable</i> : 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

```
raisecom#config
```

```
raisecom(config)#ethernet cfm enable
```

```
raisecom(config)#exit
```

15.4.15 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. <i>enable</i> : in GLOBAL mode, enable CFM <i>disable</i> : in GLOBAL mode, disable CFM
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

```
raisecom#config
```

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

```
Raisecom(config-port)#ethernet cfm enable
```

15.5 Monitoring and Maintenance

Commands	Description
show ethernet cfm traceroute-cache	Show LinkTrace database studied route trace information.
show ethernet cfm mp local	Show local MP configure information, include MEP and MIP.
show ethernet cfm errors	Show error CCM database information.
show ethernet cfm domain	Show indicated maintenance domain configuration information.
show ethernet cfm mp remote	Show remote MEP information.
show ethernet cfm mp remote detail	Show remote MEP detail information.
show ethernet cfm	Show 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.
--	--

15.5.1 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: 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 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

15.5.2 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: Show 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

15.5.3 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: 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`

<i>Level</i>	<i>VLAN</i>	<i>MPID</i>	<i>RemoteMEP MAC</i>	<i>ErrorType</i>	<i>AffectedService</i>

1	4	2	CCCC	ErrorCCM	md1-ma4

15.5.4 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: 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

<i>Service</i>	<i>Vlan</i>	<i>CCMInterval</i>
----------------	-------------	--------------------

ma3-1-4	4	10
---------	---	----

In maintenance domain md5-1:

Level: 5

Total services: 0

<i>Service</i>	<i>Vlan</i>	<i>CCMInterval</i>
----------------	-------------	--------------------

15.5.5 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: 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

15.5.6 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:

- [Compulsory] choose to indicate remote MEP's MEP ID or MAC address.
- [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: 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)
```

15.5.7 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

15.5.8 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

15.5.9 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

15.5.10 Clear Indicated Remote MEP Information

Command Format: Clear Ethernet CFM mp remote [domain domain-name | level level-id]

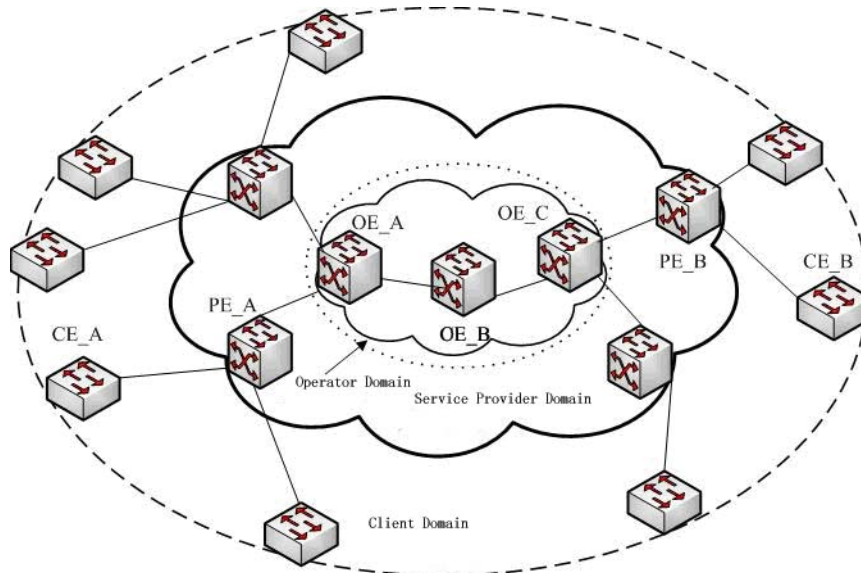
Function: It is used to clear CC database indicated remote MEP information and it also can indicate the MD which needs to be cleared.

Example: Clear remote MEP information in MD named md3-1

Raisecom(config)#clear ethernet cfm mp remote domain md3-1

15.6 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 16 IP Source Guard Configuration

16.1 IP Source Guard principle overview

Without authentication, a way to handle IP address embezzlement is IP source guard. IP source guard can cooperate with DHCP snooping and build up dynamic binding relationship, manually configuring stable binding relationship is also available. DHCP snooping provides a kind of safety feature by creating and maintaining a DHCP binding database to filtrate the unauthentic DHCP messages. It makes sure the validness by starting DHCP snooping. That is to say, all the DHCP OFFER are sent out from DHCP Server, not faked. With this guarantee IP source guard can be used to prevent IP embezzlement.

IP source guard's realization is based on IP source binding table to implement the IP traffic constraint on the port, only the source IP in the binding table is allowed to pass, while others can not.. IP source binding table can be learned dynamically (through DHCP Snooping), or by stable configuration.

The message feature items that IP Source Guard supports include: source IP address, source MAC address, VLAN. The combination of a port and the following feature item is supported:

- ✧ IP
- ✧ IP+MAC
- ✧ IP+VLAN
- ✧ IP+MAC+VLAN

16.2 Configure IP Source Guard

16.2.1 Default IP Source Guard configuration

By default IP Source Guard configuration is as follows:

Feature	State
Stable binding function	disable
Dynamic binding function	disable
Port credit state	no

16.2.2 Enable/disable global stable binding function

By default, IP Source Guard global stable binding function is disabled. When it is disabled, the stable binding relationship don not affect the hardware, and the binding relationship is not available. Only when global stable binding function is enabled can the stable binding relationship take effect.

Step	Command	Description
1	config	Enter global configuration mode
2	ip verify source	Enable static binding function
3	exit	Return to privileged EXEC mode

For example: Raisecom (config) # **ip verify source**

16.2.3 Enable/disable global dynamic binding function

By default, IP Source Guard global dynamic binding function is disabled. When it is disabled, the dynamic binding relationship learned from DHCP SNOOPING module does not affect the hardware, and the binding relationship is not available. Only when global dynamic binding function is enabled can dynamic binding relationship take effect.

Step	Command	Description
1	config	Enter global configuration mode
2	ip verify source dhcp-snooping	Enable dynamic binding function
3	exit	Return to privileged EXEC mode

For example: Raisecom (config) # **ip verify source dhcp-snooping**

16.2.4 Configure port credit state

By default, port is in unauthentic state, when all the IP messages except DHCP message or these according to binding relationship can not be transmitted. When a port is in credible state, all the messages can be transmitted normally. The commands to configure port credit state are as follows:

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	interface port <i>port_id</i>	Enter the figure of one port
3	ip verify source <i>trust</i>	Set the port to credible state
4	no ip verify source <i>trust</i>	Set the port to incredible state
5	exit	Return to global configuration mode
6	exit	Return to privileged EXEC mode

For example:

```
Raisecom(config)# interface port 10
```

```
Raisecom(config-port)# ip verify source trust
```

```
Raisecom(config-port)# no ip verify source trust
```

16.2.5 Configure stable binding relationship

Stable binding relationship can be configured manually, and the static binding relationship can cover the dynamic binding relationship that has the same IP. When the stable binding relationship is deleted manually, the system will recover to the stable binding relationship that has the same IP (if it exists). If the binding relationship that does not exist is deleted, the system will take it as successful operation.

Step	Command	Description
1	config	Enter global configuration mode
2	ip source binding <i>ip-address</i> [<i>mac-address</i>] [vlan <i>vlanid</i>] port <i>port-id</i>	Set stable binding relationship
3	no ip source binding <i>ip-addres</i>	Delete stable binding relationsip
4	exit	Return to privileged EXEC mode

For example:

```
Raisecom(config)# ip source binding 1.2.3.4 port 10
```

```
Raisecom(config)# ip source binding 10.10.1.5 1234.1234.1234 port 10
```

```
Raisecom(config)# ip source binding 100.1.101.50 5678.5678.5678 vlan 100 port 10
```

Raisecom(config)# **no ip source binding** *1.2.3.4*

Raisecom(config)# **no ip source binding** *100.1.101.50*

16.2.6 Transfer dynamic binding relationship to static binding

To transfer dynamic binding relationship to static binding, when deleting static binding relationship by manual, system automatically recover to dynamic binding relationship with identical IP (if there is one).

Step	Command	Description
1	config	Enter global configuration mode
2	ip source binding dhcp-snooping static	Transfer dynamic binding to static binding relationship.
3	no ip source binding <i>ip-address</i>	Delete static binding IP.
4	exit	Return to Privileged EXEC vmode.

Example: Raisecom(config)# **ip source binding dhcp-snooping static**

16.2.7 Enable/disable auto-update to static binding

After enabling this switch, the dynamic binding IP learned by dhcp-snooping will auto-update to static binding.

Step	Command	Description
1	config	Enter global configuration mode
2	[no] ip source binding auto-update	Enable/disable auto-update function.
3	exit	Return to Privileged EXEC vmode.

Example: Raisecom(config)# **ip source binding auto-update**

16.3 Monitoring and maintenance

Use the **show** commands to look over the running state and configuration state of IP Source Guard

for monitoring and maintaining. The **show** commands are shown as follows:

Command	Description
show ip source binding [port port-id]	Show the binding relationship table of the switch
show ip verify source	Show stable/dynamic binding and port credit state

Raisecom#**show ip verify source**

Static Bind: Enable

Dhcp-Snooping Bind: Enable

Port Trust

1 yes

2 no

3 no

4 no

5 no

6 no

7 no

8 no

9 no

10 yes

11 no

12 no

13 no

14 no

15 no

16 no

17 no

18 no

19 no

20 no

21 no

22 no

23 no

24 no

25 no

26 no

27 no

28 no

Raisecom#

Raisecom#show ip source binding*History Max Entry Num: 6**Current Entry Num: 6*

<i>Ip Address</i>	<i>Mac Address</i>	<i>VLAN</i>	<i>Port</i>	<i>Type</i>	<i>Inhw</i>

2.2.2.3	--	--	10	static	no
1.2.3.4	--	--	10	static	no
10.10.1.5	1234.1234.1234	--	10	static	no
100.1.101.50	5678.5678.5678	100	10	static	no
2.3.5.8	--	--	13	static	yes
1.3.5.8	--	10	22	static	yes

Raisecom#

Raisecom#show ip source binding port 10

<i>Ip Address</i>	<i>Mac Address</i>	<i>VLAN</i>	<i>Port</i>	<i>Type</i>	<i>Inhw</i>

2.2.2.3	--	--	10	static	no
1.2.3.4	--	--	10	static	no
10.10.1.5	1234.1234.1234	--	10	static	no
100.1.101.50	5678.5678.5678	100	10	dhcp-snooping	no

Raisecom#

16.4 Typical configuration example

✧ Destination

The switch allow all the IP message passing port 10, and the IP message that is assigned IP as 10.10.10.1 and dynamic binding relationship message learned from dhcp snooping module passing port 3, while only the dynamic binding relationship message learned from dhcp snooping module is allowed to pass other ports.

✧ Configuration step

Raisecom(config)# **ip verify source**Raisecom(config)# **ip verify source dhcp-snooping**Raisecom(config)# **interface port 10**Raisecom(config-port)# **ip verify source trust**

Raisecom(config)# **ip source binding** *10.10.10.1* **port** *3*

16.5 IP Source Guard command list

Command	Description
[no] ip source binding <i>ip-address</i> <i>[mac-address] [vlan vlanid] port port-id</i>	[cancel] the binding based on port
show ip source binding [port <i>port-id</i>]	Show the configured port binding
[no] ip verify source dhcp-snooping	The switch of global dynamic binding function
[no] ip verify source	The switch of stable binding function
[no] ip verify source trust	Bind enable switch in the port
show ip verify source	Show stable/dynamic and port credit state



Chapter 17 Ethernet Ring

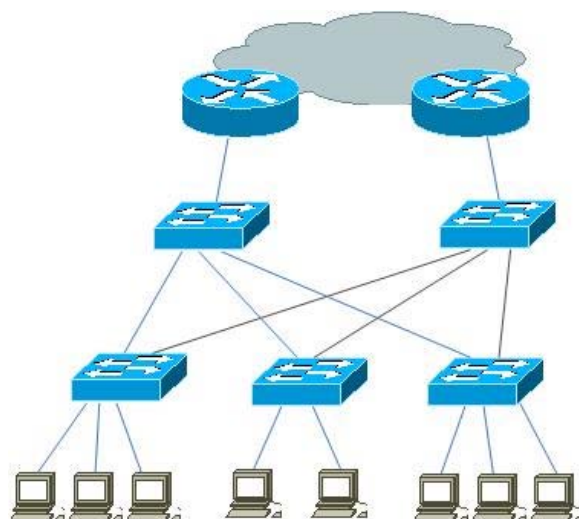
17.1 Overview

Most Ethernet network uses stellate or dual-homed structure. Usually stellate network is used in access layer without protective redundancy, and a single fault of a critical point may lead to network unavailable. Dual-homed network is usually used on or above in the aggregation layer of the network, which supports protective redundancy, but needs doubled equipments and lines and lead to network resource waste. Both the two typical link mode has the inborn limitation on network response time, protection mechanism and multicast.

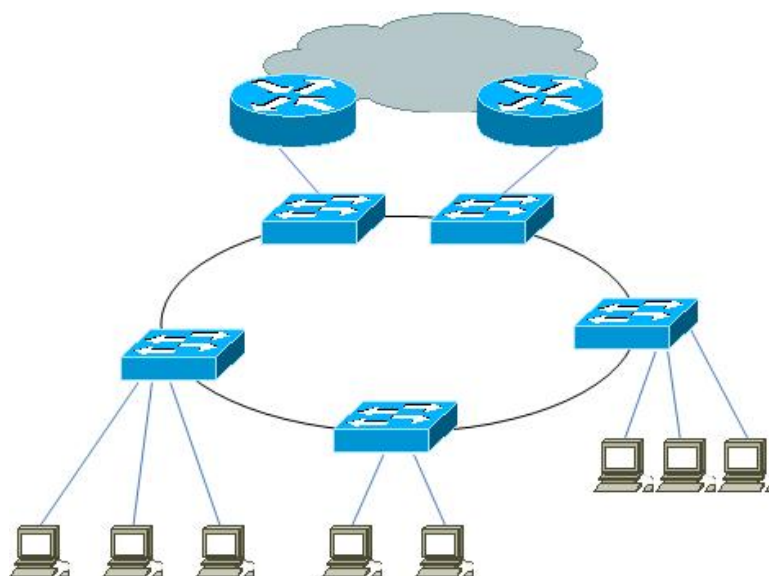
As Ethernet develops to metropolitan area network, voice and video multicast have more need on Ethernet protective redundancy and fault recovery time. The former STP mechanism needs seconds for fault recovery convergence, which is far from metropolitan area network's need on fault recovery.

Ethernet ring technology is a solution to the problem mentioned above. As a metropolitan Ethernet technology, Ethernet ring helps traditional data network from the problems like poor protection ability and long fault recovery time, and it provides 50ms rapid protection in theory. At the same time, it is compatible to typical Ethernet protocols. It's an important technology and solution to MAN access network optimization and improvement.

Raisecom Ethernet ring technology uses self-developed protocol and simple configuration, realize the function like removing loop, fault protection switching and automatic fault recovery, and the fault switching time is less than 50ms.



Dual-homed network topology



Ring network topology

17.2 Default Ethernet ring configuration list

Function	Default value
Hello message sending interval	1s
Fault recovery delay time	5s
Bridge priority	1
Ring description	Ethernet ring X

Ring port holdtime	15s
Ring protocol message	2

Note: To all the equipments on a ring, it is suggested to configure the values of the parameters above to the same.

17.3 Configure Ethernet ring

17.3.1 Create and delete ring

Step	Command	Description
1	config	Enter global configuration mode
2	interface port primaryport	Enter primary port mode
3	ethernet ring <1-8> secondaryport	Create ring and configure the corresponding ring port
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show ethernet ring	Show ring configuration
7	config	Enter global configuration
8	interface port secondaryport	Enter secondary port mode
9	no ethernet ring <1-8>	Delete ring

Note: You can delete Ethernet ring in both primary port mode and secondary mode.

17.3.2 Configure global switch and ring switch

By default, global switch and ring switch is disabled.

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet ring X enable	Enable ring switch
3	show ethernet ring	Show ring configuration information

17.3.3 Configure Hello message sending interval

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet ring X hello-time 5	Configure Ethernet ring hello time.
3	exit	Quit from global configuration mode and enter privileged EXEC mode
4	show ethernet ring	Show Ethernet ring information

17.3.4 Configure fault-delay

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet ring X restore-delay 10	Configure Ethernet ring restore delay
3	exit	Quit from global configuration and enter privileged EXEC mode
4	show ethernet ring	Show Ethernet ring information

17.3.5 Configure bridge priority information

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet ring X priority 3	Configure Ethernet ring bridge priority
3	exit	Quit from global configuration mode and enter privileged EXEC mode
4	show ethernet ring	Show Ethernet ring information

17.3.6 Configuration ring description information

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet ring X description <i><word></i>	Configure Ethernet ring description information
3	exit	Quit from global configuration mode and enter privileged EXEC mode
4	show ethernet ring	Show Ethernet ring information

17.3.7 Configure ring port holdtime

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet ring X hold-time <i><3-100></i>	Configure Ethernet ring port holdtime
3	exit	Quit from global configuration mode and enter privileged EXEC mode
4	show ethernet ring	Show Ethernet ring information

17.3.8 Configure ring protocol VLAN

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet ring X protocol-vlan <i><2-4094></i>	Configure Ethernet ring protocol VLAN
3	exit	Quit from global configuration mode and enter privileged EXEC mode
4	show ethernet ring	Show Ethernet ring information

17.3.9 Clear ring port static.

Step	Command	Description
1	config	Enter global configuration mode
2	clear ethernet ring X statistics	Clear ring port static.
3	exit	Quit global configuration mode and enter privileged EXEC mode
4	show ethernet ring port statistic	Show Ethernet ring port message static.

17.3.10 upstream-group

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet ring upstream-group {1-10}	Configure upstream-group.
3	exit	Quit global configuration mode and enter privileged EXEC mode
4	show ethernet ring	Show Ethernet ring information.

Note:

- The upstream-group must combine the fault-pass number, to support the application of double attribution topological
- The upstream-group number corresponds to fault-pass number

17.4 Monitoring and maintenance

Use **show** to show the configuration and running state of Ethernet ring. Related commands are shown below:

Command	Description
show ethernet ring [ringID]	Show all/designated Ethernet ring information
show ethernet ring [ringID] port	Show all/designated Ethernet ring port information

show ethernet ring port statistic

Show ring port message static.

17.4.1 Ethernet ring information monitoring

Use **show ethernet ring** to show the priority of Ethernet ring, hello time and fault recovery delay time, you can also check out local node state and nodes state, main node information (red means the option can be configured). Specified configuration is shown below:

Raisecom# **show ethernet ring** *RingId*

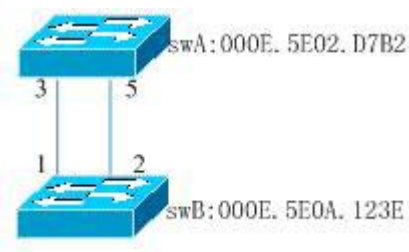
```

Ethernet Ring Upstream-Group:1
Ethernet Ring 1:
Ring Admin:      Enable
Ring State:      Unenclosed
Bridge State:     Down
Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds
Bridge Priority:  1
Bridge MAC:       000E.5E03.5B81
Ring DB State:    Down
Ring DB Priority:  1
Ring DB:          000E.5E03.5B81
Hello Time:       1
Restore delay:    5
Hold Time:        15
Protocol Vlan:    2

```

17.4.2 Ethernet ring port information monitoring

User can use **show Ethernet ring port** to show Ethernet ring port information, including ring port, the actual effected ring port number and ring equipment list.



Single ring topology

In the figure above, two equipments forms a ring network, on swA ring network port it is shown:

swA#show Ethernet ring port

<default Ethernet ring description, by default it is Ethernet ring X>

Ethernet Ring 1:

Primary Port: 3
State: Block
Port Active State: Active
State: Block
Peer State: None
Switch counts: 5
Current state duration: 0 days, 3 hours, 32 minutes, 33 seconds
Peer Ring Node:
 --1:000E.5E0A.123E:2—

Secondary Port: 5
State: Block
Port Active State: Active
State: Forward
Peer State: None
Switch counts: 6
Current state duration: 0 days, 3 hours, 32 minutes, 37 seconds
Peer Ring Node:
 --2:000E.5E0A.123E:1--

swA#show ethernet ring port statistics

<default Ethernet ring description, by default it is Ethernet ring X>

Primary Port: 3
Receive hello packets: XX
Receive change packets: XX
Receive change relay packets: XX
Receive flush packets: XX
Send hello packets: XX
Send change packets: XX
Send change relay packets: XX
Send flush packets: XX

Secondary Port: 5
Receive hello packets: XX
Receive change packets: XX
Receive change relay packets: XX
Receive flush packets: XX
Send hello packets: XX
Send change packets: XX
Send change relay packets: XX

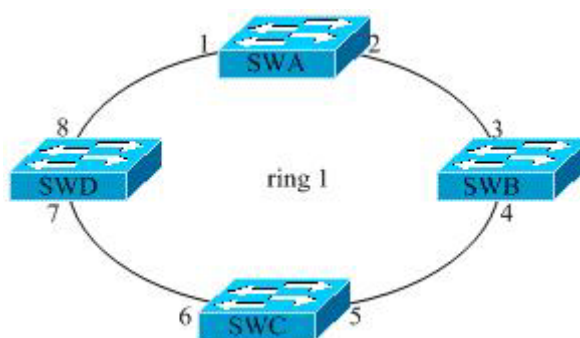
Send flush packets: XX

17.5 Typical application

17.5.1 Ethernet ring Typical application

Raisecom Ethernet ring itself can be used in single-ring or double E-ring tangent network.

17.5.2 Single E-ring Configuration



Single E-ring

As above, four switches are added in ring 1 with Mac addresses: SWA (000E.5E00.000A), SWB (000E.5E00.000B), SWC (000E.5E00.000C), and SWD (000E.5E00.000D).

Configuration Steps

SWA

SWA#config

SWA(config)#interface port 1

SWA(config-port)#ethernet ring 1 2

SWA(config)#ethernet ring 1 enable

SWB

SWB#config

SWB(config)#interface port 3

SWB(config-port)#ethernet ring 1 4

SWB(config)#**ethernet ring 1 enable**

SWC

SWC#**config**

SWC(config)#**interface port 5**

SWC(config-port)#**ethernet ring 1 6**

SWC(config)#**ethernet ring 1 enable**

SWD

SWD#**config**

SWD(config)#**interface port 7**

SWD(config-port)#**ethernet ring 1 8**

SWD(config)#**ethernet ring 1 enable**

Normal ring status

If the ring is normal, first ring port of master node SWD: port 7 is blocked, to dismiss data ring loop.

SWD and SWB status:

SWD

SWD# **show ethernet ring**

Ethernet Ring Upstream-Group:1

Ethernet Ring 1:

Ring Admin: Enable

Ring State: Enclosed

Bridge State: Block

Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds

Bridge Priority: 1

Bridge MAC: 000E.5E00.000D

Ring DB State: Block

Ring DB Priority: 1

Ring DB: 000E.5E00.000D

Hello Time: 1

Restore delay: 5

Hold Time: 15

Protocol Vlan: 2

SWD#show ethernet ring port*Ethernet Ring 1:**Primary Port:* 7*State:* Block*Port Active State:* Active*Peer State:* Full*Switch counts:* 5*Current state duration:* 0 days, 3 hours, 32 minutes, 33 seconds*Peer Ring Node:**--6:000E.5E00.000C:5--**--4:000E.5E00.000B:3--**--2:000E.5E00.000A:1--**Secondary Port:* 8*State:* Block*Port Active State:* Active*Peer State:* Full*Switch counts:* 6*Current state duration:* 0 days, 3 hours, 32 minutes, 37 seconds*Peer Ring Node:**--1:000E.5E00.000A:2--**--3:000E.5E00.000B:4--**--5:000E.5E00.000C:6—***SWD#show ethernet ring port statistic***Primary Port:* 7*Receive hello packets:* xx*Receive change packets:* xx*Receive change relay packets:* xx*Receive flush packets:* xx*Send hello packets:* xx*Send change packets:* xx*Send change relay packets:* xx*Send flush packets:* xx*Secondary Port:* 8*Receive hello packets:* xx*Receive change packets:* xx*Receive change relay packets:* xx*Receive flush packets:* xx*Send hello packets:* xx*Send change packets:* xx

Send change relay packets: *xx*
Send flush packets: *xx*

SWB

SWB# show ethernet ring

Ethernet Ring Upstream-Group:1
Ethernet Ring 1:
Ring Admin: *Enable*
Ring State: *Enclosed*
Bridge State: *Two-Forward*
Ring state duration: *0 days, 3 hours, 30 minutes, 15 seconds*
Bridge Priority: *1*
Bridge MAC: *000E.5E00.000B*
Ring DB State: *Block*
Ring DB Priority: *1*
Ring DB: *000E.5E00.000D*
Hello Time: *1*
Restore delay: *5*
Hold Time: *15*
Protocol Vlan: *2*

SWB#show ethernet ring port

Ethernet Ring 1:
Primary Port: *3*
State: *Forward*
Port Active State: *Active*
Peer State: *Full*
Switch counts: *5*
Current state duration: *0 days, 3 hours, 32 minutes, 33 seconds*
Peer Ring Node:
--2:000E.5E00.000A:1--
--8:000E.5E00.000D:7--
--6:000E.5E00.000C:5--

Secondary Port: *4*
State: *Forward*
Port Active State: *Active*
Peer State: *Full*
Switch counts: *6*
Current state duration: *0 days, 3 hours, 32 minutes, 37 seconds*

Peer Ring Node:

--5:000E.5E00.000C:6--

--7:000E.5E00.000D:8--

--1:000E.5E00.000A:2—

SWB#show ethernet ring port statistic

Primary Port: 3

Receive hello packets: xx

Receive change packets: xx

Receive change relay packets: xx

Receive flush packets: xx

Send hello packets: xx

Send change packets: xx

Send change relay packets: xx

Send flush packets: xx

Secondary Port: 4

Receive hello packets: xx

Receive change packets: xx

Receive change relay packets: xx

Receive flush packets: xx

Send hello packets: xx

Send change packets: xx

Send change relay packets: xx

Send flush packets: xx

Ring status after link switch

If there is a link fault between SWA and SWB, SWD port 7 will change its **block** status into **forwarding** status, SWB port 3 is going to change **forwarding** status into **block** status.

SWD

SWD# show ethernet ring

Ethernet Ring Upstream-Group:1

Ethernet Ring 1:

Ring Admin: Enable

Ring State: Unenclosed

Bridge State: Two-Forward

Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds

Bridge Priority: 1

Bridge MAC: 000E.5E00.000D

Ring DB State: *Block*
Ring DB Priority: *1*
Ring DB: *000E.5E00.000B*
Hello Time: *1*
Restore delay: *15*
Hold Time: *15*
Protocol Vlan: *2*

SWD#show ethernet ring port

Ethernet Ring 1:
Primary Port: *7*
State: *Forward*
Port Active State: *Active*
Peer State: *Full*
Switch counts: *5*
Current state duration: *0 days, 3 hours, 32 minutes, 33 seconds*
Peer Ring Node:
--6:000E.5E00.000C:5--
--4:000E.5E00.000B:3--

Secondary Port: *8*
State: *Block*
Port Active State: *Active*
Peer State: *Full*
Switch counts: *6*
Current state duration: *0 days, 3 hours, 32 minutes, 37 seconds*
Peer Ring Node:
--1:000E.5E00.000A:2--

SWB

SWB# show ethernet ring

Ethernet Ring Upstream-Group:1
Ethernet Ring 1:
Ring Admin: *Enable*
Ring State: *Unenclosed*
Bridge State: *Block*
Ring state duration: *0 days, 3 hours, 30 minutes, 15 seconds*
Bridge Priority: *1*
Bridge MAC: *000E.5E00.000B*
Ring DB State: *Block*
Ring DB Priority: *1*

Ring DB: 000E.5E00.000B
Hello Time: 1
Restore delay: 15
Hold Time: 15
Protocol Vlan: 2

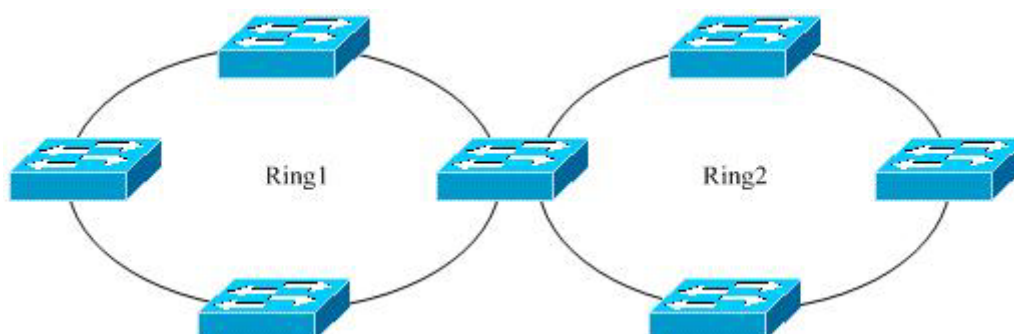
SWB#show ethernet ring port

Ethernet Ring 1:
Primary Port: 3
State: Block
Port Active State: Active
Peer State: Full
Switch counts: 5
Current state duration: 0 days, 3 hours, 32 minutes, 33 seconds
Peer Ring Node:

Secondary Port: 4
State: Forward
Port Active State: Active
Peer State: Full
Switch counts: 6
Current state duration: 0 days, 3 hours, 32 minutes, 37 seconds
Peer Ring Node:

--5:000E.5E00.000C:6--
 --7:000E.5E00.000D:8--
 --1:000E.5E00.000A:2--

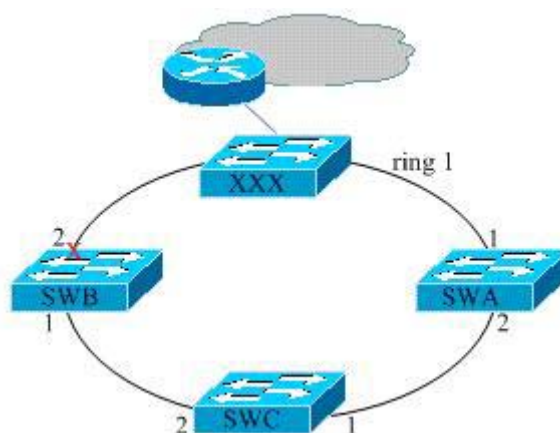
17.5.3 Double E-ring



Double/multi E-ring topology

Double E-ring is formed by two E-rings. Thus the configuration in each ring is same as single-ring.

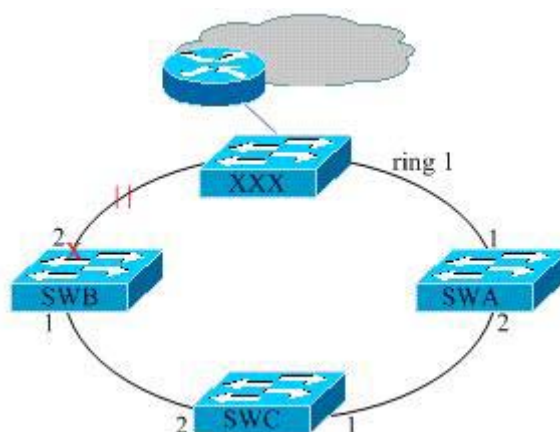
17.5.4 Non-Raisecom Uplink Device

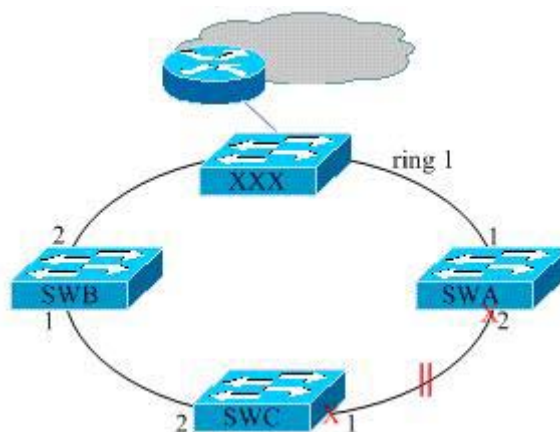
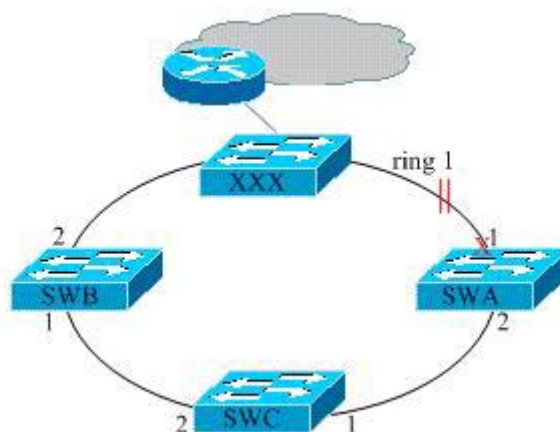


As above, ring 1 is formed by SWA, SWB, SWC, and XXX, which Switch XXX does not use Raisecom E-ring protocol. Mac addresses: SWA (000E.5E00.000A), SWB (000E.5E00.000B), SWC (000E.5E00.000C).

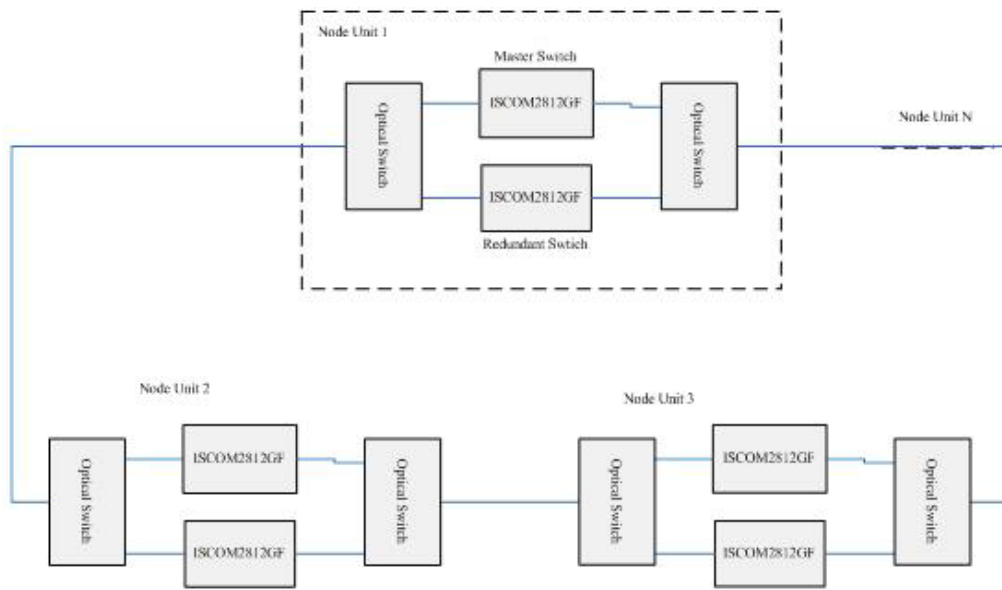
Normally, ring 1 is blocked at SWB port 2 because port 2 could not discover its neighbor and SWB Mac address is bigger than SWA Mac address. There is no loopback in ring 1.

Possible abnormal situations may happen are shown as below, X represents port block, || represents link fault.





17.5.5 Ring Double-link Protection

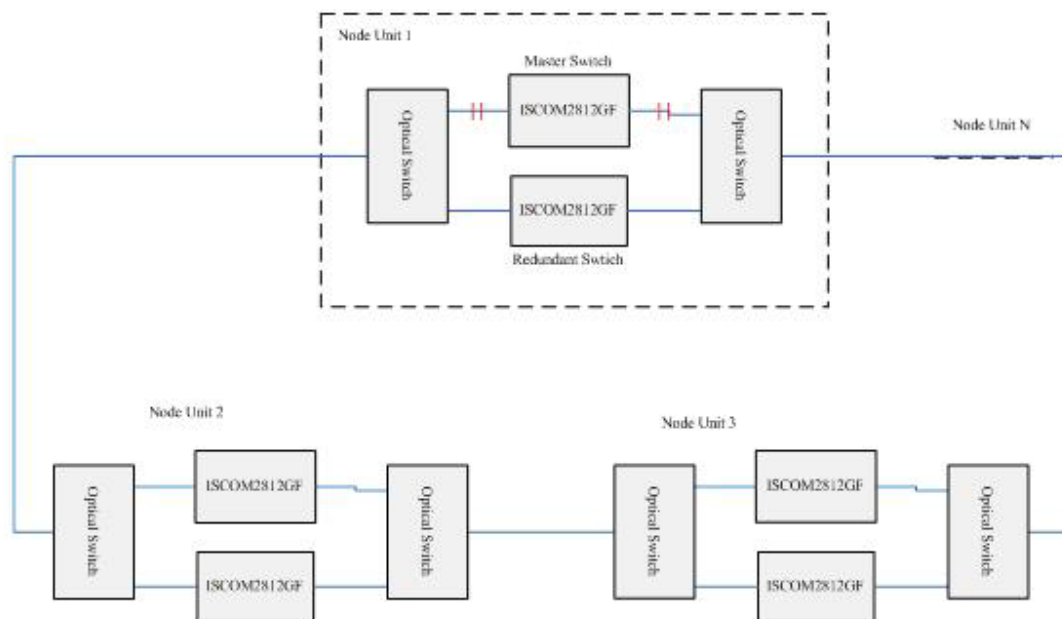


We can consider all three Node Units are in one ring. When there is power fault in Node Unit 1, optical Switch will detect the optical signal changing and informs Node Unit 2. The redundant switch is switched on.

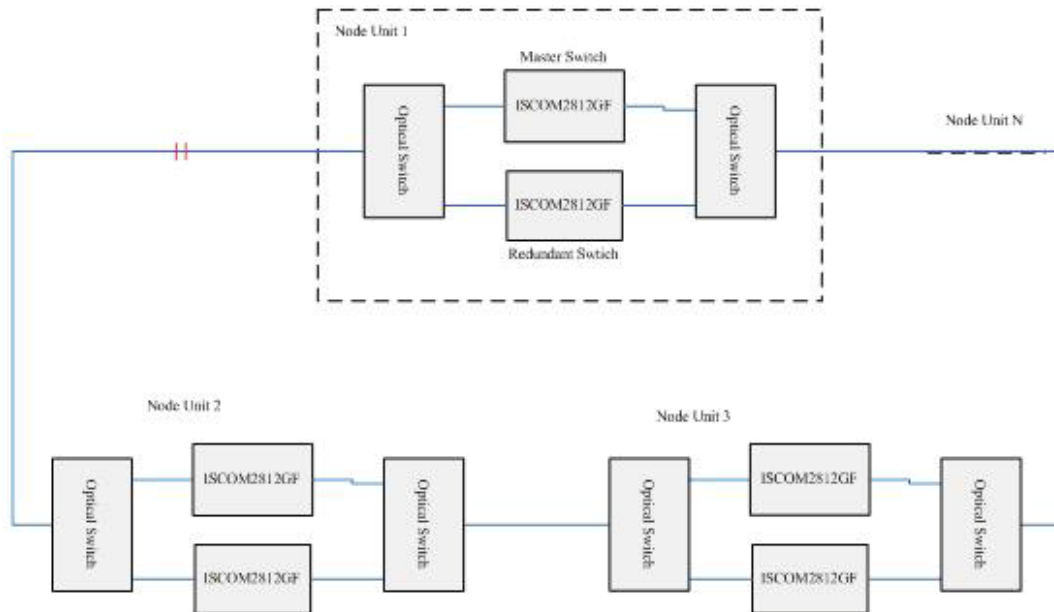
In this application, we use optical switch and ISCOM switches to achieve fault fast switch and link redundancy. This case is mainly used in more safety areas as Power factory, banks, etc.

Note: If link is ok, optical switches should be connected to master switch for communication.

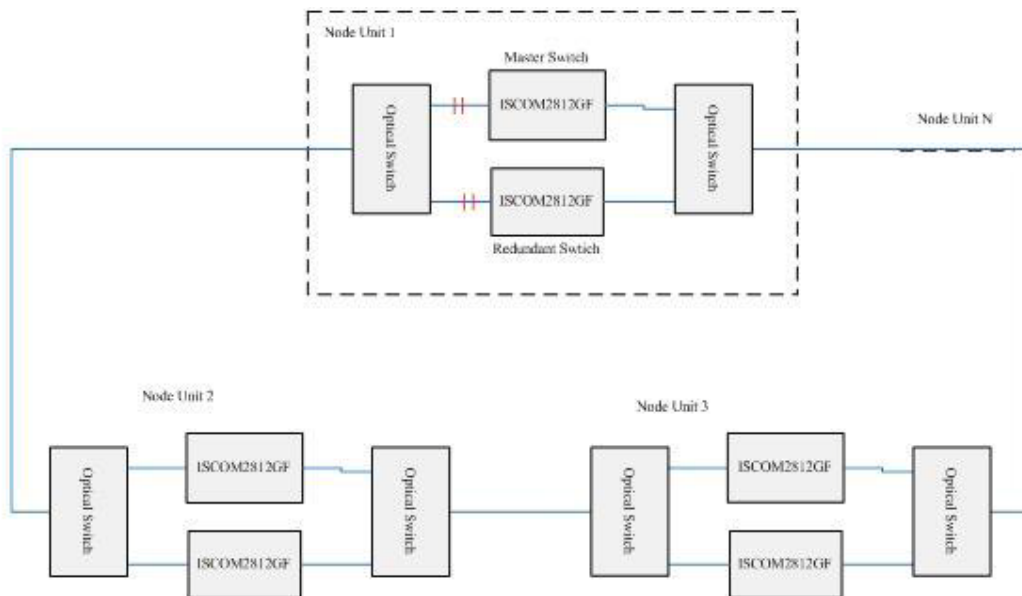
Figures below shows different fault situations:



Where there is link fault at Master switch, optical switch can detect optical signal in DOWN event and switch link to redundant switch for communication.

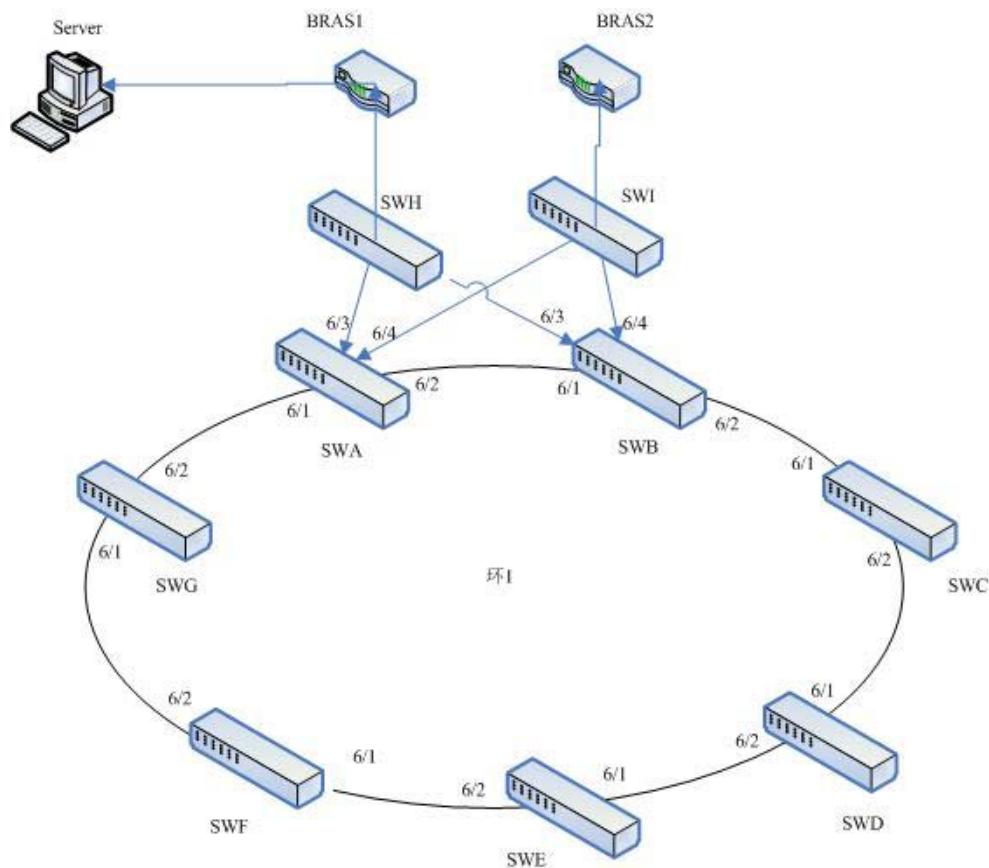


If there is link fault between Node Units, as figure above, Node Unit 1 is informed to unblock its redundant switch for communication.



If there is link fault in both master and redundant switches, the ring is in uncompleted status. Node Unit 1 will open the unblock port for communication.

17.5.6 Double attribution topology



SWA ~ SWG (OLT) compose ring 1, unlinked SWI and SWH. Enable port backup on SWI and SWH, set restore-delay for 0; compared with SWC ~ SWG, SWA and SWB ont only open Ethernet ring, but also configure fault-pass group and Ethernet ring upstream-group;

Configuration Steps:

SWA

SWA#config

SWA(config)#interface port 1

SWA(config-port)#ethernet ring 1 2

SWA(config)#ethernet ring 1 enable

SWA(config)#link-state-track group 1

SWA(config)#link-state-track group 2

SWA(config)#interface port 3

SWA(config-port)#link-state-group 1 upstream

SWA(config-port)#switchport trunk allowed vlan 1-100

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

SWA(config)#**interface port 4**

SWA(config-port)#**link-state-group 2 upstream**

SWA(config-port)#**switchport trunk allowed vlan 101-200**

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

SWA(config)#**ethernet ring upstream 1,2**

SWH

SWB#**config**

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

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

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

SWB(config)#**switchport backup restore-delay 0**

SWC

SWC#**config**

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

SWC(config-port)#**ethernet ring 1 2**

SWC(config)#**ethernet ring 1 enable**

Other equipment steps are similar, so not do in detail.

The network can not only realize the load sharing, which vlan1-100 and vlan101-200 respectively take different uplink equipment SWH and SWI; but also has a mutual backup. Then when SWI or SWH is at fault, related service can smooth switch to another one.

Chapter 18 TACACS+

This chapter introduces how to configure TACACS+ on switches and the contents are:

- ✧ TACACS+ Overview
- ✧ TACACS+ Function Configuration
- ✧ TACACS+ Monitoring and Maintenance

18.1 TACACS+ Theory

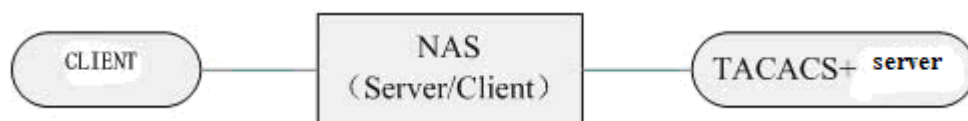
TACACS was developed by BBN for MEILNET as a simple control protocol based on UDP; Cisco has improved several times on it, so called XTACACS; TACACS+ is newest version of TACACS. Now, there are three versions of TACACS, and the third version TACACS+ is not compatible with the old two versions.

TACACS+ is the newest version of TACACS and compare with old versions, it has certain improvements:

- It separates authentication, authorization and fee service;
- It encrypts all data (except message head) between NAS and server instead of only adding password.
- It is based on TCP, unlike the old version are based on UDP. Tacacs+'s port number is 49.

TACACS+ provide access control service for router, network access server and other network process devices through one or more central servers. TACACS+ can provide separately authentication, authorization and fee service.

Figure 1-1 shows the relation among clients, NAS and TACACS+ server. We can say AAA application which runs on NAS is the server end to client; however, we also can say that AAA application is client end to TACACS+ server; TACACS+ protocol describes the telecommunication mechanism between NAS and TACACS+ server.



Client, NAS and TACACS+ server

18.2 TACACS+ Function Configuration

18.2.1 TACACS+ Function Default Configuration

In default, switch is not configured tacacs+ authorization server address and shared key. Client login mode and enable login mode are both set as local-user.

18.2.2 TACACS+ function configuration

1. Configure tacacs+ server address and shared key:

Steps	Commands	Description
1	tacacs-server <i>A.B.C.D</i>	Configure tacacs+ server address
2	tacacs-server key <i>WORD</i>	Configure tacacs+ shared key
3	show tacacs-server	Display tacacs+ server address, shared key and authentication message statistics.

Correspondingly, we also can use *no Commands* to cancel tacacs+ server and shared key configuration:

Steps	Commands	Description
1	no tacacs-server	Remove tacacs+ authentication server address
2	no tacacs-server key	Remove tacacs+ shared key

2. Configure client login mode

Commands	Description
user login { <i>local-radius</i> / <i>local-user</i> / <i>radius-local</i> [<i>server-no-response</i>] / <i>radius-user</i> / <i>tacacs-user</i> / <i>tacacs-local</i> [<i>server-no-response</i>] / <i>local-tacacs</i> }	Configure client login mode
enable login { <i>local-radius</i> / <i>local-user</i> / <i>radius-local</i> [<i>server-no-response</i>] / <i>radius-user</i> / <i>tacacs-user</i> / <i>tacacs-local</i> [<i>server-no-response</i>] / <i>local-tacacs</i> }	Configure enable login mode

18.2.3 Monitoring and Maintenance

We can check switch tacacs+ server address, shared key and authentication message statistics by using *show Commands*. That makes it easy to monitor and maintenance. Show command is:

Commands	Description
show tacacs-server	Display tacacs+ server address, shared key and authentication message statistics.

18.2.4 Basic Configuration Example

Suppose that Tacacs+ server address is 192.168.0.100; shared key is set as 123; client name and password are individually set as *test* and *test* in tacacs+ server. Configuring steps are:

```
Raisecom#tacacs-server 192.168.0.100
```

```
Raisecom#tacacs-server key 123
```

```
Raisecom#user login tacacs-local
```

Chapter 19 SLA Configuration

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

19.1 SLA 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.

19.1.1 SLA modules

➤ Task

Static concept, it is an end-to-end SLA network performance test task, including layer-2 network delay/jitter test (y1731-echo / y1731-jitter) and layer-3 network delay/jitter test (icmp-echo / icmp-jitter).

➤ Exploration

Dynamic concept, it is used to describe the process of an exploration message being sent and received in task test.

➤ Test

Dynamic concept, it is used to describe 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).

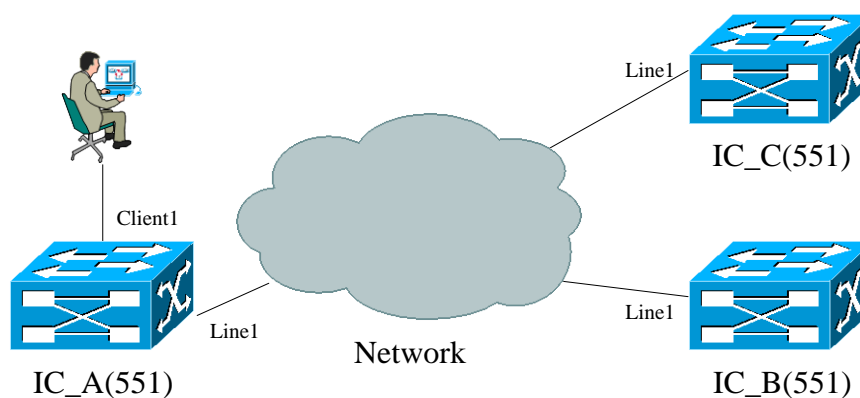
➤ Schedule

Dynamic concept, it is used to describe a schedule of one task, a schedule may contain several seasonal test execution.

19.1.2 Basic SLA function

SLA module is mainly used to measure network performance and take the result as the basic for user performance guarantee. Therefore, choosing two checking points (source and destination switch), configure SLA on one and schedule to run it, then user can detect network performance between the two points.

The basic topology shows as below. If IC_A and IC_B is the same user located at different position, and user want to know the network performance between these two points. Then user configures SLA on IC_A with destination IC_B, to operate SLA performance test by scheduling and get statistic result. The upper layer application software (NMS) can statis tic data through SLA module, test out packets dropping ratio between IC_A and IC_B, bi-directional or uni-directional (SD/DS) delay, jitter, jitter variance, jitter distribution, etc. and then perform network performance analysis to get data user want to see.



Topology of SLA Application

19.2 SLA default configuration list

No.	Attribute	Default value
-----	-----------	---------------

1	SLA lay-2 service level	Service level is level 0 (the highest).
2	SLA jitter detecting time interval	Detecting interval is 20ms.
3	SLA jitter detecting packets number	Detecting packets number is 10.
4	SLA schedule subsistence period.	Schedule period is forever (always in schedule status).
5	SLA schedule test period.	Test period is 20s.

19.3 SLA configuration guide and limit

- Layer-2 SLA operation schedule requires CFM environment (refer to CFM Configuration Guide for related description of CFM).
- It is suggested to set CFM packets transmitting interval in 1S to improve layer-2 operation executing accuracy. If transmitting interval is set long, it cannot reflect remote change in time and affect network performance detection.
- Max. configuration items of sla operation is 100, after configuring the basic information of one operation (identified by operation ID), users cannot modify or configure it again. Delete the operatio before modifying basic information of it.
- Max. concurrent schedule for sla operation is 10 pieces. One operation cannot be modified or schedule again before stopping it. User must wait the schedule to stop (reach schedule exist period or schedule halt) for the next time schedule.
- Statistic information of one operation is at most 5 groups. If it over 5 groups, the oldest statistic information (take the starting time of schedule as benchmark) will be got aging.

19.4 SLA configuration list and instruction

- Configure basic information for SLA operation
 - Configure SLA y1731-echo
 - Configure SLA y1731-jitter
 - Configure SLA icmp-echo
 - Configure SLA icmp-jitter
- Configure SLA schedule information and enable schedule

19.4.1 Configure SLA y1731-echo

Delete sla: **no sla oper-num.**

Steps	Commands	Description
1	config	Enter global configuration mode
2	sla <i>oper-num</i> y1731-echo remote-mep <i>mep-id</i> level <i>level-id</i> svlan <i>vlan-id</i> [cvlan <i>vlan-id</i>][cos <i>cos-id</i>]	Configure basic information for y1731-echo. <i>oper-num</i> : ID of sla operation, range in 1-65535. <i>mep-id</i> : remote mep, range in 1-8191. <i>level-id</i> : MD level, range in 0-7. <i>vlan-id</i> : vlan ID, range in 1- 4094. <i>cos-id</i> : service level, range in 0-7.
3	exit	Return to Privileged EXEC mode.
4	show sla {all oper-num } configuration	Show configuration information related to sla operation.

Example: Configure y1731-echo, operation ID is 2, remote mep is 2, MD level is 3, vlan id is 4, and service level is 1.

Raisecom#**config**

Raisecom (config)# **sla 2 y1731-echo remote-mep 2 level 3 svlan 4 cvlan 2 cos 1**

Raisecom (config)#**exit**

19.4.2 Configure SLA y1731-jitter

Delete sla: **no sla oper-num**.

Steps	Commands	Description
1	config	Enter global configuration mode
2	sla <i>oper-num</i> y1731-jitter remote-mep <i>mep-id</i> level <i>level-id</i> svlan <i>vlan-id</i> [cvlan <i>vlan-id</i>][interval <i>interval-time</i>][packets <i>packets-num</i>][cos <i>cos-id</i>]	Configure basic information for SLA y1731-jitter. <i>oper-num</i> : ID of sla operation, range in 1-65535. <i>mep-id</i> : remote mep, range in 1-8191. <i>vlan-id</i> : vlan ID, range in 1-4094. <i>interval-time</i> : detecting time interval, range in 1- 6000 ms. <i>packets-num</i> : detecting packets number, range in 1-20. <i>cos-id</i> : service level, range in 0-7.
3	exit	Return to Privileged EXEC mode.
4	show sla {all oper-num } configuration	Show configuration information related to sla operation.

Example: Configure y1731-jitter, operation ID is 2, remote mep is 2, MD level is 3, vlan id is 4,

probe detecting interval is 10ms, detecting packets number is 10, and service level is 1.

Raisecom#**config**

Raisecom (config)# **sla 2 y1731-jitter remote-mep 2 level 3 svlan 4 cvlan 2 interval 10 packets 10 cos 1**

Raisecom (config)#**exit**

19.4.3 Configure SLA icmp-echo

Delete sla: **no sla oper-num**.

Steps	Commands	Description
1	config	Enter global configuration mode
2	sla oper-num icmp-echo ip-address	Configure basic information for SLA icmp-echo. <i>oper-num</i> : operation ID of sla, range in 1-65535. <i>ip-address</i> : destination IP address, format in XXX.XXX.XXX.XXX.
3	exit	Return to Privileged EXEC mode.
4	show sla {all oper-num } configuration	Show configuration information related to sla operation.

Example: Configure icmp-echo, operation ID is 2, destination IP address is 20.0.0.20.

Raisecom#**config**

Raisecom (config)#**sla 2 icmp-echo dest-ipaddr 20.0.0.20**

Raisecom (config)#**exit**

19.4.4 Configure SLA icmp-jitter

Delete sla: **no sla oper-num**.

Steps	Commands	Description
1	config	Enter global configuration mode
2	sla oper-num icmp-jitter ip-address [interval interval-time] [packets	Configure basic information for SLA icmp-jitter. <i>oper-num</i> : operation ID of sla, range in 1-65535. <i>ip-address</i> : destination IP address, format in

	<i>packets-nums]</i>	XXX.XXX.XXX.XXX. <i>interval-time</i> : detecting time interval, range in 1-60000 ms. <i>packets-num</i> : detecting packets number, range in 1-20.
3	exit	Return to Privileged EXEC mode.
4	show sla {all oper-num } configuration	Show configuration information related to sla operation.

Example: Configure icmp-jitter, operation ID is 2, destination IP address is 20.0.0.20, detecting time interval is 10s, packets number is 5.

Raisecom#**config**

Raisecom (config)#**sla 2 icmp-jitter dest-ipaddr 20.0.0.20 interval 10 packets 5**

Raisecom (config)#**exit**

19.4.5 Configure SLA schedule information and enable schedule

Make sure the basic information has been configured when user performs sla operation schedule.

Use this command to stop sla operation schedule: **no sla schedule oper-num**.

There is no keyword begin in schedule command, which means immediate performing schedule operation and the command is not saved in auto-configuration loading.

Steps	Commands	Description
1	config	Enter global configuration mode
2	sla schedule oper-num [life {forever life-time}] [period period-time]	Configure information for SLA schedule and enable sla operation schedule. <i>oper-num</i> : operation ID of sla, range in 1-65535. forever : always in schedule state; <i>life-time</i> : schedule period, range in 1- 604800s. <i>period-time</i> : test period, range in 1-604800s.
3	exit	Return to Privileged EXEC mode.
4	show sla {all oper-num } result	Show test information of the latest operation.
5	show sla {all oper-num } statistic	Show statistic information of operation schedule.

Example: Schedule information of sla operation 2, life time is 20s, period time is 10s, enable schedule.

Raisecom#**config**

Raisecom (config)#**sla schedule 2 life 20 period 10**

Raisecom (config)#**exit**

NOTE:

- The meaning of keyword **begin** in schedule command: this command is only used for auto-load, doesn't schedule operation.
- No keyword of **begin** in the command: the command is for schedule operation, doesn't save in auto-loading.
- It is suggested to set CFM packet transmitting in interval of 1S to improve accuracy of layer-2 operation execution. The longer transmitting interval cannot reflect remote change in time and may affect network performance detection.

19.4.6 Configure auto-load SLA schedule

Configure the switch auto-load schedule command when starting up by the command of **sla schedule oper-num begin**.

Delete a schedule command from auto-loading: **no sla schedule oper-num begin**.

Steps	Commands	Description
1	config	Enter global configuration mode
2	sla schedule oper-num [life {forever life-time}] [period period-time] begin	Configure information for SLA schedule and enable sla operation schedule. <i>oper-num</i> : operation ID of sla, range in 1-65535. forever : always in schedule state; <i>life-time</i> : schedule period, range in 1- 604800s. <i>period-time</i> : test period, range in 1-604800s. begin : used for auto-loading.
3	exit	Return to Privileged EXEC mode.
4	show running-config	Show command in operation auto-loading.
6	write	Write auto-loading information into auto-loading file.

Example: Schedule SLA operation 2 when starting up the switch, life time is 20s, test period is 10s, enable schedule.

Raisecom#**config**

Raisecom (config)#**sla schedule 2 life 20 period 10 begin**

Raisecom (config)#**exit**

Raisecom# **write**

Delete auto-loading:

Raisecom (config)#**no sla schedule 2 begin**

NOTE:

- The meaning of keyword begin in schedule command: this command is only used for auto-load, doesn't schedule operation.
- No keyword of begin in the command: the command is for schedule operation, doesn't save in auto-loading.

19.5 Monitoring and maintenance

Command	Description
show sla {all oper-num } configuration	Show configuration information related to operation.
show sla {all oper-num } result	Show the latest test information of operation.
show sla {all oper-num } statistic	Show statistic information of operation schedule.

19.5.1 Show configuration information related to operation

Command Format: show sla {all | oper-num } configuration

Function: to show basic configuration information of sla operation and schedule information.

Show result:

1). Configure icmp-jitter, operation ID is 2, destination IP address is 11.0.0.20, detecting time interval is 10s, packets number is 5. At present operation 2 doesn't enable schedule.

IC_A# **show sla 2 configuration**

Operation <2>:

Type: icmp jitter

StartTime:<0>

Destination Ip Address: 11.0.0.20

Jitter Interval(msec): 10

Frame Numbers: 5

Timeout(sec): 5

Schedule Life(sec): 0

Schedule Period(sec): 0
Schedule Status: Initial!

2). Configure y1731-echo, operation ID is 1, remote mep is 2, MD level is 3, vlan id is 4, service level is 0, at present operation has finished schedule.

IC_A# show sla 1 configuration

Operation <1>:
Type: cfm echo
StartTime: <146400>

Cos: 0
Vlan ID: 4
MD Level: 3
Remote MEP ID: 2
Timeout(sec): 5
Schedule Life(sec): 20
Schedule Period(sec): 10
Schedule Status: Completed!

19.5.2 Show the latest test information of operation

Command Format: show sla {all | oper-num } result

Function:

- Showing as below for sla-echo (delay) operation:
 - Test successful or not;
 - Delay of this test.
- Showing as below for sla-jitter (jitter) operation:
 - Sending detection number;
 - Successful detection number in this test;
 - Packets dropping ratio in this test;
 - Max. delay of successful detection in this test (bi-directional/uni-directional SD/DS);
 - Min. delay of successful detection in this test (bi-directional/uni-directional SD/DS);
 - Sum of all successful detection delay in this test (bi-directional/uni-directional SD/DS);
 - Sum of all successful detection delay square in this test (bi-directional/uni-directional SD/DS);
 - Current delay of successful detection in this test (bi-directional/uni-directional SD/DS);
 - Max. jitter of successful detection in this test (bi-directional/uni-directional SD/DS);
 - Min. jitter of successful detection in this test (bi-directional/uni-directional SD/DS);
 - Sum of all successful detection jitter in this test (bi-directional/uni-directional SD/DS);
 - Current jitter of successful detection in this test (bi-directional/uni-directional SD/DS).

Show result:

1). Configure icmp-jitter, operation ID is 2, destination IP address is 11.0.0.20, detection time interval is 10s, packets number is 5, operation 2 enable schedule, life time is 20s, test period is 10s.

IC_A# show sla 2 result

Operation <2>:

Schedule Status: *Active*

Number of Send Test: *19*

Number of Successful Test: *19*

Percent of Drop Pkts: *0.00000%*

Info of Latest Test : *TWO-WAY* *ONE-WAY(SD)* *ONE-WAY(DS)*

<i>Delay Min(usec)</i>	<i>:</i>	<i>463</i>	<i>232</i>
<i>Delay Max(usec)</i>	<i>:</i>	<i>489</i>	<i>245</i>
<i>Delay Current(usec)</i>	<i>:</i>	<i>477</i>	<i>239</i>
<i>Delay Sum(usec)</i>	<i>:</i>	<i>2386</i>	<i>1195</i>
<i>Jitter Min(usec)</i>	<i>:</i>	<i>1</i>	<i>1</i>
<i>Jitter Max(usec)</i>	<i>:</i>	<i>18</i>	<i>9</i>
<i>Jitter Current(usec)</i>	<i>:</i>	<i>10</i>	<i>5</i>
<i>Jitter Sum(usec)</i>	<i>:</i>	<i>40</i>	<i>21</i>

2). Configure y1731-echo, operation ID is 1, remote mep is 2, MD level is 3, vlan id is 4, service level is 0, operation 1 enable schedule, life time is 20s, test period is 10s.

IC_A# show sla 1 result

Operation <1>: Success!

Info of Latest Test : *TWO-WAY* *ONE-WAY(SD)* *ONE-WAY(DS)*

<i>Current Delay(usec)</i>	<i>:</i>	<i>---</i>	<i>---</i>

19.5.3 Show statistic information of operation schedule

Command Format: `show sla {all | oper-num } statistic`

Function:

- Showing information as below for one schedule:
 - Starting time
 - Life time and schedule period
 - Total amount of transmitted detection
 - Total amount of successful detection

- Packets dropping percent
- Max. delay of successful detection (bi-directional/uni-directional SD/DS)
- Min. delay of successful detection (bi-directional/uni-directional SD/DS)
- Average delay of successful detection (bi-directional/ uni-directional SD/DS)
- Showing the below information also for SLA jitter operation:
 - Sum of all successful detection delay (bi-directional/ uni-directional SD/DS)
 - Sum of all successful detection delay square (bi-directional/ uni-directional SD/DS)
 - Current dealy of successful detection (bi-directional/ uni-directional SD/DS)
 - Max. jitter of successful detection (bi-directional/ uni-directional SD/DS)
 - Min. jitter of successful detection (bi-directional/ uni-directional SD/DS)
 - Sum of all successful detection jitter (bi-directional/ uni-directional SD/DS)
 - Current jitter of successful detection (bi-directional/ uni-directional SD/DS)

Show result:

1). Configure icmp-jitter, operation ID is 2, destination IP address is 11.0.0.20, detection time interval is 10s, packets amount is 5, operation 2 enable schedule, life time is 20s, test period is 10s, operation 2 has finished two schedules.

IC_A# show sla 2 statistic

```

Operation <2>:
StartTime <519330304>:
Schedule Life(sec):      20
Schedule Period(sec):    10
Number of Send Test:     1700
Number of Successful Test: 1631
Percent of Drop Pkts:    4.06%
Statistic of Schedule: TWO-WAY      ONE-WAY(SD)  ONE-WAY(DS)
-----
Delay Min(usec)          :      457          228          228
Delay Max(usec)          :     1624          812          812
Delay Average(usec)      :      487          243          243
Delay Sum(usec)          :     85261        42667        42667
Jitter Min(usec)         :         1          < 1          < 1
Jitter Max(usec)         :     1147          573          573
Jitter Average(usec)     :         29          14           14
Jitter Sum(usec)         :     5173        2581        2581

```

```

Operation <2>:
StartTime <519307376>:
Schedule Life(sec):      20
Schedule Period(sec):    10
Number of Send Test:     10
Number of Successful Test: 10
Percent of Drop Pkts:    0.00%

```

<i>Statistic of Schedule: TWO-WAY</i>	<i>ONE-WAY(SD)</i>	<i>ONE-WAY(DS)</i>
<hr/>		
<i>Number of Successful Test :</i>	<i>10</i>	<i>10</i>
<i>Delay Min(usec) :</i>	<i>0</i>	<i>0</i>
<i>Delay Max(usec) :</i>	<i>0</i>	<i>1</i>
<i>Delay Avreage(usec) :</i>	<i>28</i>	<i>28</i>
<i>Delay Sum(usec) :</i>	<i>0</i>	<i>7</i>
<i>Jitter Min(usec) :</i>	<i>1</i>	<i>1</i>
<i>Jitter Max(usec) :</i>	<i>3</i>	<i>3</i>
<i>Jitter Avreage(usec) :</i>	<i>2</i>	<i>2</i>
<i>Jitter Sum(usec) :</i>	<i>4</i>	<i>4</i>

2). Configure y1731-echo, operation ID is 1, remote mep is 2, MD level is 3, vlan id is 4, service level is 0, operation 1 enable schedule, life time is 20s, test period is 10s, operation 1 has finished 3 schedule.

IC_A# show sla 1 statistic

Operation <1>:

StartTime <519650608>:

Schedule Life(sec): 20

Schedule Period(sec): 10

Number of Send Test: 10

Number of Successful Test: 10

Percent of Drop Pkts: 0.00%

<i>Statistic of Schedule: TWO-WAY</i>	<i>ONE-WAY(SD)</i>	<i>ONE-WAY(DS)</i>
<hr/>		
<i>Delay Min(usec) :</i>	<i>0</i>	<i>0</i>
<i>Delay Max(usec) :</i>	<i>0</i>	<i>0</i>
<i>Delay Avreage(usec):</i>	<i>0</i>	<i>0</i>

Operation <1>:

StartTime <519522992>:

Schedule Life(sec): 20

Schedule Period(sec): 10

Number of Send Test: 10

Number of Successful Test: 10

Percent of Drop Pkts: 0.00%

<i>Statistic of Schedule: TWO-WAY</i>	<i>ONE-WAY(SD)</i>	<i>ONE-WAY(DS)</i>
<hr/>		
<i>Delay Min(usec) :</i>	<i>0</i>	<i>0</i>
<i>Delay Max(usec) :</i>	<i>0</i>	<i>1</i>
<i>Delay Avreage(usec):</i>	<i>0</i>	<i>0</i>

Operation <1>:

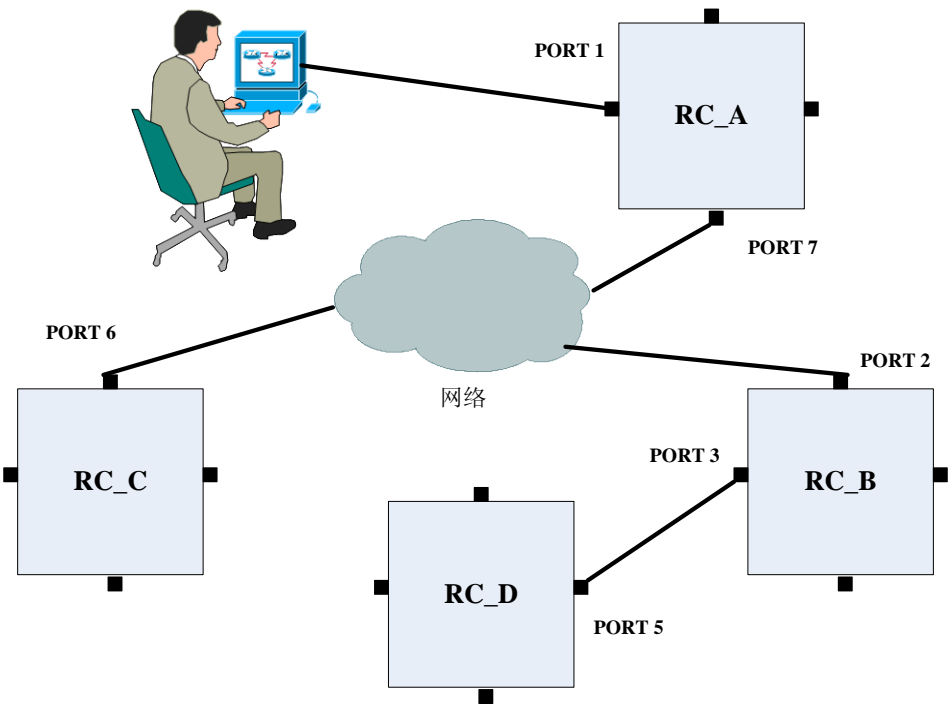
StartTime <146400>:

Schedule Life(sec):	20		
Schedule Period(sec):	20		
Number of Send Test:	10		
Number of Successful Test:	10		
Percent of Drop Pkts:	0.00%		
Statistic of Schedule:	TWO-WAY	ONE-WAY(SD)	ONE-WAY(DS)

Number of Successful Test :	1	1	1
Delay Min(usec) :	0	0	0
Delay Max(usec) :	0	0	0
Delay Avreage(usec):	0	0	0

19.6 Typical configuration applications

As figure shows below, MAC address of RC_A is 000e.5e03.451e, IP address is 11.0.0.10; IP address of RC_C is 11.0.0.20; MAC address of IC_B is 000E.5EE8.ED56.



Configure CFM for RC_A as below:

Configure VLAN:

RC_A(config)# create vlan 4 active

Configure MD:

RC_A(config)# **ethernet cfm domain md-name md5 level 5**

RC_A(config)# **ethernet cfm domain md-name md3 level 3**

Configure service instance:

RC_A(config)# **service ma4 level 3**

Associating VLAN:

RC_A (config-service)# **service vlan-list 4**

Enable CC:

RC_A (config-service)# **service cc enable**

Set port mode:

RC_A(config)# **interface port 7**

RC_A (config-port)# **switchport mode trunk**

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

Enable cfm:

RC_A(config)# **ethernet cfm enable**

Configure CFM for RC_B as below:

Configure VLAN:

RC_B (config)# **create vlan 4 active**

Configure MD:

RC_B (config)# **ethernet cfm domain md-name md5 level 5**

RC_B (config)# **ethernet cfm domain md-name md3 level 3**

Configure service instance:

RC_B(config)# **service ma4 level 3**

Associating VALN:

RC_B (config-service)# **service vlan-list 4**

Enable CC:

RC_B (config-service)# **service cc enable**

Configure MEP:

```
RC_B (config-service)# service mep up mpid 2 port 3
```

Set port mode:

```
RC_B(config)# interface port 2
```

```
RC_B (config-port)# switchport mode trunk
```

```
RC_B (config-port)# exit
```

```
RC_B(config)# interface port 3
```

```
RC_B (config-port)# switchport mode trunk
```

```
RC_B (config-port)# exit
```

Enable cfm:

```
RC_B(config)# ethernet cfm enable
```

1). RC_A switch performs layer-3 jitter test to RC_C switch, make sure network connection between RC_A and RC_C is OK (the two device can ping successfully). RC_A configures with icmp-jitter, operation ID is 2, destination IP address is 11.0.0.20 (RC_C IP address), detection time interval is 10s, packets number is 5, life time is 20s, and test period is 10s.

Configure IC_A as below:

```
RC_A#config
```

```
RC_A (config)# sla 2 icmp-jitter dest-ipaddr 11.0.0.20 interval 10 packets 5
```

```
RC_A (config)# sla schedule 2 life 20 period 10
```

```
RC_A (config)# exit
```

```
RC_A# show sla 2 configuration
```

Operation <2>:

Type: icmp jitter

StartTime:<519330304>

Destination Ip Address: 11.0.0.20

Jitter Interval(msec): 10

Frame Numbers: 5

Timeout(sec): 5

Schedule Life(sec): 20

Schedule Period(sec): 10

Schedule Status: Completed!

RC_A# show sla 2 result*Operation <2>:**Schedule Status:* Active*Number of Send Test:* 19*Number of Successful Test:* 19*Percent of Drop Pkts:* 0.00000%*Info of Latest Test :* TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

<i>Delay Min(usec)</i>	:	460	230	230
<i>Delay Max(usec)</i>	:	491	246	246
<i>Delay Current(usec)</i>	:	472	236	236
<i>Delay Sum(usec)</i>	:	2363	1183	1183
<i>Jitter Min(usec)</i>	:	13	7	7
<i>Jitter Max(usec)</i>	:	27	14	14
<i>Jitter Current(usec)</i>	:	19	10	10
<i>Jitter Sum(usec)</i>	:	77	40	40

RC_A# show sla 2 statistic*Operation <2>:**StartTime <519330304>:**Schedule Life(sec):* 20*Schedule Period(sec):* 10*Number of Send Test:* 1700*Number of Successful Test:* 1631*Percent of Drop Pkts:* 4.05882%*Statistic of Schedule:* TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

<i>Delay Min(usec)</i>	:	453	227	227
<i>Delay Max(usec)</i>	:	4913	2457	2457
<i>Delay Average(usec)</i>	:	508	254	254
<i>Delay Sum(usec)</i>	:	374054	187186	187186
<i>Jitter Min(usec)</i>	:	2	1	1
<i>Jitter Max(usec)</i>	:	4429	2215	2215
<i>Jitter Average(usec)</i>	:	62	31	31
<i>Jitter Sum(usec)</i>	:	45967	22986	22986

2). RC_A switch performs layer-2 delay test to RC_B switch, make sure network connection between RC_A and RC_B is OK (the two device can ping successfully). RC_A configures with y1731-echo, operation ID is 1, remote mep is 2, MD level is 3, vlan id is 4, service level is 0, life time is 20s, and test period is 10s.

Configure RC_A as below:

RC_A#config

RC_A (config)# sla 2 y1731-echo remote-mep 2 level 3 vlan 4 cos 0

RC_A (config)# sla schedule 2 life 20 period 10

RC_A (config)# exit

RC_A# show sla 1 configuration

Operation <1>:

Type: cfm echo

StartTime: <519522992>

```
-----
Cos:                                0
Vlan ID:                            4
MD Level:                           3
Remote MEP ID:                       2
Timeout(sec):                        5
Schedule Life(sec):                  20
Schedule Period(sec):                10
Schedule Status:                     Completed!
```

RC_A# show sla 1 result

Operation <1>: Success!

Info of Latest Test : TWO-WAY ONE-WAY(SD) ONE-WAY(DS)

```
-----
Current Delay(usec): 466          233          233
```

RC_A# show sla 1 statistic

Operation <1>:

StartTime <519522992>:

```
Schedule Life(sec):      20
Schedule Period(sec):    10
Number of Send Test:     50
Number of Successful Test: 50
Percent of Drop Pkts:    0.00%
Statistic of Schedule: TWO-WAY ONE-WAY(SD) ONE-WAY(DS)
-----
Delay Min(usec)   :    452          226          226
Delay Max(usec)   :    3426         1713         1713
Delay Average(usec) :    486          243          243
```


Chapter 20 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 of Y.1731
- ✧ Monitoring and maintenance of Y.1731
- ✧ Typical configuration examples of Y.1731

20.1 Functional overview of Y.1731

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 brings forward for the Ethernet management maintenance and reliability. Traditional Ethernet has not carrier-managed capabilities, cannot 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: Continuity Check) the provision of, end-to-end connectivity fault recognition tools (LB: LoopBack) and fault isolation tools (LT: LinkTrace).

20.1.1 Components of Y.1731

➤ 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.

➤ 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 cannot 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.

➤ 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.

➤ MIP

MIP is a management activity entity configured within service instance, a MIP is component of 2 MHF (MIP Half Function). MIP cannot take the initiative to send CFM message, but can handle and respond to LTM and LBM messages. MIP is created by automation according to auto-configuration rule, cannot be created by manual.

Auto-configuration rules for MIP showing as below, for each port and each vlan:

● Finding out matched MD

1. If the port is configured with MEP, suppose the highest level of all configured MEP is N, then the minimum level is the matching MD if there is MD level higher than N; or else, there is no matched MD.

Example: In case of a MA port is configured with two MEP, and associated four MD for this MA.

MEP1 level = 2, MEP2 level = 3;

MD1 level = 2, MD2 level = 3, MD3 level = 5, MD4 level = 6

Then, MD3 is the matched MD.

2. If there is no MEP configured on port, configure MD of minimum level as matched MD.

● Processing according to MIP configuration rules

Create MIP under MD if only there is matched MD.

➤ MP

MEP and MIP are called by a joint name MP.

20.1.2 Basic function of Y.1731

The realization of Y.1731 function based on the 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)
- 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.

- Failure confirm function

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-3 ping, and therefore failure confirm function form as layer-2 ping in application

- Fault isolation

Fault isolation is used to determine trace from source MEP to the target MP. This function sent LTM through source MEP (Link Trace Message) to destination MP, each bridge device configured with 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-3 traceroute functions, so in application it forms as Layer-2 traceroute.

Altogether, Y.1731 realizes OAM technology on end-to-end layer, which helps reduce service providers' operation coast and enhance their competition advantages.

20.2 Default configuration list of Y.1731

No.	Property	Default
1	Default MD configuration status	No MD
2	Default service instance configuration status	No service instance
3	Default global functional switch status	Disable
4	Default port functional switch status	Enable
5	Default error CCM database saving time	100 minutes
6	Default fault alarm level	macRemErrXcon, in support of 4 bug alarms: port fault, loss of remote end, CCM error, cross-connection.
7	Default service instance VLAN mapping	No VLAN mapping

8	Default MEP configuration status in service instance	No MEP
9	Default static remote MEP in service instance	No static remote MEP
10	Default MEP configuration status in port	No MEP
11	Default static remote MEP configuration in port	No static remote MEP
12	Default service instance CCM sending time interval	10 seconds
13	Default MEP CCM transmitting switch status	disable
14	Default MEP CCM transmitting mode	Passive mode
15	Default remote MEP dynamic import function	Doesn't import dynamically
16	Default cc check function learned by remote MEP	disable
17	Default aging time of dynamic remote MEP	100 minutes
18	Default service instance OAM packets priority	6
19	Default LBM number transmitted by layer-2 ping	5
20	Default TLV length of layer-2 ping data	64
21	Default source MEP of layer-2 ping	Auto searching
22	Default initial TTL of layer-2 traceroute	64
23	Default source MEP of layer-2 traceroute	Auto searching
24	Default LT database switch	disable
25	Default LT database max. save data amount	Save at most 100 data item by default when LT database enable. Save 0 data item by default when LT database disable.
26	Default LT database save data time	100 minutes
27	Default service instance OAM packets C-VLAN configuration	No C-VLAN

20.3 CFM configuration constraints and limitations

- 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;
- 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;
- Before delete the maintenance domain, user should delete all MEP of maintenance domain, otherwise deletion of the maintenance domain will lead to failure;
 - When configuring service instance, the allowed string length of MA Name is between 1-13 bytes;
 - Each service instance is mapped to 32 VLAN at most, use the smallest VLAN as main VLAN, MEP in service instance utilize main VLAN for OAM transmitting messages, other 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
 - If the service instance has not yet been mapped to any VLAN, then configure the local MEP in service instance is not allowed
 - If the service instance has been configured MEP, it mustn't delete and modify VLAN mapping of services instance
 - 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.
 - Before modifying CCM transmitting interval, user need to close all CCM transmitting switch of MEP in services instance
 - Before delete the service instance user should delete all MEP in service instance, otherwise will lead to the failure of delete services instances;
 - Maximum MEP of each device exist differences in equipment, the details may refer to the list of equipment characteristics and other related document

20.4 CFM configuration list and instruction

- 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
- Fault detection
 - Configure CCM transmitting switch
 - Configure CCM transmitting interval
 - Configure CCM transmitting mode
 - Configure dynamic import function learned by remote MEP
 - Configure aging time of remote MEP
 - Configure client VLAN of OAM message
 - Configure OAM message priority
 - Configure hold time of error CCM message
 - Configuration fault alarm level
- Failure confirm-the implementation of layer-2 ping operation
- Fault isolation
 - The implementation of layer-2 traceroute operation
 - Configure switch status of database LT
 - Configure hold time of database LT
 - Configure preservable data entries of database LT

20.4.1 Configure overall functional switch of Y.1731

Disable Y.1731 global function by default (Disable).

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	ethernet cfm {enable / disable}	Enable/disable 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.

Example: Enable global functional switch in global configuration mode.

```
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.

20.4.2 Configure ports functional switch of Y.1731

When Y.1731 port switch function switch disable, MP configured on the port will not take into effect, OAM message of Y.1731 cannot be transmitted or received on port. Enable functional switch of all ports by default.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port port-id	Enter specified <i>port-id</i> 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

Example: Enable Y.1731 function on ports 3.

```
Raisecom#config
```

```
Raisecom(config)#interface port 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.

20.4.3 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 use 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. <i>domain-name</i> : name of the maintenance domain, the string length: 1-16 bytes; <i>level</i> : the level of maintenance domain, range in: 0-7.
3	exit	Return to privileged user mode.
4	show ethernet cfm domain [level <0-7>]	Show configuration information of maintenance domain.

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, level-3.

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.

20.4.4 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 <i>CSIID</i> level level	Create service instance and to enter the service instance mode. <i>CSIID</i> : name in service instance, the length of 1-13 bytes; <i>level</i> : 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 [level <0-7>]	Shows maintenance domain and configuration information in service instance

Example: Configure the service instance of name ma3-1-4 in a level-3 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 configurations in service instance reach the maximum, configuration in service instance will lead to failure.

20.4.5 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, other VLAN is not used to transmit or receive packets.

Service instance is mapped to a group of VLAN, namely the VLAN in VLAN list is fully equivalent, as use main VLAN for transmitting and receiving packets, which all of other VLAN in the list are mapped to the main 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 repeatedly to the main VLAN 10 and the main 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, main VLAN 100-120 is mapped to main VLAN 100, and 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 main VLAN.

The following is legal:

Positive Example 1: service instance ma3-1-5 in maintenance domain of Level 3 map to VLAN 10-20, service instance ma5-1-1 in maintenance domain of Level 5 is mapped 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 <i>service-instance</i> : name in service instance, the length of 1-13 bytes; <i>level</i> : the range of maintenance domain level: 0-7;
3	service vlan-list vlan-list	<i>vlan-list</i> : 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 level [<0-7>]	Shows maintenance domain and configuration information in service instance.

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.

20.4.6 Configure MEP

There are two kinds of MEP configuration: one is MEP configuration over service instance, and the other one is over port. Before configuring MEP over service instance, user should configure maintenance domain first, and then 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. For MEP configuration over port, one port can only configure one MEP and the direction is down.

Delete designated MEP over service instance: **no service mep mepid**

Delete designated MEP over port: **no ethernet cfm down-mep**

Step	Command	Description
1	config	Enter global configuration mode
2	service <i>CSIID level level</i>	Enter service instance mode <i>CSIID</i> : name in service instance, the length of 1-13 bytes; <i>level</i> : the range of maintenance domain level: 0-7.
3	service mep [up down] mpid <i>mepid</i> { port <i>port-id</i> line <i>line-id</i> client <i>client-id</i> }	Configure MEP in service instance <i>up</i> : up-bound MEP <i>mepid</i> : MEPID; <i>port-id</i> : Port ID, value 1 to the largest port ID; <i>line-id</i> : Line port ID, value 1 to the largest line port ID; <i>client-id</i> : Client port ID, value 1 to the largest Client port ID.
4	exit	Return to global configuration mode.
4	exit	Return to privileged user mode.
5	show ethernet cfm local-mp [interface port <i><1-MAX_PORT_STR></i> level <i><0-7></i>]	Show information of local MEP.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter port mode <i>portid</i> : port ID
3	ethernet cfm down-mep mpid <i><1-8191></i>	Configure down mep over port <i><1-8191></i> : MEPID range in 1-8191.
4	show ethernet cfm local-mp [interface port <i><1-MAX_PORT_STR></i> level <i><0-7></i>]	Show information of local MEP

Example: Configure MEP in the service instance, port 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)#**exit**

Configure MEP under port:

Raisecom#**config**

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

```
Raisecom(config-port)#ethernet cfm down-mep mpid 1
```

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

```
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;
- Configure failed if there is MEP existing in configuration over port;
- Configure failed if the MEP over port has been configured as static remote over port.

20.4.7 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 remote-mep static** to show all the static MEP information under service instance.

Before configuring static remote MEP, you should configure maintaining domain first, and configure service instance in the maintaining domain.

When MEP receives CCM, if service instance enables cc check function and no remote MEP with identical MEP ID as CCM carried from MEP list, MEP is considered to receive unexpected CCM. User can direct configure static remote over port under the port and one port can only configured one static remote.

Delete the specified static remote MEP: **no service remote mep mepid**

Delete static remote MEP under port: **no ethernet cfm down-mep.**

Step	Command	Description
1	config	Enter global configuration mode
2	service service-instance level level	Enter service instance mode <i>service-instance</i> : name in service instance, the length of 1-13 bytes; <i>level</i> : the range of maintenance domain level: 0-7.
3	service remote-mep {1-8191}	Configure static remote MEP.
4	exit	Return to global configuration mode
5	exit	Return to privileged user mode
6	show ethernet cfm remote-mep static	Show information of static remote mep.

Example: Configure static remote MEP in service instance.

```
Raisecom#config
```

```
Raisecom(config)#ethernet cfm domain level 3
```

```
Raisecom(config)#service ma3-1-4 level 3
```

```
Raisecom(config-service)#service remote-mep 100-1000
```

```
Raisecom(config)#exit
```

Configure static remote MEP under port.

```
Raisecom#config
```

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

```
Raisecom(config-port)#ethernet cfm remote-mep 2
```

```
Raisecom(config)#exit
```

Note: If the assigned MEPID is used by local MEP in service instance or static remote MEP, the configuration is unsuccessful.

20.4.8 Configure CCM transmitting switch

Configure CCM sending switch for MEP. When CCM switch of MEP is disabled, disable MEP transmitting CCM. MEP default status is disable transmitting CCM packets.

Step	Command	Description
1	config	Enter global configuration mode
2	service <i>CSIID</i> level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain, value in 0-7.
2	service cc {enable disable} mep { {1-8191} all }	Enable/disable MEP transmitting CCM. enable : enable disable : disable {1-8191}: MEPID list, value in 1-8191. all : all of the configured MEP
3	exit	Return to Privileged EXEC mode.
4	show ethernet cfm local-mp [interface port <1-MAX_PORT_STR> level <0-7>]	Show MP configuration information of local maintenance domain.

Example: Enable MEP1 CCM transmitting switch in 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
```

20.4.9 Configure CCM transmitting interval

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 <i>CSIID</i> level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain, value in 0-7.
3	service cc interval {1 / 10 /60 /600}	Configure CCM transmitting interval for service instance. Unit: second
4	exit	Return to global configuration mode.
5	exit	Return to Privileged EXEC mode.
6	show ethernet cfm domain [level <0-7>]	Show configuration information of maintenance domain and service instance

Example: Set transmitting interval in service instance as 60 seconds

```
Raisecom#config
```

```
Raisecom(config)#ethernet cfm domain md3-1 level 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 configuring CCM transmitting interval in service instance, user needs 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.

20.4.10 Configure CCM transmitting mode

CCM transmitting mode includes master mode and slave mode. By default, it is slave mode. This command is a global configuration command. For the device, all service instance transmits CCM packets according to configured mode. When it is configured in master mode, transmitting multicast CCM packet, the packet will take its own private TLV to denote the CCM packet is in master mode; when configured in slave mode, the device transmit multicast CCM packet in normal, but in below

conditions it is special: when device receives CCM packets from remote is master mode, the device will transmit unicast CCM packet.

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet cfm mode <i>(slave/master)</i>	Configure mode for all service instance on device transmits CCM packets.
3	exit	Return to Privileged EXEC mode.
4	show ethernet cfm	Show local MD information.

Example: Set device in master transmitting mode.

Raisecom#**config**

Raisecom(config)#**ethernet cfm mode** *master*

Raisecom(config)#**exit**

Note: Since the master device mode is written mac address through acl, the configuration of master mode request for the device supporting acl.

20.4.11 Configure dynamic import function for remote learning

By default, service instance remote MEP learning dynamic import function is not effective.

This command is to transfer dynamic learned remote MEP to static remote MEP, namely, every time receiving CCM packets, automatic transfer the dynamic remote MEP to static remote.

Step	Command	Description
1	config	Enter global configuration mode
2	service CSIID level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain.
3	service remote mep learning active	Configure dynamic import function learned by remote MEP.
4	exit	Return to global configuration mode.

Example: Execute operation of importing remote mep dynamically.

Raisecom#**config**

Raisecom(config)#**ethernet cfm domain md3-1 level** 3

Raisecom(config)#**service ma3-1-4 vlan** 4

Raisecom(config-service)#**service remote mep learning** *active*

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

Raisecom(config)#**exit**

20.4.12 Configure cc check function of remote MEP

By default, this function is disabled. When enabling this function, system check dynamic learned remote MEP ID consistent with static remote MEP ID once it receives CCM message, if inconsistent, the CCM message is considered incorrect.

Step	Command	Description
1	config	Enter global configuration mode
2	service <i>CSIID</i> level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain.
3	service remote-mep cc-check (<i>enable</i> <i>disable</i>)	Configure cc check function learned by remote MEP.
4	exit	Return to global configuration mode.
5	show ethernet cfm domain [<i>level</i> <0-7>]	Show configuration of local maintenance domain and service instance.

Example: Execute cc check function of remote mep.

```
Raisecom#config
```

```
Raisecom(config)#ethernet cfm domain md3-1 level 3
```

```
Raisecom(config)#service ma3-1-4 vlan 4
```

```
Raisecom(config-service)#s service remote-mep cc-check enable
```

```
Raisecom(config- service)#exit
```

```
Raisecom(config)#exit
```

20.4.13 Configure aging time for remote MEP

By default, the remote MEP aging time is 100 minutes.

To restore the default aging time by command of **no ethernet cfm remote mep age-time**.

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet cfm remote mep age-time <i>minutes</i>	Configure MEP aging time <i>minutes</i> : range in 1-65535, unit: minute
3	exit	Return to Privileged EXEC mode.
4	show ethernet cfm	Show the global configuration information.

Example: Configure remote MEP aging time for 101 minutes.

```
Raisecom#config
```

```
Raisecom(config)# ethernet cfm remote mep age-time 101
```

```
Raisecom(config)#exit
```


20.4.14 Configure client VLAN for Y.1731 OAM message

Defaulted Y.1731 OAM message does not carry C-TAG, after configuring CVLAN for the service instance, all CCM, LTM, LBM and DMM sent by MEP under service instance will use double-TAG, C-TAG uses CVLAN.

Delete Client VLAN of Y.1731 OAM message by the command of **no service cvlan**.

Step	Command	Description
1	config	Enter global configuration mode
2	service <i>CSIID</i> level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain
3	service cvlan <i>vlan</i>	Configure client vlan of OAM message <i>vlan</i> : client VLAN, range in 1-4094
3	exit	Return to global configuration mode.
4	exit	Return to Privileged EXEC mode.
5	show ethernet cfm domain	Show configuration information of maintenance domain and service instance.

Example: Set client VLAN for Y.1731 OAM message as 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
```

Note: When service instance has configured client VLAN, OAM packets of Y.1731 CCM, LTM, LBM, DMM use double TAG, VLAN configured client VLAN in C-TAG; but for OAM packets in type of LBR, LTR, DMR, whether use double TAG is consistent to LBM, LTM and DMM packets received by VLAN in C-TAG.

20.4.15 Configure priority for Y.1731 OAM message

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 by the command of **no service priority**.

Step	Command	Description
1	config	Enter global configuration mode
2	service <i>CSIID</i> level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain
3	service priority <i>priority</i>	Configure priority of OAM message <i>priority</i> : priority ,value 0-7

4	exit	Return to global configuration mode.
5	exit	Return to Privileged EXEC mode.
6	show ethernet cfm domain	Show configuration information of maintenance domain and service instance.

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.

20.4.16 Configure hold time for 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 this command won't 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 hold time of error CCM data: **no ethernet cfm error archive-hold-time**.

Step	Command	Description
1	config	Enter global configuration mode
2	ethernet cfm error archive-hold-time minutes	Configure hold time of error CCM message <i>minutes</i> : retention time(min), range in 1-65535
3	exit	Return to Privileged EXEC mode.
4	show ethernet cfm	Show relative information of cfm

Example: Set the hold time of error CCM database as 50.

Raisecom#**config**

Raisecom(config)#**ethernet cfm error archive-hold-time 50**

Raisecom(config)#**exit**

20.4.17 Configure CFM fault alarm level

CC function of Y.1731 can detect fault in five levels, in accordance with the order of descending order: 5-cross-connect faults, 4-CCM error fault, 3-Remote MEP lost fault, 2-port state fault and 1-RDI fault.

Configure all to allow five types of alarm transmitting;

Configure macRemErrXcon allows transmitting four kinds of fault: cross-connect fault, CCM error fault, remote MEP lost fault, port state fault, namely transmitting alarms types 2-5;

Configure remErrXcon allows transmitting three kinds of fault: cross-connect fault, CCM error fault, remote MEP lost fault, namely transmitting alarms types 3-5;

Configure errXcon allows transmitting two kinds of fault: cross-connect fault, CCM error fault, namely transmitting alarms types 4-5;

Configure Xcon allows transmitting one kind of fault: cross-connect fault, namely transmitting alarms type 5;

Configure **none** doesn't transmit any alarm.

Default state is macRemErrXcon.

Restoration types of the transmitting alarm: **no snmp-server cfm-trap**.

Step	Command	Description
1	config	Enter global configuration mode
2	service <i>CSIID</i> level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintaince domain.
3	snmp-server trap cfm {all macRemErr remErr ccmErr xcon none} mep {<i>mepid-list</i> 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. <i>mepid-list</i> : meplist, range in1-8191
3	exit	Return to Privileged EXEC mode.
4	show ethernet cfm local-mp	Show configuration information of local MP

Example: Set fault alarm level as 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.

20.4.18 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.

Layer-2 ping function contains ping over service instance and over port two kinds, the two are of identical functional after configuration. 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 ways 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 <i>CSIID</i> level <i>level</i>	Enter service instance mode <i>CSIID</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain.
3	ping { <i>HHHH.HHHH.HHHH</i> mep <i>rmepid</i> } [count <i>count</i>] [size <i>size</i>] [source <i>mepid</i>]	Execute layer-2 PING, used for fault reset <i>HHHH.HHHH.HHHH</i> : remote MP MAC address, unicast valid address. <i>rmepid</i> : remote MEP ID, range in 1-8191 <i>count</i> : transmitted LBM amount, range in 1-1024. <i>size</i> : data TLV length, range in 1-1484. <i>mepid</i> : source MEPID, range in 1-8191.
3	exit	Return to global configuration mode.
4	exit	Return to Privileged EXEC mode.

Example: ping service instance.

```
Raisecom#config
```

```
Raisecom(config)#ethernet cfm enable
```

```
Raisecom(config)#ethernet cfm domain md-name md3-1 level 3
```

```
Raisecom (config)#service ma3-1-4 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 replies: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

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

Ping over port:

Raisecom#**config**

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

Raisecom (config-port)#**ethernet cfm 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 replies: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

Raisecom (config-port)#**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 other user is using designated source MEP to execute PING it may cause operation failure.

20.4.19 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 CSIID level level	Enter service instance mode CSIID: name of service instance, 1-13 bytes. level: maintaining domain level
3	traceroute {HHHH.HHHH.HHHH 	Execute layer-2 TRACEROUTE function, used for fault isolation.

	mep rmepid} [ttl ttl] [source mepid]	<i>HHHH.HHHH.HHHH</i> : remote MP MAC address; <i>Rmepid</i> : remote MEPID, range in 1-8191; <i>Ttl</i> : original TTL, range is 1-255; <i>Mepid</i> : source MEPID, range in 1-8191
3	exit	Return to global configuration mode.
4	exit	Return to Privileged EXEC mode.

Example:

Raisecom#**config**

Raisecom(config)#**ethernet cfm enable**

Raisecom(config)#**ethernet cfm domain md-name md3-1 level 3**

Raisecom (config)#**service ma3-1-4 level 3**

Raisecom (config-service)#**traceroute 000E.5E03.5318 ttl 128**

Show result:

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.

20.4.20 Configure switch status for LT database

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 disabled, user can not see information of traceroute by command **show ethernet cfm traceroute-cache**

The switch is disabled by default.

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	ethernet cfm traceroute cache {enable disable}	Configure switch status of database LT enable : enable disable : disable
3	exit	Return to Privileged EXEC mode.
4	show ethernet cfm traceroute-cache	Show traceroute information.

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.

20.4.21 Configure data holding time in LT database

When database LT switch is enabled, 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 global configuration mode
2	ethernet cfm traceroute cache enable	Enable database LT switch
3	ethernet cfm traceroute cache hold-time minutes	Configure data hold time in LT database. <i>Minutes</i> : hold time, unit is minutes, range in 1-65535.
4	exit	Return to Privileged EXEC mode
5	show ethernet cfm traceroute-cache	Show data information

Example: After the database enable, set holding time for data as 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
```

20.4.22 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 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 database, range in 1-512
4	exit	Return to global configuration mode.
5	show ethernet cfm traceroute-cache	Show data information

Example: Set stored entries as 150 after enabling database LT.

Raisecom#**config**

Raisecom(config)#**ethernet cfm traceroute cache enable**

Raisecom(config)#**ethernet cfm traceroute cache size 150**

Raisecom(config)#**exit**

20.4.23 Configure overtime for Rfc2544 throughput measurement

NOTE: RC551 series is not in support of this function.

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 global configuration mode
2	service CSIID level level	Enter service instance mode CSIID: name of service instance, 1-13 bytes. level: level of maintenance domain
3	service performance-monitor throughput timeout seconds	seconds: overtime, range in 2-30, unit: second
4	exit	Return to global configuration mode.
5	exit	Return to Privileged EXEC 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

Example: Configure overtime of rfc2544 in 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 throughput timeout 20
```

```
Raisecom(config)#exit
```

20.4.24 Start rfc2544 throughput measurement

NOTE: RC551 series is not in support of this function.

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 global configuration mode
2	service service-instance level level	Enter service instance mode <i>service-instance</i> : name of service instance, 1-13 bytes. <i>level</i> : level of maintenance domain
3	test throughput object band-wide [packet-size {64/128/256/512/1024/1280/1518}]	<i>band-wide</i> : target bandwidth, range in 2-900, unit: Mbps packet-size : length of measurement message 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 EXEC mode.
6	show ethernet cfm performance-monitor throughput level <0-7> service CSIID	Show result of throughput measurement.

Example: Enable overtime of rfc2544in the service instance, bandwidth of the measurement target is 3Mbps

```
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 throughput timeout 20**

Raisecom(config-service)#**test throughput object 3 packet-size 256**

Maintenance Domain Level : 3

Service : ma3-1-4

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: succeeded

Far End throughput test result:

<i>Local Send(Bps)</i>	<i>Remote Recv(Bps)</i>	<i>Local Send(pps)</i>	<i>Remote Recv(pps)</i>
------------------------	-------------------------	------------------------	-------------------------

<i>3,000,000</i>	<i>2,890,000</i>	<i>1169</i>	<i>1168</i>
------------------	------------------	-------------	-------------

Near End throughput result:

<i>Remote Send(Bps)</i>	<i>Local Recv(Bps)</i>	<i>Remote Send(pps)</i>	<i>Local Recv(pps)</i>
-------------------------	------------------------	-------------------------	------------------------

<i>3,000,000</i>	<i>2,889,000</i>	<i>1170</i>	<i>1164</i>
------------------	------------------	-------------	-------------

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.

20.5 Monitoring and maintenance

Command	Description
show ethernet cfm traceroute-cache	Show traceroute discovery information of database LT
show ethernet cfm local-mp [interface port <i>port-id</i> level <i>level</i>]	Show configuration information of local MP, contains MEP and MIP
show ethernet cfm remote-mep [level <i>level</i>] [service <i>service-instance</i> [mep <i>mepid</i>]]	Show discovery information of remote MEP
show ethernet cfm errors [level <i>level</i>]	Show information of error CCM database
show ethernet cfm domain [level <i>level</i>]	Show configuration information of maintenance domain and service instance
show ethernet cfm mep level <i>level</i>	Show MEP information in service instance

service <i>service-instance</i>	
show ethernet cfm remote-mep static	Show static remote MEP information.
show ethernet cfm	Show global configuration information of Y.1731.
Show ethernet cfm	Show measurement result of last RFC2544
performance-monitor throughput level	
<i>level</i> service <i>service-instance</i>	
clear ethernet cfm traceroute-cache	Delete information of database LT
clear ethernet cfm remote-mep [<i>level</i> <i>level</i> [<i>service</i> <i>service-instance</i> [<i>mpid</i> <i>mepid</i>]]]	Delete specified information of remote MEP database
clear ethernet cfm errors [<i>level</i> <i>level</i>]	Delete specified information of remote MEP database

20.5.1 Show LT database traceroute 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 toCCCC on domain md1, level 3, VLAN 4.

<i>Hops</i>	<i>HostMAC</i>	<i>Ingress/EgressPort</i>	<i>IsForwarded</i>	<i>RelayAction</i>	<i>NextHop</i>
1	AAAA	8/1	Yes	RlyFdb	BBBB
2	BBBB	2/3	Yes	RlyFdb	CCCC
!3	CCCC	-/9	No	RlyHit	CCCC

20.5.2 Show local MEP configuration information

Command format: show ethernet cfm local-mp [*interface* *port* *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

<i>Level</i>	<i>Type</i>	<i>Port</i>	<i>Mac Address</i>

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	

20.5.3 Show discovery information of 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 MEP 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.

20.5.4 Show error CCM database information

Command Format: `show ethernet cfm errors [level level]`

Function: to view fault MD level, fault MA associated VLAN, MEPID of fault local MEP, MAC address of remote MEP related to fault, and meanwhile to view error type. User can choose to display error CCM information in assigned MD, error CCM information in assigned MD level.

Show result: Show error CCM information of level 1, fault associated vlan is 4, MPID of fault discover local MEP is 2, remote MAC address is CCCC, error type is ErrorCCM.

IC_A#`show ethernet cfm errors level 1`

Level	VLAN	MPID	RemoteMEP MAC	ErrorType	AffectedService

1	4	2	CCCC	ErrorCCM	md1-ma4

20.5.5 Show configuration information of maintenance 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
-----
```

20.5.6 Show information of static remote MEP

Command format: show ethernet cfm remote-mep static

Function: To view static remote MEP information.

Show result: Show MD level 3, with empty name, MA named ma2 and static remote MEP list under MA is 5-9.

Raisecom#**show ethernet cfm remote-mep static**

```
Maintenance Domain(MD) level: 3
Maintenance Domain(MD) name:
Service Instance: ma3
Static remote MEP list: 5-9
```

20.5.7 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.

Show result: 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

20.5.8 Show the measurement results of previous RFC2544 throughput

Command Format: `show ethernet cfm performance-monitor throughput level <0-7> service CSIID`

Function: Display measurement results information of previous RFC2544 throughput.

Show result:

RFC2544 throughput test information:

Throughput testing between MEP 100 in port 1 and remote mep 200:

Expected object: 3 Mbps

Packet length: 256

Rfc2544 throughput test result: succeeded

Far End throughput result:

<i>Local Send(bps)</i>	<i>Remote Recv(bps)</i>	<i>Local Send(pps)</i>	<i>Remote Recv(pps)</i>
------------------------	-------------------------	------------------------	-------------------------

3,000,000	2,890,000	1700	1701
-----------	-----------	------	------

Near End throughput result:

<i>Remote Send(bps)</i>	<i>Local Recv(bps)</i>	<i>Remote Send(pps)</i>	<i>Local Recv(pps)</i>
-------------------------	------------------------	-------------------------	------------------------

3,000,000	2,960,000	1710	1708
-----------	-----------	------	------

20.5.9 Clear information of database LT

Clear all the layer-2 traceroute information in database LT.

Step	Command	Description
1	config	Enter global configuration mode
2	clear ethernet cfm traceroute-cache	Clear information of LT database
4	exit	Return to Privileged EXEC mode.
5	show ethernet cfm traceroute-cache	Show data information

Example: Clear all information in LT database.

Raisecom#**config**

Raisecom(config)#**clear ethernet cfm traceroute-cache**

Raisecom(config)#**exit**

20.5.10 Clear information of remote MEP database

Clear specified information of remote MEP database.

Step	Command	Description
------	---------	-------------

1	config	Enter global configuration mode
2	clear ethernet cfm remote-mep [<i>level level</i> [<i>service</i> <i>service-instance</i> [<i>mpid mepid</i>]]]	Clear information of remote MEP database <i>level</i> : level of maintenance domain, value in 0-7. <i>service-instance</i> : name in service instance length:1-13 bytes. <i>mepid</i> : local MEPID.
4	exit	Return to Privileged EXEC mode.
5	show ethernet cfm remote-mep	Show data information.

Example: Clear remote MEP information of 3-level maintenance domain.

Raisecom#**config**

Raisecom(config)#**clear ethernet cfm remote-mep level 3**

Raisecom(config)#**exit**

20.5.11 Clear information of error CCM database

Clear specified information of remote MEP database.

Step	Command	Description
1	config	Enter global configuration mode
2	clear ethernet cfm errors [<i>level level</i>]	Clear information of error CCM database. <i>level</i> : level of maintenance domain, value in 0-7.
4	exit	Return to Privileged EXEC mode.
5	show ethernet cfm error	Show data information

Example: Clear specified information of remote MEP database.

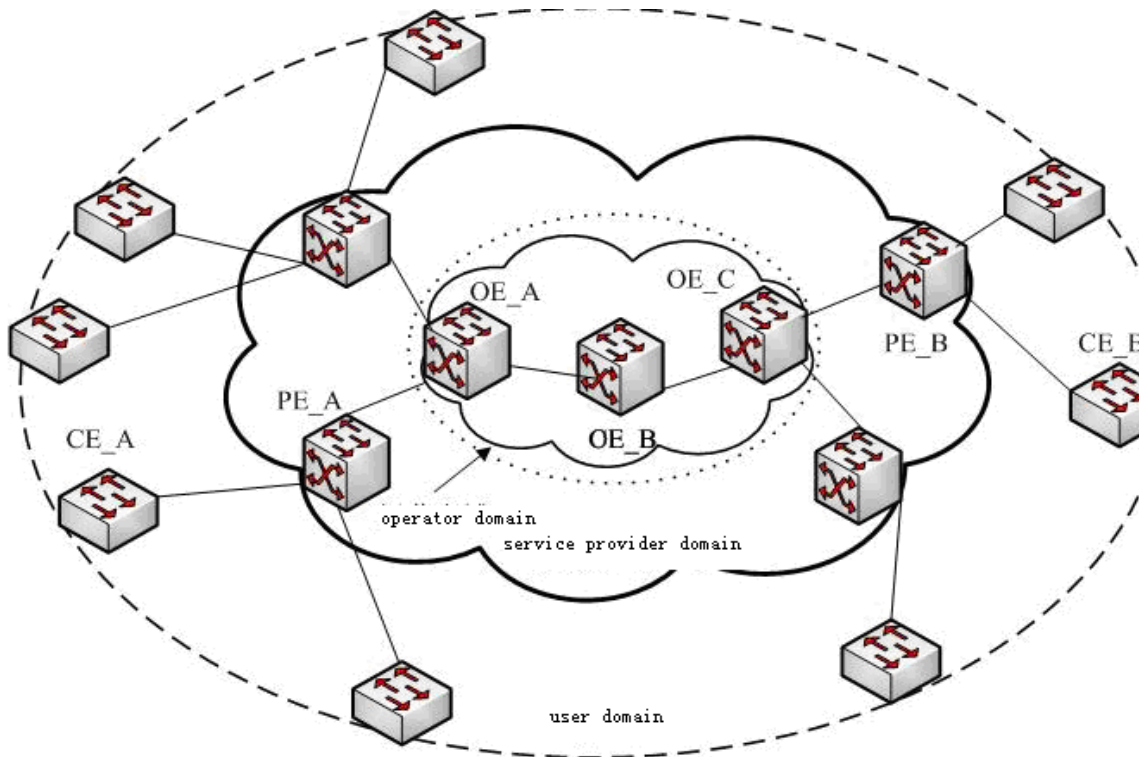
Raisecom#**config**

Raisecom(config)#**clear ethernet cfm errors level 3**

Raisecom(config)#**exit**

20.6 Typical configuration

Topology structure:



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 steps 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 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)#exit
```



```
Raisecom(config)#interface port 1  
Raisecom(config-port)#switch access vlan 100  
Raisecom(config-port)#exit  
Raisecom(config)#interface port 2  
Raisecom(config-port)#switch mode trunk  
Raisecom(config-port)#exit  
Raisecom(config)#snmp-server cfm-trap all  
Raisecom(config)#ethernet cfm enable
```

Configuration steps 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 port 1  
Raisecom(config-port)#switch mode trunk  
Raisecom(config-port)#exit  
Raisecom(config)#interface port 2  
Raisecom(config-port)#switch mode trunk  
Raisecom(config-port)#exit  
Raisecom(config)#ethernet cfm enable
```

Configuration steps 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 port 1  
Raisecom(config-port)#switch mode trunk  
Raisecom(config-port)#exit  
Raisecom(config)#interface port 2
```

Raisecom(config-port)#**switch mode trunk**

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

Raisecom(config)#**ethernet cfm enable**

Configuration steps 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 port 1**

Raisecom(config-port)#**switch mode trunk**

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

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

Raisecom(config-port)#**switch mode trunk**

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

Raisecom(config)#**ethernet cfm enable**

Configuration steps of PE_B:

Raisecom(config)#**ethernet cfm domain md-name md5-1 level 5**

Raisecom(config)#**ethernet cfm domain level 3**

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

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 all**

Raisecom(config-service)#**service remote mep 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)#exit
Raisecom(config)#interface port 1
Raisecom(config-port)#switch access vlan 100
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switch mode trunk
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 equipment 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 ma3-1-4 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 replies: < 5/0/0 > (Total/Out of order/Error)

Ping successfully.

Ping the MAC of the peer MEP on PE_A:

```
Raisecom(config)#service ma3-1-4 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>.

```
-----
```

<i>Hops</i>	<i>HostMAC</i>	<i>Ingress/EgressPort</i>	<i>IsForwarded</i>	<i>RelayAction</i>	<i>NextHop</i>
<i><1></i>	<i><AAAA></i>	<i><2/1></i>	<i><yes></i>	<i><RlyFDB></i>	<i><AAAA></i>
<i><2></i>	<i><AAAA></i>	<i><-/1></i>	<i><yes></i>	<i><RlyFDB></i>	<i><CCCC></i>
<i><3></i>	<i><CCCC></i>	<i><-/-></i>	<i><yes></i>	<i><RlyFDB></i>	<i><DDDD></i>
<i><4></i>	<i><DDDD></i>	<i><1/-></i>	<i><yes></i>	<i><RlyFDB></i>	<i><EEEE></i>
<i>!<5></i>	<i><EEEE></i>	<i><2/-></i>	<i><no></i>	<i><RlyHit></i>	<i><BBBB></i>

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>.

```
-----
```

<i>Hops</i>	<i>HostMAC</i>	<i>Ingress/EgressPort</i>	<i>IsForwarded</i>	<i>RelayAction</i>	<i>NextHop</i>
<i><1></i>	<i><AAAA></i>	<i><2/1></i>	<i><yes></i>	<i><RlyFDB></i>	<i><AAAA></i>
<i><2></i>	<i><AAAA></i>	<i><-/1></i>	<i><yes></i>	<i><RlyFDB></i>	<i><CCCC></i>
<i><3></i>	<i><CCCC></i>	<i><-/-></i>	<i><yes></i>	<i><RlyFDB></i>	<i><DDDD></i>
<i><4></i>	<i><DDDD></i>	<i><1/-></i>	<i><yes></i>	<i><RlyFDB></i>	<i><EEEE></i>
<i>!<5></i>	<i><EEEE></i>	<i><2/-></i>	<i><no></i>	<i><RlyHit></i>	<i><BBBB></i>

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 21 Switch Port Backup

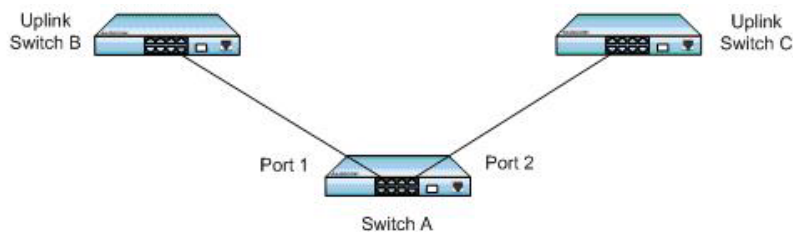
21.1 Overview

21.1.1 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.



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.

21.1.2 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.

21.2 Configure switch port backup

21.2.1 Default configuration

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

21.2.2 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 switch port backup, while when configured switch port backup STP can not be enabled.

21.2.3 Configure switch port backup

Configure switch port backup group

Step	Command	Description
1	config	Enter global configuration mode
2	interface port <i>port_num</i>	Enter port configuration mode
3	switch port backup port <i>portNum</i> [vlanlist <i>vlanlist</i>]	Configure <i>portNum</i> to backup port on <i>vlanlist</i> , <i>port_num</i> : 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

Configure restore delay

Step	Command	Description
1	config	Enter global configuration group.
2	switch port backup restore-delay <0-300>	Configure restore delay time.
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

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

- When main port and backup port are in LINK_UP state, configure restore delay to 35s, when the main port turns to LINK_DOWN state and then LINK_UP and keeps still for 35s, then the main port turn to Up state
- When main port and backup port are 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.

Configure restore mode

Step	Command	Description
1	config	Enter global configuration mode
2	switch port backup restore-mode {port-up / neighbor-discover/disable }	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

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

- 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 are 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.

Configure force-switch

Step	Command	Description
1	config	Enter global configuration mode
2	switchport backup [port portnum] force-switch	Configure force-switch. Available on master port and specify the backup port in the command.
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)# **interface port X**

Raisecom(config-port)# **switchport backup port Y force-switch**

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

Restore delay: 15s

Restore mode: neighbor-discover

Active Port(State) Backup Port(State) Vlanlist

Note: This command can force switch the data from main link to backup link, regardless of current link state.

- When the main port and backup port are both in LINK_UP state, the data is transmitting on main port. Then use force-switch command.
- After carry on the command **no switchport backup [port portnum] force-switch**, data transmission link will re-choose according to link state, selecting principle is: the up port first; main port is the priority if two up ports;

21.3 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

```

21.4 Typical configuration example

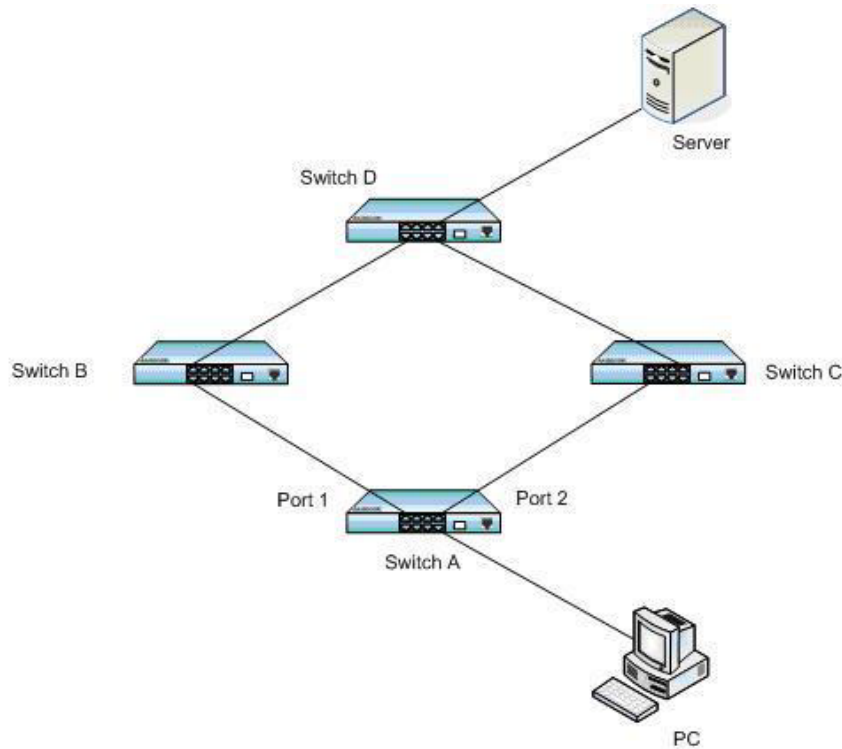
21.4.1 Network requirement

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.

21.4.2 Network structure



21.4.3 Typical configuration

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

<i>Active Port(State)</i>	<i>Backup Port(State)</i>	<i>Vlanlist</i>

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

<i>Active Port(State)</i>	<i>Backup Port(State)</i>	<i>Vlanlist</i>

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

<i>Active Port(State)</i>	<i>Backup Port(State)</i>	<i>Vlanlist</i>

1 (Up)	2(Standby)	1-100
2 (Standby)	1(Up)	101-200

Chapter 22 SSH Management

22.1 SSH Function Instruction

SSH (Secure Shell) is a protocol which is used for providing a secure remote login and other secure network services on the insecure network. When the user makes a telnet to network devices through insecure network environment, each time before sending data, SSH will automatically encrypt data. When the data arrive at their destination, SSH automatically decrypts the encrypted data, thus providing secure information safeguards to protect the network device from interception and other attacks, such as clear-text passwords. In addition, SSH provides strong authentication to protect against such a "middleman" and other attacks. SSH uses a client - server model. SSH server accepts the connection of SSH Client and provides authentication, SSH client establishes SSH connection with SSH server so that it can achieve to the SSH server through the SSH login. In addition, SSH also supports other features, such as the transmission of data can be compressed, thus speeding up the transfer speed. They can replace Telnet, or FTP, Pop and even PPP. It provides a secure 'channel'.

22.1.1 SSH Default Configuration

Function	Default
SSH server status	stop
Key pair	N/A

22.1.2 SSH Configuration

Before starting the server, user must create the server key pair at first. User creates or cancels key pair through management command of key pair, creating key pair through generate command of key pair. Only one key pair is allowed to be created in one device, so user must delete the old key pair before creating a new one.

Step	Command	Description
1	config	Enter the global configuration mode.
2	key-pair generate <i>KEYNAME</i> rsa [modulus <768-2048>] [comment <i>COMMENT</i>]	Generate SSH server key pair. <i>KEYNAME</i> : name of key pair <i>768-2048</i> : size range of modulus <i>COMMENT</i> : comments of key pair
3	ssh server <i>KEYNAME</i>	Start SSH server. <i>KEYNAME</i> : name of key pair.
4	exit	Exit the global configuration mode.
5	show key-pair <i>KEYNAME</i>	Show information of key pair.

When the SSH server starts, the user can stop it by **no SSH server**.

Once creating a key pair successfully, it is saved in device by automation until user to destroy it or format device.

Step	Command	Description
1	config	Enter the global configuration mode.
2	key-pair destroy <i>KEYNAME</i>	Destroy key pair. <i>KEYNAME</i> : name of key pair.
3	exit	Return to the global configuration mode.
4	show key-pair <i>KEYNAME</i>	Show information of key pair.

22.1.3 Monitoring and Maintenance

Command	Description
show key-pair <i>KEYNAME</i>	Show information of key pair.
show SSH server	Show server configuration information.
show SSH session	Show session information.

