RAISECOM

www.raisecom.com

ROS Switch Configuration Guide

Raisecom ROS 4 Series

200707

Legal Notices

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

Warranty.

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

Restricted Rights Legend.

Copyright Notices.

Trademark Notices

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

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

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

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

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

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

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

Microsoft Corporation.

Contact Information

Technical Assistance Center

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

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

Tel: +86-10-82883305

Fax: +86-10-82883056

World Wide Web

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

http://www.raisecom.com

Feedback

Comments and questions about how the Raisecom Operation System (ROS) works are welcomed. Please review the FAQ in the related manual, and if your question is not covered, send email by using the following web page:

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

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

export@raisecom.com

We hope to hear from you!

CONTENTS

Preface

About This Manual

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

Who Should Read This Manual

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

Compliance

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

YD/T900-1997 SDH Equipment Technical Requirements - Clock

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

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

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

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

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

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

YD/T1179- 2002 Technical Specification of Ethernet over SDH

G.703 Physical/electrical characteristics of hierarchical digital interfaces

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

levels

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

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

G.781 Synchronization layer functions

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

G.784 Synchronous digital hierarchy (SDH) management

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

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

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

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

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

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

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

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

G.841 Types and characteristics of SDH network protection architectures

G.842 Interworking of SDH network protection architectures

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

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

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

I.731 ATM Types and general characteristics of ATM equipment

I.732 ATM Functional characteristics of ATM equipment

IEEE 802.1Q Virtual Local Area Networks (LANs)

IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering

IEEE 802.3 CSMA/CD Access Method and Physical Layer Instruction

Chapter 1 Overview

1.1 Layer-2 management and hardware functions

- ✧ Port traffic mirroring (allow the traffic mirroring from any port to any port);
- ✧ Storm control: provide storm control of broadcast, multicast and DLF (Destination Lookup Failure) frames
- ✧ The static management for the ARL table of the switching chip (capacity is 8K).

1.2 Standard layer-2 protocols

- ✧ IEEE802.1w Rapid Spanning Tree Protocol;
- ✧ IEEE802.1D/W, IEEE802.1Q;
- ✧ IGMP Snooping(multicast address:256);

1.3 Management Capability

- ✧ Support cluster management function;
- ✧ Support SNMP(RFC1157), SNMPv2 and SNMPv3;
- ✧ Support CONSOLE management;
- ✧ Support remote management by TELNET;
- ✧ Support automatic configuration function, that is to say the switches can download configuration files automatically from assigned network management server.
- ✧ Support RMON 1, 2, 3 and 9 groups;

1.4 DHCP

- ✧ Support DHCP SERVER and DHCP RELAY function (layer-3 supported) after being authenticated.

1.5 Rate limiting

- ✧ Rate limiting function based on per port.

1.6 Layer-3 functions

- ✧ Support static routing;
- ✧ RIP/OSPF routing protocol;
- ✧ Support wire-speed forwarding of layer-3 packets.

Chapter 2 How to Use Command-line

2.1 Environment

- ✧ Hardware requirement: ISCOM series switches
- ✧ Software requirement: ROS 3.0.

2.2 Command line mode

Mode	Mode description	Access	Prompt
User EXEC mode	To connect the remote device, change terminal settings on a temporary basis, perform basic tests, and display system information.	Login	Raisecom>
Privileged EXEC mode	In this mode, user can configure the basic information of a switch.	From User EXEC mode, enter **enable** and password	Raisecom#
Global configuration mode	Use this command to configure parameters that apply to the whole switch.	From **Privileged EXEC mode** mode, enter **config.**	Raisecom(config)#
Physical interface configuration mode.	Configure parameters of physical Ethernet interface.	From global configuration mode enter **interface port *portid*** command.	Raisecom(config-port)#

Physical interface range configuration mode	In this mode, configure parameters of more than one Ethernet physical interface.	From global configuration mode enter **interface range** ***port-list*** command.	Raisecom(config-range)#
Layer-3 interface configuration mode.	Configure the L3 interface parameter in this mode.	Under global configuration mode, type **interface ip** id command.	Raisecom(config-ip)#
VLAN configuration mode	Configure or modify VLAN parameters for VLANs	Under global configuration mode, type **Vlan** ***vlan_id*** command	Raisecom(config-vlan)#
Class Map configuration mode	Configure parameters of particular data flows in this mode.	From global configuration mode, type **class-map** class-map-name **[match-all | match-any]** command.	Raisecom(config-cmap)#
Policy Map configuration mode	Configure the data flow of class-map defined encapsulation and classification.	From global configuration mode, type **policy-map** policy-map-name command.	Raisecom(config-pmap)#
Traffic classification configuration mode	Configure the data flow under this mode.	From policy map exec mode, type **class-map** class-name command.	Raisecom(config-pmap-c)#

Cluster configuration mode	Configure the cluster under this mode.	From global configuration mode, type **cluster** command.	Raisecom(config-cluster)#
ACL configuration mode	Configure ACL filtering table	From global configuration mode, type access-list-map <0-399> {permit | deny} command.	Raisecom(config-aclmap)#

2.3 Getting help

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

2.4 Use Commands History

Switch records 20 history commands in his history buffer by default. User can use Raisecom>**terminal history** <*0-20*> command to change the number of history commands that will be recorded.

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

2.5 Using Editing Features

up arrow:	last entered command
down arrow:	next entered command
left arrow:	move a character left
right arrow:	move a character right
backspace:	delete a character in front of the cursor
Ctrl+d:	delete a character at the cursor
Ctrl+a:	move the cursor to the beginning of the command line
Ctrl+e:	move the cursor to the end of the command line
Ctrl+k:	delete all the characters to the right the cursor
Ctrl+w:	delete all the characters to the left of the cursor
Ctrl+u:	delete the row all
Ctrl+z:	exit from other modes to privileged mode

Chapter 3 System Command Configuration

This chapter introduces the basic system configuration and user management.

3.1 Basic system command and configuration

chinese show help information of the command in Chinese

english show help information of the command in English

clear clear the information on the screen

list Use this command to show all commands under the mode in the form of list.

clock set: Change system time.

3.2 Configuration files and boot files management

3.2.1 Configuration files.

- ✧ Default name for current configuration files is: startup_config.conf;
- ✧ Use write command to save configuration information to flash, when the system is restarted, the configuration information will be reloaded automatically.
- ✧ Use erase command to delete files.
- ✧ With upload and download commands, user can upload configuration file startup_config.conf to the server, or download new configuration information from the server by TFTP protocol or by FTP protocol.
- ✧ Use show startup_config command to show saved configuration information.
- ✧ Use show runnging_config command to show current system configuration information.

3.2.2 Startup files

- ✧ That is program file, the program file name for current system is system_boot.z;
- ✧ User can use TFTP or FTP software to upload files to the server or download program files from the server.
- ✧ User dir command to check system files in flash.
- ✧ Use show version command to check software version information.

3.3 User management

The system has a default username **raisecom** and the password **raisecom;**

Add a new user, the steps are as follows:

Step	Command	Description
1	**user** *USERNAME* **password** { **no-encryption | md5** } *PASSWORD*	·*USERNAME* Username; ·**Password** password key word; · **{no-encryption | md5}** use **no-encryption or md5**

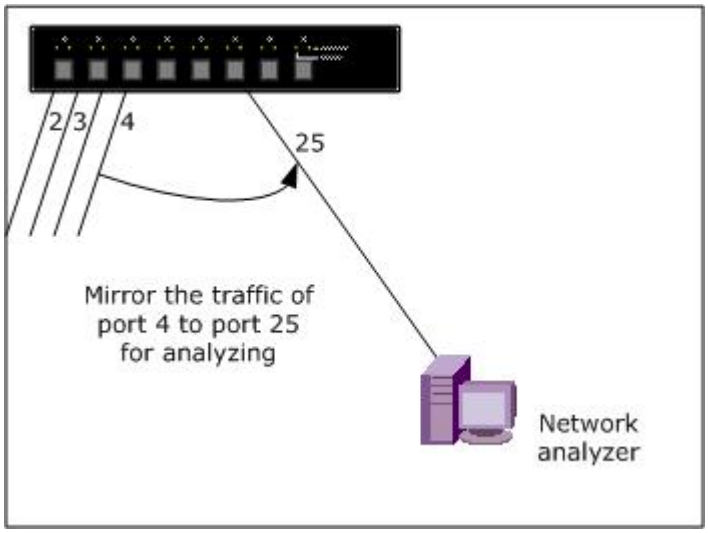
		encryption password. ·*PASSWORD* password information;
2	**user** *USERNAME* **privilege** *<1-15>*	·*USERNAME* username; ·**Privilege** privilege key word; ·***<1-15>*** user privilege.
3	**Write**	Save configuration information
4	**show user**	Show user information.

Chapter 4 Mirror Function Configuration

This chapter includes the following parts:

- ✧ Enable or disable mirror function.
- ✧ Configure the monitor ports
- ✧ Configure the source port

Network administrator can analyze network traffic passing through one port by using mirror function, sending the traffic of one port to a specified port according to configured rules for real-time analysis. Administrator can use this function to analyze network traffic on assigned ports. Mirror function allows more than one target port's incoming or outgoing traffic to be monitored but only one monitor port. It is disabled by default. The following figure show how the mirror function works.



4.1 Enable or disable mirror function

All the configurations are enabled after the mirror function is enabled globally.

Step	Command	Description
1	**config**	Access global configuration mode
2	**mirror {enable | disable}**	Enable/disable mirror function globally.
3	**exit**	Exist from global configuration mode to privileged EXEC mode.
4	**show mirror**	Show mirror configuration information.

4.2 Configure the monitor port

Monitor port: the monitor port will receive a copy of traffic from source port/ports.
The traffic of source port will be copied to monitor port, so that network administrators can analyze the network. Port 1 is monitor port by default, the source port and the monitor can not be same as source port.

Step	Command	Description
1	**config**	Access global configuration mode.
2	**mirror monitor-port** *port_number*	Set the monitor port. *port_number* is physical port number, range is 1-26.
3	**exit**	Exist from global configuration mode and enter **privileged EXEC mode**.
4	**show mirror**	Show mirror configuration

Use **no mirror monitor-port** command to recover to default settings.

4.3 Configure the source port.

Source port: a source port is a target port that you monitor for network traffic analysis.
When the mirror function is enabled, the egress/ingress traffic of source port will be copied to the monitor port. Users should configure the direction of monitored traffic (received, transmitted or bidirectional) to be monitored when configuring source port: both, ingress and/ egress. The port cannot be set to source port if it has been set to monitor port. All Raisecom switches support unlimited number of source ports.

(1) Mirror both the ingress and egress traffic of source port.

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**mirror source-port-list both** *port-list*	Set the source port and the direction of monitored traffic is bidirectional: that is copy both the ingress and egress traffic of source port to monitor port. *Port-list* is the physical port list; range is 1-26, comma "," and "-"to set multiple ports setting.

3	**exit**	Exist from global configuration mode to privileged EXEC mode
4	**show mirror**	Show mirror function configuration information.

(2) Mirror the ingress traffic of source port.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mirror source-port-list ingress** *port-list*	Set the source port and the direction of monitored traffic is ingress: that is copy the ingress traffic of source port to monitor port. *Port-list* is the physical port list; range is 1-26, use "," and "_" for multiple source ports setting.
3	**exit**	Exist from global configuration mode to privileged EXEC mode
4	**show mirror**	Show mirror function configuration information.

(3) Mirror the egress traffic of source port.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mirror source-port-list egress** *port-list*	Set the source port and the direction of monitored traffic is egress: that is copy the egress traffic of source port to monitor port. *Port-list* is physical port list, range is 1-26, can use "," and "-"for multiple source ports setting.
3	**exit**	Exist from global configuration mode to privileged EXEC mode
4	**Show mirror**	Show mirror function configuration

	information.

(4) Mirror the ingress traffic of some source ports and egress traffic of some other source ports through on command:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**mirror source-port-list ingress** *port-list* **egress** *prot-list*	Mirror the ingress traffic of some source ports and egress traffic of some other source ports. *Port-list* is the physical port list, range is 1-26, use ","and"-"for multiple source ports setting.
3	**exit**	Exist from global configuration mode to privileged EXEC mode
4	**show mirror**	Show mirror function configuration information.

Use **no mirror source-port-list** command to clear the mirroring of the source port.

Use global configuration command **no mirror all** to clear all the mirror settings, and use **show mirror** command to show all the mirror settings.

4.4 Example

Set port 26 as monitor port, monitoring the ingress traffic of port 5-8 and egress traffic of port 7-12.

```
iscom2826#config
iscom2826(config)#mirror enable
iscom2826(config)#mirror monitor-port 26
iscom2826(config)#mirror source-port-list ingress 5-8 egress 7-12
iscom2826(config)#exit
iscom2826#show mirror
Mirror: Enable
Monitor port: 26
-----------the ingress mirror rule-----------
Mirrored ports: 5-8
-----------the egress mirror rule-----------
Mirrored ports: 7-12
```

Chapter 5 Port Rate Limiting Configuration

This chapter describes the port rate limiting of Raisecom ISCOM series switches.

Port rate limiting allows the network administrator to control the maximum rate of the received and transmitted traffic of the physical port/ports. Rate limiting is configured on ports at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limiting will be normally forwarded, while exceeded will be dropped.

Rate limiting can be applied to individual port. When a port is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic will be dropped while conforming traffic is forwarded directly.

The rate limiting function of Raisecom series switches is based on hardware, enabling the efficient utilizing of available bandwidth and network resources. The hardware based rate limiting ensures that the overall performance of the switch will not be affected at all when performing the rate limiting on ports.

Raisecom port rate limiting function provides bidirectional rate limiting: both ingress and egress, allowing carriers and service providers to configure different rate limits depending on utilization and traffic requirements efficiently.

5.1 Configure port rate liming of ingress traffic

(1) Configure the rate limiting and the burst of ingress traffic.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rate-limit port-list** {*all* | *port-list*} **ingress** *rate* [*burst*]	Configure the rate limiting and the burst of ingress traffic. *port-list* physical port number, range is 1-26, use "," and "-" for multiple ports' rate limiting. *rate* stands for the maximum bandwidth allowed to be transmitted, unit is kbps, range is 1-1048576. (The actual value may be a little bit different from the configured value because it can only be the exponential of 2).

		burst: unit is KBps, the available value is 1-512. *The real value can be different with the configured value.* *Ingress:* rate limiting of the incoming traffic
3	**exit**	Exist from global configuration mode and enter privileged EXEC mode.
4	**show rate-limit port-list** [*port-lis*]	Show the rate limiting of the port *port-list* physical port number, range is 1-26,use "," and "-" for multiple ports configuration.

(2) Configure bandwidth and the burst of egress traffic.

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**rate-limit port-list** {*all* | *port-list*} **egress** *rate* [*burst*]	Configure the rate limiting and the burst of egress traffic. *port-list* physical port, range is 1-26, use"," and"-"for multiple ports rate limiting. *rate* stands for the maximum bandwidth allowed to be transmitted, unit is kbps, range is 1-1048576. (The actual value may be a little different from the configured value because it can only be the exponential of 2). burst: unit is KBps, the available value is 1-512. *The real value can be different with the set value.* *Egress:* ate limiting of the outgoing traffic
3	**exit**	Exist from global configuration mode and enter privileged EXEC mode.

4	**show rate-limit port-list** [*port-list*]	Show the bandwidth limitation for the port. *port-list*: physical port number, range is 1-26,use “,” and “-“ for multiple ports configuration.

Use global configuration command **no rate-limit port-list** {*all* | *port-list*} {*both* | ingress | egress} to clear the rate limiting configuration.

5.2 Example

Set the ingress bandwidth of port 5-7 to 1000Kbps, burst is 64kbps, port 1,9 egress bandwidth is 4096kbps, burst is 70kbps.

Raisecom#**config**

ISCOM2826(config)# rate-limit port-list 5-7 ingress 1000 64

Set successfully

Actual ingress rate of FE port: 1000

Actual ingress burst of FE port: 64

ISCOM2826(config)# rate-limit port-list 1,9 egress 4096 60

Set successfully

Actual Egress rate of FE port: 5000

Actual egress burst of FE port: 64

ISCOM2826(config)#exit

Raisecom# show rate-limit port-list 1,5-7,9

I-Rate: Ingress Rate

I-Burst: Ingress Burst

E-Rate: Egress Rate

E-Burst: Egress Burst

Port	I-Rate(Kbps)	I-Burst(KBps)	E-Rate(Kbps)	E-Burst(KBps)
1	0	0	5000	64
5	1000	64	0	0
6	1000	64	0	0
7	1000	64	0	0
9	0	0	5000	64

Chapter 6 Managing the MAC Address Table

The MAC address table contains the MAC address information which is used by switch for the packets forwarding between ports. The switch will record the source MAC address, port number and VLAN ID of incoming packets.

The address table includes these types of addresses:

*Dynamic address: a source MAC address that the switch learns and then ages when it is not in use;

*Static address: a manually entered uni-cast or multicast address that does not age and that is not lost when the switch resets.

This chapter includes the following parts.

- ✧ Configure the aging time of MAC address.
- ✧ Enable/disable the MAC address learning function.
- ✧ Configure static MAC addresses.
- ✧ Search MAC address.
- ✧ Clear the entries MAC address table.
- ✧ Show MAC address.

6.1 Configure the aging time of MAC address

Dynamic addresses are incoming packets' source MAC addresses switch learned, the dynamic addresses will be aged if they are not used for some time.

If the aging time is too short, the MAC address will be removed from MAC address table prematurely. And when the switch receives a packet with an unknown destination, the packet will be flooded to all the ports within the VLAN. The unnecessary flooding will occupy more bandwidth. If the aging time is too long, the MAC address table will be filled with unused MAC address, and no more new MAC address can be learned.

The default aging time of Raisecom series switches is 300 seconds.

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**mac-address-table aging-time** { *0* | *time* }	Set the aging time of MAC address table. 0 stands for MAC address will not be aged

		time is the target MAC address aging time, unit is second, range is 3-765, and default value is 300.
3	**exit**	Exist from global configuration mode and enter privileged EXEC mode.
4	**show mac aging-time**	Show MAC address aging time.

Recover the default value of aging time, and use **no mac-address-table aging-time**.

For example:

Set the aging time to 500 seconds.

```
Raisecom#config
Raisecom(config)#mac-address-table aging-time 500
Raisecom(config)#exit
Raisecom#show mac aging-time
Aging time: 500 seconds.
```

Disable MAC address aging

```
Raisecom#config
Raisecom(config)#mac-address-table aging-time 0
Raisecom(config)#exit
Raisecom#show mac aging-time
Auto-aging is disable!
```

6.2 Configure static MAC address

Static MAC address is a manually entered uni-cast or multicast address that will not be aged and is retained when the switch restarts. There is no static MAC address by default.

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**mac-address-table static** *HHHH.HHHH.HHHH* **vlan** *vlan_id* **port** *port-number*	Set the static MAC address. *HHHH.HHHH.HHHH is the static MAC address which will be set; format is hex,* dotted notation for every four characters. Vlan_id range is 1-4094. *port_number* is the physical port number, range is 1-26.
3	**exit**	Exist from global configuration

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

Use **no mac-address-table static** HHHH.HHHH.HHHH **vlan** *vlan_id* **port** *port-number* command to remove static MAC address.

For example: add a static MAC address 1234.1234.1234, belongs to VLAN 1, port 10.

```
Raisecom#config
Raisecom(config)# mac-address-table static unicast 1234.1234.1234 vlan 1 port 10
Raisecom(config)#exit
Raisecom#show mac-address-table static
Port        Vlan        Static Mac Address
---------------------------------------
10          1           1234.1234.1234
```

6.3 Enable/disable dynamic MAC address learning function

Dynamic MAC address learning function can be enabled or disabled based on per port:

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

	1-26.

For example:

Disable the MAC address learning function of port 10.

Raisecom#config

Raisecom(config)#mac-address-table learning disable port 10

Raisecom(config)#exit

Raisecom#show interface port 10

R: Receive Direction

S: Send Direction

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

---

10 enable down auto off/off disable

6.4 Clear MAC address table

Clear layer-2 MAC address table entries of the switch, includes static and dynamic MAC address.

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

For example:

Delete the dynamic MAC addresses in the MAC address table.

Raisecom#clear mac-address-table dynamic

6.5 Show MAC address table.

Show MAC address information of the switch.

Step	Command	Description
1	**show mac-address-table l2-address** [{**count** [{**port**	Show the MAC address information for the switch.

	port-number | **vlan** *vlan_id*}] | **port** *port-number* | **vlan** *vlan_id*}]	**Count** the number of MAC address related to a port *port_number physical port, range is 1-26*. *vlan_id* rane is 1-4094.

For example:

Show the MAC address related to port 1.

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

MAC address port VLAN

0001.0297.60F5 1 1

0001.0340.6A0B 1 1

0001.0340.6B23 1 1

0002.1EE6.5157 1 1

0002.1EE6.5643 1 1

0002.1EE6.5820 1 1

0002.1EF2.200F 1 1

0002.1EF7.6271 1 1

.

.

……

For example:

Show the total number of the entire MAC address related port 1.

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

MAC address count of port 1: 97

6.6 Search particular MAC address.

Search the MAC address within the switch for the relative information.

Step	Command	Description
1	**search mac-address** *HHHH.HHHH.HHHH*	Search MAC address *HHHH.HHHH.HHHH: the MAC address which will be searched, format is hexdecial, dotted notation for every four characters.*

For example:

Add static MAC address 1234.1234.1234, and search that MAC address for the relative

information.

Raisecom#config

Raisecom(config)#mac-address-table static 1234.1234.1234 vlan 1 port 10

Raisecom(config)#exit

Raisecom#search mac-address 1234.1234.1234

MAC address	port	VLAN	Symbol
1234.1234.1234	10	1	Static

Chapter 7 Configuring the Switch Interfaces

This chapter includes following parts:

- ✧ Configure the speed and duplex mode
- ✧ Configure the 802.3x flow control function of the port.
- ✧ Open or shutdown the port.

7.1 Configure the speed and duplex mode of the port.

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.

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**interface port** *port-number* **interface range** *port-list*	Enter Ethernet physical interface configuration mode or physical interface range configuration mode. *port_number* is the physical interface, range is 1-26. *port-list r*ange is 1-26, use "," and "-"for multiple interfaces configuration.
3	**speed** {auto | 10| 100 |1000 } **duplex** { full | half }	Set the speed and duplex mode of the port. *auto*: represents that both the speed and duplex are set according to the result of auto negotiation. *10*: represents that the speed is set to 10Mbps. *100*: represents that the speed is set to 100Mbps. *1000*: represents that the speed is set to 1000Mbps. *full*: set the duplex mode to full duplex.

		half: set the duplex mode to half duplex.
4	**exit**	Exit from Ethernet physical interface configuration mode to global configuration mode.
5	**exit**	Exit from global configuration mode to privileged EXEC mode
6	**show interface port** *port-number*	Show the status for the port. *port_number* physical port, range is 1-26.

Use Ethernet physical port configuration command **speed auto** to set the speed and duplex mode in auto negotiation mode.

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

Raisecom**#config**
ISCOM2826(config)**#interface port** 15
ISCOM2826(config-port)**#speed** *10*
ISCOM2826(config-port)**# duplex** full
ISCOM2826(config-port)**#exit**
ISCOM2826(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

7.2 Configure 802.3x flow control function of the port

Flow control function enables the Ethernet ports to control traffic rate during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive more traffic, it will notify the other end port to let it stop sending packets until the condition clears.

If local device detects any congestion at its end, it can notify the remote device by sending a pause frame. When receives the pause frame, the remote device will slow its sending rate or stop sending packets to accommodate with local device, enabling no packet loss.

The flow control function of Raisecom series switches is set on both RX and TX direction, that is to say, you can set the interface's ability to receive and send pause frame to on/off separately. By default, flow control function is disabled on both directions.

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

For example: Set the flow control for port 10.

Raisecom**#config**

ISCOM2826(config)# **interface port** *10*

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

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

ISCOM2826(config)**#exit**

Raisecom#**show interface port** *10*

R: RX Direction

S: tx Direction

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

---

10 enable down auto on/off enable

7.3 Open up or shut down the physical port

Ethernet port can be open or shutdown flexibly according to user requirements:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**interface port** *port-number* **interface range** *port-list*	Enter Ethernet physical port configuration mode or interface range configuration mode. *port_number* physical port number, range is 1-26. *port-list* port list, range is 1-26,can use"," and "-" for multiple setting.
3	{ **shutdown | no shutdown** }	Close or start physical port. **shutdown** shut down physical port. **no shutdown** open up physical port.
4	**exit**	Exist from physical port configuration mode and enter global configuration mode.
5	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
6	**show interface port** *port-number*	Show port status. *port_number* physical port number, range is 1-26.

For example: shutdown port 20.

Raisecom#**config**

ISCOM2826(config)# **interface port** 20

ISCOM2826(config-port)#**shut down**

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

ISCOM2826(config)**#exit**

Raisecom**#show interface port** *20*

R: Receive Direction

S: Send Direction

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

Chapter 8 Strom Control

A packet storm occurs when a large number of broadcast, unicast, or multicast packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. Storm control is configured for the switch as a whole but operates on a per-port basis. By default, storm control is enabled.

Storm control uses thresholds to limit the forwarding of broadcast, unicast, or multicast packets. The thresholds can either be expressed as a percentage of the total available bandwidth that can be used by the broadcast, multicast, or unicast traffic (x% of the port's available rate), or as the rate at which the interface receives multicast, broadcast, or unicast traffic (PPS: packet per second).

8.1 Enable the control function

This function is used to enable/disable storm control function globally.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**storm-control {**broadcast | multicast | dlf | all**} {**enable | disable**}**	Enable/disable the storm control function, and configure the packet limitation for broadcast packet, multicast packet and DLF packet. *Broadcast*: broadcast packet. *multicast*: multicast packet. *dlf*: destination lookup failure unicast packet. all: broadcast, multicast and dlf unicast packets.
3	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
4	**show storm-control**	Show storm control status.

Example: disable the storm control of broadcast packet.

Raisecom**#config**

ISCOM2826(config)# **storm-control** broadcast disable

ISCOM2826(config)**#exit**

Raisecom#show storm-control

Broadcast: Disable
Multicast: Enable

Unicast destination lookup failed (DLF): Enable

Threshold: 1024 pps

8.2 Threshold of storm control

Storm control uses rising and falling thresholds to block and then restore the forwarding of broadcast, multicast and DLF unicast packets.

Configure the threshold of storm control. Unit is pps (packet per second).

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**storm-control pps** *value*	Set the threshold of storm control. Threshold of storm-control packet. Range is 0-262143.
3	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
4	**show storm-control**	Show the status of storm control

Example: set the threshold of storm control to 2000 packet per second.

Raisecom#**config**

ISCOM2826(config)# **storm-control pps** 2000

ISCOM2826(config)#**exit**

Raisecom#show storm-control

Broadcast: Disable

Multicast: Enable

Unicast destination lookup failed(DLF): Enable

Threshold: 2000 pps

Chapter 9 Shared VLAN

In Shared VLAN Learning (SVL), the switch makes use of address information learnt across a number of VLANs in making forwarding decisions in connection with other VLANs. In Independent VLAN Learning (IVL), the switch makes use of address information learnt in one VLAN only and does not use this information in making forwarding decisions with any other VLAN.

In SVL, all VLAN share the same learnt MAC address information, regardless of which VLAN the information was learnt in. In IVL, each VLAN makes use only of MAC address information learnt within that VLAN.

9.1 Enable SVL

Step	Command	Description
1	**config**	Enter global configuration mode
2	**svl** { **enable** | **disable** }	Enable/disable SVL function.
3	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
4	**show svl**	Show SVL status.

Example: start SVL mode.

Raisecom # **config**

ISCOM2826 (config)# **svl** enable

ISCOM2826 (config)# **exit**

Raisecom # **show svl**

SVL: Enable

9.2 Configure SVL of port

MAC address learned by that port will be available for all the other VLAN.

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**interface port <1-26>**	Enter port configuration mode
3	**switchport svl vlanlist {1-4094}**	Set SVL of the port.
4	**end**	Exit from port configuration mode and enter privileged EXEC mode.
5	**show switchport [<1-26>] svl vlanlist**	Show the port and VLAN list.

For example: Set the shard VLAN of port 1 to 1-4.

Raisecom**#config**

ISCOM2826(config)**#interface port** 1

ISCOM2826(config-port)**# switchport svl vlanlist 1-4**

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

ISCOM2826(config)**#exit**

Raisecom# show switchport 1 svl vlanlist

Port SVL VLAN list

---

1 1-4

9.3 Configure SVL default VLAN

If there is no SVL VLAN list configuration of a port, MAC address table is shared with SVL default VLAN. The default SVL VLAN configuration is as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**svl default vlan <1-4094>**	Set SVL default VLAN
3	**exit**	Withdraw global configuration mode and enter privileged user mode.
4	**show svl default vlan**	Show SVL default VLAN.

Example 1: Set VLAN 3 as SVL default VLAN.

Raisecom **# config**

ISCOM2826 (config)**# svl default vlan** 3

ISCOM2826 (config)**# exit**

Raisecom **#** show svl default vlan

SVL default vlan: 3

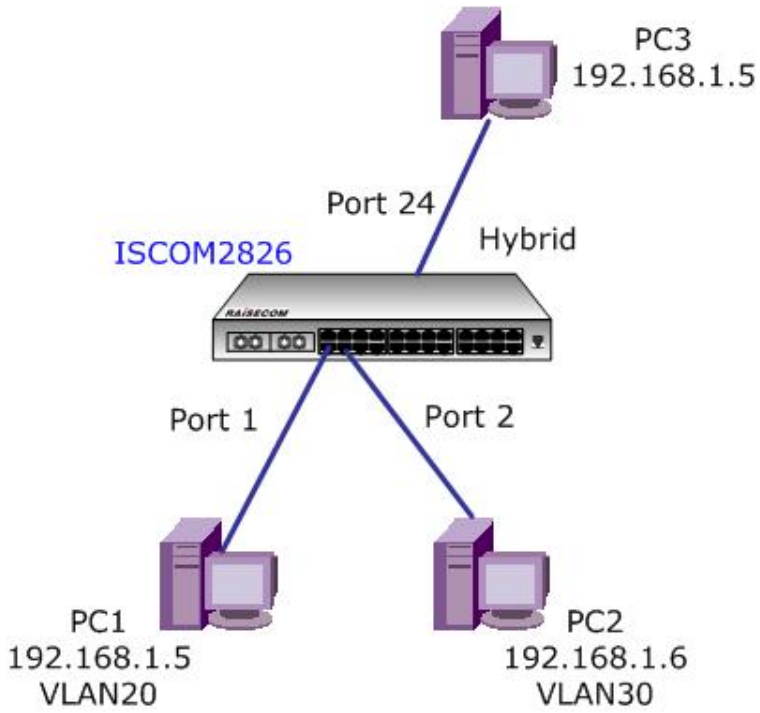
9.4 SVL typical application

A VLAN is a switched network that is logically segmented without regard to the physical locations of users. Any switch port can belong to a VLAN, and unicast, multicast and broadcast packets are forwarded and flooded within the limitation of a VLAN. So VLAN is widely used by carriers and network administrators for eliminating conflict domains and separating users.

However, the total number of VLAN is limited to 4096 for carriers and network administrators. In some condition an access switch can only have one available VLAN ID or cannot have an available VLAN ID at all, while network administrators also need to use VLAN to separate end users for efficiently utilizing

bandwidth.

The following example is a typical application:



Switch port 1 and port 2 are connected with two different users: PC 1 (192.168.1.5) and PC 2 (192.1687.1.6). And there is not enough available VLAN ID for this switch, the incoming and outgoing packets are all untagged. So problems arise here:

1 How can we separate the two users?

2 If we use VLAN to separate the users, how can port 1 and port 2 communicate with uplink port 24?

The answer is that we can use SVL function to let uplink port 24 use the MAC addresses learned by VLAN 20 and VLAN 30.

Configurations:

Raisecom(config)#interface port 1

Raisecom(config-port)#switchport access vlan 20 /*Configure port 2 to belong to VLAN20*/

Raisecom(config)#interface port 2

Raisecom(config-port)#sw access vlan 30 /* Configure port 3 to belong to VLAN30*/

Raisecom(config)#interface port 24

Raisecom(config-port)#switchport mode hybrid /* Configure port 24 in hybrid mode*/

Raisecom(config-port)#switchport hybrid untagged vlan 1,20,30 /*Port 24 will forward the packets of VLAN 20 and 30 in untagged mode*/

Raisecom(config-port)#switchport svl vlanlist 20,30 /*Port 24 can utilize the MAC addresses learned by VLAN 20 and VLAN 30*/

Raisecom(config)#svl enable /*Enable SVL function*/

Chapter 10 Packets Transparent Transmission

10.1 Overview

Some transmission control packets need to be forwarded through the whole network, BPDU packets for example. So layer-2 switches need to transparently forward some packets such as BPDU, Dot1x, LACP, GARP, GMRP and GVRP to make it more convenient for other network elements.

10.2 Configure the port to transparently transmit some control packets

Configure the port and the control packets type that need to be transparently transmitted. By default, switch port will not forward the control packets any more once it receives.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**relay {**bpdu | dot1x | lacp | garp | gmrp | gvrp | all**} port-list** *port-list*	Assign the port and configure the types of control packets that will be transparently transmitted. Packet types: bpdu, dot1x, lacp, garp, gmrp and gvrp *port-list* physical port list, use "," and "-" for multiple ports configuration, range is 1-26.
3	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
4	**show relay port-list**	Show the configuration of packets transparent transmission port.

Clear the function of transparent transmission of a port: use command **no relay {**bpdu | dot1x | lacp | garp | gmrp | gvrp | all**} port-list** *port-list*.

Example: let port 1-4 transmit BPDU packet transparently, 3-6 transmit Dotlx packet transparently.

```
iscom2826#config
iscom2826(config)# relay bpdu port-list 1-4
Set forwarding ports successfully.
iscom2826(config)# relay dot1x port-list 3-6
Set forwarding ports successfully.
iscom2826(config)#exit
 iscom2826# show relay port-list
```

```
Type          Ports
---------------------------
BPDU          1-4
Dot1x         3-6
LACP          --
GARP          --
GMRP          --
GVRP          --
```

10.3 Forward DLF (Destination Lookup Failure) packets

In default status, the DLF unicast packets will be dropped locally. But in some condition, DLF packets need to be broadcasted.

DLF packets forwarding is disabled by default. The configuration steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**dlf-forwarding {**enable | disable**}**	Whether to broadcast DLF message or not. Enable: enable broadcast. Disable: disable broadcast.
3	**exit**	Exit from global configuration mode and enter privileged EXEC mode.
4	**show dlf-forwarding**	Show DLF transmission configuration.

Example: enable the forwarding of DLF packets.

```
iscom2826#config
iscom2826(config)# dlf-forwarding enable
SUCCESS !
iscom2826(config)#exit
 iscom2826# show dlf-forwarding
 DLF-forwarding: Enable
```

Chapter 11 Management Port Configuration

An IP address is used for management access to the switch over the network and it provides a virtual management interface for network administrators. Raisecom series switches support more than one layer-3 management IP address which can belong to VLANs. Use **ip address** command to configure the interface IP address and specify the related VLAN, use **no ip address** command to delete it. Please refer to chapter 13 for the VLAN configuration.

ISCOM2826 supports 15 layter-3 management interfaces, and each interface corresponds to a static VLAN. One VLAN can only associate with one management interface.

Following procedures show how to create three layer interface and IP configuration:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**interface ip** <0-14>	Enter Ethernet layer-3 interface configuration mode.
3	**ip address** *ip-address [ip-mask] vlan-id*	Set the IP address of layer-3 interface and associated static VLAN ID.
4	**exit**	Exit to global configuration mode.
5	**exit**	Exit to privileged EXEC mode.
6	**show interface ip**	Show layer-3 management interface configuration

Chapter 12 Link Aggregation Control Protocol

12.1 About link aggregation control protocol (LACP)

Link aggregation or trunking is a method of combining physical network links into a single logical link for increased bandwidth. With link aggregation we are able to increase the capacity and availability of the communications channel between switches. Two or more gigabit Ethernet connections are combined in order to increase the bandwidth capability and to create resilient and redundant links. A set of multiple parallel physical links between two switches is grouped together to form a single logical link.

Link aggregation also provides load sharing where the processing and communications activity is distributed across several links in a trunk of that no single link is overwhelmed.

Raisecom series switches support up to 6 trunk groups and there can be 8 ports in each group for the increasing the transmission capacity and availability.

This chapter describes the following parts:

- ✧ Enable or disable trunking function
- ✧ Add or delete trunk group
- ✧ Set the load sharing mode for all the trunk groups.

12.2 Enable or disable trunking function

Disable or enable the trunking (LACP) function:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**trunk {enable|disable}**	Enable or disable trunking function

Example: disable the trunking function

Raisecom#config

Raisecom(config)#trunk disable

Raisecom(config)#exit

12.3 Add or delete trunk group

Interfaces in one trunk group will act as a single logical link.

User can add or delete trunk group based on following steps.

Step	Command	Description

1	**config**	Enter global configuration mode.
2	**trunk group** *trunk-group-id portlist*	Set trunk group.

Example: Create trunk group 3, port 1, 5, 6 and 7 are included.

Raisecom#config

Raisecom(config)#trunk-group 3,1, 5-7

Raisecom(config)#exit

12.4 Set load sharing mode

Interfaces in one trunk group will act as a single logical link, and the load sharing mode decides how the interfaces in one trunk group share the loads.

There are 6 kinds of load sharing mode:

- ✧ **smac** choose the forwarding port based on source MAC address.
- ✧ **dmac** choose the forwarding port based on destination MAC address.
- ✧ **sxordmac** select forwarding port based on logical “or” of source and destination MAC addresses.
- ✧ **sip** choose forwarding port based on source IP address.
- ✧ **dip** choose forwarding port based on destination IP address.
- ✧ **sxordip** select forwarding port based on logical “or” of source and destination IP addresses.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**trunk loading-sharing mode {smac | dmac | sxordmac | sip | dip | sxordip}**	Set the load sharing mode for all the trunk groups.

Example: set the load-sharing mode based on source MAC address for all the trunks groups .

Raisecom#config

Raisecom(config)#trunk loading-sharing mode smac

12.5 Maintenance

User can use show command to check associated configuration of trunking.

Step	Command	Description
1	**show trunk**	Whether to start the trunking function, load sharing mode, ports that belong to each trunk group and current efficient ports of the group.

Use **show trunk** command to display trunking information, load sharing mode, ports that belong to trunk group and current efficient ports of the group.

Current efficient ports are the ports which are transmitting packets:

```
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
```

Chapter 13 MSTP configuration

【support device】

ISCOM2000/2100/2800/2900/3000 series

- ✧ MSTP overview
- ✧ MSTP default configuration list
- ✧ MSTP configuration guide and limit
- ✧ MSTP configuration list and explaination
- ✧ MSTP monitor and maintenance

13.1 MSTP overview

MSTP stands for Multiple Spanning Tree Protocol, which is compatible with SpanningTree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP). STP is not fast in state transition. Even on a point-to-point link or an edge port, it has to take an interval twice as long as forward delay before the port transits to the forwarding
state. RSTP converges fast, but has the following drawback like STP: all the network bridges in a LAN share one spanning tree and the redundant links cannot be blocked based on VLANs. Packets of all VLANs are forwarded along one spanning tree.MSTP makes up for the drawback of STP and RSTP. It not only converges fast, but also allows the traffic of different VLANs to be distributed along their respective paths, which
provides a better load-balance mechanism for the redundant links. MSTP keeps a VLAN mapping table to associate VLANs with their spanning trees. Using MSTP, you can divide one switching network into multiple regions, each of which can have multiple spanning trees with each one independent of others. MSTP prunes
the ring network into a loop-free tree to avoid the generation of loops and infinite circulations. It also provides multiple redundant paths for data forwarding to implement the load-balance mechanism of the VLAN data.

13.2 MSTP default configuration list

	attribute	Default vaule
1	The work mode is STP	MSTmode
2	Max hop of switch MST region	20
3	Network diameter	7
4	Max send speed of interface	3 packages/ Hello Time
5	Time parameter——Hello Time	2
6	Time parameter——Forward Delay	15
7	Time parameter——Max Age	20
8	Switch priority（instance）	32768
9	Port priority（instance）	128
10	Port cost（instance）	<=10Mbps：2000000

	<=100Mbps：200000 <=1000Mbps：20000 <=10000Mbps：2000 <=100000Mbps：200 <=1000000Mbps：20 <=10000000Mbps：2

13.3 MSTP configuration guide and limit

MSTP configuration guide and limit

- ✧ Max Multiple Spanning Tree Instance (MSTI):16
- ✧ Range of MSTI: 1-4095, 1-4094 VLAN, one or multiple VLAN can be mapped to one MSTI. Each VLAN can only be belonged to one MSTI (if one multiple MSTIs are set, only one can take effect).
- ✧ Maxhops of MST restrict the scale of MST region.
- ✧ Network Diameter of restrict the network scale, actually the number of region (for STP / RSTP switch, each switch is a region), so only the CIST switch can take effect.
- ✧ The time parameter is a range, which can only take effect on the CIST root switch.
- ✧ When set the root and backup root switch, it is suggested that do not set the priority.

13.4 MSTP configuration list and explaination

- ✧ Enabling/Disabling MSTP
- ✧ Configuration MSTP mode
- ✧ Configuring the MST Region for a Switch
- ✧ Configuring the Max Hops in an MST Region
- ✧ Configuring the Switching Network Diameter
- ✧ Configuring the Max Transmission Speed on a Port
- ✧ Configuring the Time Parameters of a Switch
- ✧ Specifying the Switch as a Primary or a Secondary Root bridge
- ✧ Configuring the Bridge Priority for a Switch
- ✧ Configuring the Priority of a Port
- ✧ Configuring the Path Cost of a Port
- ✧ Configuring attribute of edge port
- ✧ Configuring link type
- ✧ Configuring mcheck
- ✧ Clearing information of port

13.4.1Enabling/Disabling MSTP in EXEC mode

MSTP is enable by default

step	Command	Description

1	**Config**	Enter global configuration mode
2	**spanning-tree {enable | disalbe}**	Enable and disable MSTP
3	**Exit**	Back to privileged EXEC MODE
4	**show spanning-tree**	Show MSTP configuration

13.4.2 Enabling/Disabling MSTP in port mode

MSTP is enable by default

step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port <1-MAX_PORT_NUM>**	Enter port mode
3	**spanning-tree {enable | disalbe}**	Enable and disable MSTP of a interface
4	**Exit**	Back to global configuration mode
5	**Exit**	Back to privileged EXEC MODE
6	**show spanning-tree**	Show MSTP configuration

Example:

Raisecom**#config**
Raisecom(config)**#spanning-tree enable**
Raisecom(config)**#interface port 2**
Raisecom(config-port)**#spanning-tree disable**
Raisecom(config-port)**#end**
Raisecom**#show spanning-tre**e

13.4.3 Configuration MSTP mode

MSTP and RSTP are compatible and they can recognize the packets of each other. However, STP cannot recognize MSTP packets. To implement the compatibility, MSTP provides two operation modes, STP-compatible mode and MSTP mode. In STP-compatible mode, the switch sends STP packets via every port. In MSTP mode, the switch ports send MSTP or STP packets (when connected to the STP switch) and
the switch provides multiple spanning tree function.

You can use the following command to configure MSTP running mode. MSTP can intercommunicate with STP. If there is a STP switch in the switching network, you may use the command to configure the current MSTP to run in STP-compatible mode. Otherwise, configure it to run in MSTP mode. Generally, if there is a STP switch on the switching network, the port connected to it will automatically transit from MSTP mode to STP-compatible mode. But the port cannot automatically transit back to MSTP mode after the STP switch is removed. In this case, you can execute the **stp mcheck** command to restore the MSTP mode.

step	Command	Description

1	**config**	Enter global configuration mode
2	**spanning-tree mode {stp | mstp}**	Set spanning-tree mode
3	**exit**	Back to privileged EXEC MODE
4	**show spanning-tree**	Show MSTP configuration

Example:
Raisecom**#config**
Raisecom(config)**#spanning-tree mode mstp**
Raisecom(config)**#exit**
Raisecom**#show spanning-tree**

13.4.4 Configuring the MST Region for a Switch

For two or more switches to be in the same MST region, they must have the same VLAN-to-instance mapping, the same configuration revision number, and the same name.

A region can have one member or multiple members with the same MST configuration; each member must be capable of processing RSTP BPDUs. There is no limit to the number of MST regions in a network, but each region can support up to 16 spanning-tree instances. You can assign a VLAN to only one spanning-tree instance at a time.

Beginning in privileged EXEC mode, follow these steps to specify the MST region configuration and enable MSTP. This procedure is required.

step	Command	Description
1	**config**	Enter global configuration mode
2	**spanning-tree region-configuration**	Enter MST region configuration mode
3	**[no] name name**	Set MST region name
4	**[no] revision-level level**	Set revision level of MST region
5	**instance <0-4095> vlan <1-4094>** **no instance <1-4095>**	Set the map between MST region and VLAN
6	**exit**	Back to global configuration mode
7	**spanning-tree region-configuration active**	Enable MST region configuration information
3	**exit**	Back to privileged EXEC MODE
4	**show spanning-tree region-configuration**	Show MST region configuration information

Example:
Raisecom**#config**
Raisecom(config)**#spanning-tree region-configuration**
Raisecom(config-region)**#name** aaa
Raisecom(config-region)**#revision-level** 2
Raisecom(config-region)**#instance** 3 **vlan** 11-20

Raisecom(config-region)**#exit**
Raisecom(config)**#spanning-tree region-configuration active**
Raisecom(config)**#exit**
Raisecom**#show spanning-tree region-configuration**

13.4.5 Configuring the Max Hops in an MST Region

The scale of MST region is limited by the max hops in an MST region, which is configured on the region root. As the BPDU travels from the spanning tree root, each time when it is forwarded by a switch, the max hops is reduced by 1. The switch discards the configuration BPDU with 0 hops left. This makes it impossible for the
switch beyond the max hops to take part in the spanning tree calculation, thereby limiting the scale of the MST region.

You can use the following command to configure the max hops in an MST region. The more the hops in an MST region, the larger the scale of the region is. Only the max hops configured on the region root can limit the scale of MST region. Other switches in the MST region also apply the configurations on the region root, even if they have been configured with max hops. By default, the max hop of an MST is 20.

Perform the following configuration in system view.

step	Command	Description
1	**config**	Enter global configuration mode
2	**[no] spanning-tree max-hops <1-40>**	Set max hop of switch MST region
3	**exit**	Back to privileged EXEC MODE
4	**show spanning-tree**	Show MST configuration information

13.4.6 Configuring the Switching Network Diameter

Any two hosts on the switching network are connected with a specific path carried by a series of switches. Among these paths, the one passing more switches than all othersis the network diameter, expressed as the number of passed switches.

The network diameter is the parameter specifying the network scale. The larger the diameter is, the lager the scale of the network is. When a user configures the network diameter on a switch, MSTP automatically
calculates and sets the Hello Time, Forward-Delay and Max Age time of the switch to the desirable values.

Setting the network diameter takes effect on CIST only, but has no effect on MSTI.

By default, the network diameter is 7 and the three corresponding timers take the default values.

step	Command	Description

1	**config**	Enter global configuration mode
2	**[no] spanning-tree bridge-diameter <2-7>**	Set the diameter
3	**exit**	Back to privileged EXEC MODE
4	**show spanning-tree**	Show MST configuration information

13.4.7 Configuring the Max Transmission Speed on a Port

The max transmission speed on a port specifies how many MSTP packets will be transmitted via the port every Hello Time. The max transmission speed on a port is limited by the physical state of the port and the network structure. You can configure it according to the network conditions.

You can configure the max transmission speed on a port in the following ways.The switch has three time parameters, Forward Delay, Hello Time, and Max Age. Forward Delay is the switch state transition mechanism. The spanning tree will be recalculated upon link faults and its structure will change accordingly. However, the
configuration BPDU recalculated cannot be immediately propagated throughout the network. The temporary loops may occur if the new root port and designated port forward data right after being elected. Therefore the protocol adopts a state transition mechanism. It takes a Forward Delay interval for the root port and designated port to transit from the learning state to forwarding state. The Forward Delay guarantees a period of time during which the new configuration BPDU can be propagated throughout the network.

The switch sends Hello packet periodically at an interval specified by Hello Time to check if there is any link fault. Max Age specifies when the configuration BPDU will expire. The switch will discard the expired configuration BPDU.

You can use the following command to configure the time parameters for the switch.
Perform the following configuration in system view.

step	Command	Description
1	**config**	Enter global configuration mode
2	**[no] spanning-tree hello-time <1-10>**	Set Hello Time
3	**[no] spanning-tree forward-delay <4-30>**	Set Forward Delay
4	**[no] spanning-tree max-age <6-40>**	Set Max Age
5	**exit**	Back to privileged EXEC MODE
6	**show spanning-tree**	Show MST configuration information

13.4.8 Specifying the Switch as a Primary or a Secondary Root bridge

MSTP can determine the spanning tree root through calculation. You can also specify the current

switch as the root, using the command provided by the switch.

You can use the following commands to specify the current switch as the primary or secondary root of the spanning tree.After a switch is configured as the primary root bridge or the secondary root bridge, users cannot modify the bridge priority of the switch. You can configure the current switch as the primary or secondary root bridge of the STI (specified by the **instance** *instance-id* parameter). If the *instance-id* takes 0, the current switch is specified as the primary or secondary root bridge of the CIST.

The root types of a switch in different STIs are independent of one another. The switch can be a primary or secondary root of any STI. However, it cannot serve as both the primary and secondary roots of one STI.

If the primary root is down or powered off, the secondary root will take its place, unless you configure a new primary root. Of two or more configured secondary root bridges, MSTP selects the one with the smallest MAC address to take the place of the failed primary root. When configuring the primary and secondary switches, you can also configure the network diameter and hello time of the specified switching network.

step	Command	Description
1	**config**	Enter global configuration mode
2	**spanning-tree [instance instance-id] root {primary, secondary}**	Specifying the Switch as a Primary or a Secondary Root bridge
3	**exit**	Back to privileged EXEC MODE
4	**show spanning-tree**	Show MST configuration information

By default, a switch is neither the primary root nor the secondary root of the spanning tree.

13.4.9 Configuring the Bridge Priority for a Switch

Whether a switch can be elected as the spanning tree root depends on its Bridge priority. The switch configured with a smaller Bridge priority is more likely to become the root. An MSTP switch may have different priorities in different STIs.

You can use the following command to configure the Bridge priorities of the Designated bridge in different STIs. When configuring the switch priority with the **instance** *instance-id* parameter as 0, you are configuring the CIST priority of the switch.

Perform the following configuration in system view.

step	Command	Description

1	**config**	Enter global configuration mode
2	**[no] spanning-tree [instance instance-id] priority <0-61440>**	Set the priority
3	**exit**	Back to privileged EXEC MODE
4	**show spanning-tree**	Show MST configuration information

By default, the switch Bridge priority is 32768.

Example:
Raisecom**#config**
Raisecom(config)**#spanning-tree priority 4096**
Raisecom(config)**#exit**
Raisecom**#show spanning-tree**

13.4.10 Configuring the Bridge Priority for a Switch

For spanning tree calculation, the port priority is an importance factor to determine if a port can be elected as the root port. With other things being equal, the port with the highest priority will be elected as the root port. On the MSTP switch, a port can have different priorities in different STIs and plays different roles respectively. Thus the traffic from different VLANs can run over different physical links, thereby implementing the
VLAN-based load-balancing.

You can configure the port priority in the following ways.

step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port <1-MAX_PORT_NUM>**	Enter physical port mode
3	**[no] spanning-tree [instance instance-id] priority <0-240>**	Set the priority
4	**Exit**	Back to global configuration mode
5	**Exit**	Back to privileged EXEC MODE
6	**show spanning-tree**	Show MST configuration information

Example:
Raisecom**#config**
Raisecom(config)**#interface port 2**
Raisecom(config-port)**#spanning-tree priority 16**
Raisecom(config-port)**#exit**
Raisecom(config)**#exit**
Raisecom**#show spanning-tree**

You can configure the port priority with either of the earlier-mentioned measures. Upon the change of port priority, MSTP will recalculate the port role and transit the state. Generally, a smaller value

represents a higher priority. If all the Ethernet ports of a switch are configured with the same priority value, the priorities of the ports will be differentiated by the index number. The change of Ethernet port priority will lead to spanning tree recalculation. You can configure the port priority according to actual networking requirements.

By default, the priority of all the Ethernet ports is 128.

13.4.11 Configuring the Path Cost of a Port

Path Cost is related to the speed of the link connected to the port. On the MSTP switch, a port can be configured with different path costs for different STIs. Thus the traffic from different VLANs can run over different physical links, thereby implementing the VLAN-based load-balancing.

You can configure the path cost of a port in the following ways.

step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port <1-MAX_PORT_NUM>**	Enter physical port mode
3	**[no] spanning-tree [instance instance-id] path-cost <0-200000000>**	Set the path cost
4	**Exit**	Back to global configuration mode
5	**Exit**	Back to privileged EXEC MODE
6	**show spanning-tree**	Show MST configuration information

Example:
Raisecom**#config**
Raisecom(config)**#interface port 2**
Raisecom(config-port)**#spanning-tree instance** 3 **path-cost 1000000**
Raisecom(config-port)**#exit**
Raisecom(config)**#exit**
Raisecom**#show spanning-tree**

You can configure the path cost of a port with either of the earlier-mentioned measures. Upon the change of path cost of a port, MSTP will recalculate the port role and transit the state. When *instance-id* takes 0, it indicates to set the path cost on the CIST.

By default, MSTP is responsible for calculating the path cost of a port.

13.4.12 configuring attribute of edge port

An edge port refers to the port not directly connected to any switch or indirectly connected to a switch over the connected network.

You can configure a port as an edge port or non-edge port in the following ways.

step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port <1-MAX_PORT_NUM>**	Enter physical port mode
3	**spanning-tree edged-port {auto | force-true | force-false}**	Set atribute of edged port
4	**Exit**	Back to global configuration mode
5	**Exit**	Back to privileged EXEC MODE
6	**show spanning-tree**	Show MST configuration information

Example:

Raisecom**#config**
Raisecom(config)**#interface port 2**
Raisecom(config-port)**#spanning-tree edged-port** force-true
Raisecom(config-port)**#exit**
Raisecom(config)**#exit**
Raisecom**#show spanning-tree**

You can configure a port as an edge port or a non-edge port with either of the earlier-mentioned measures.

After configured as an edge port, the port can fast transit from blocking state to forwarding state without any delay. You can only set the port connecting with the terminal as an edge port. The configuration of this parameter takes effect on all the STIs. In other words, if a port is configured as an edge port or non-edge port, it is configured the same on all the STIs. If BPDU protection is enabled on the switch, the edged port is disabled when it receives BPDU packets from the user. Only the network administrators can enable the port.

By default, all the Ethernet ports of the switch have been configured as non-edge ports.

13.4.13 Configuring link type

The point-to-point link directly connects two switches.

You can configure the port (not) to connect with the point-to-point link in the following ways.

step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port <1-MAX_PORT_NUM>**	Enter physical port mode
3	**spanning-tree link-type {point-to-point | shared}**	Set link type
4	**Exit**	Back to global configuration mode
5	**Exit**	Back to privileged EXEC MODE
6	**show spanning-tree**	Show MST configuration information

Example:

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

Raisecom(config-port)**#spanning-tree link-type point-to-point**
Raisecom(config-port)**#exit**
Raisecom(config)**#exit**
Raisecom**#show spanning-tree**

You can configure the port to connect with the point-to-point or shanred link. If a port works in full-duplex mode, it can be configured to connect with the point-to-point link. If a port works in half-duplex mode, it can be configured to connect with the shared link.

For the ports connected with the point-to-point link, upon some port role conditions met, they can transit to forwarding state fast through transmitting synchronization packet, thereby reducing the unnecessary forwarding delay. If the parameter is configured as auto mode, MSTP will automatically detect if the current Ethernet port is connected with the point-to-point link. This configuration takes effect on the CIST and all the MSTIs. The settings of a port whether to connect the point-to-point link will be applied to all the STIs to which the port belongs. Note that a temporary loop may be redistributed if you configure a port that is not physically connected with the point-to-point link as connected to such a link by force.
By default, the parameter is configured as **auto**.

13.4.14 configuring mcheck

The port of an MSTP switch operates in either STP-compatible or MSTP mode. Suppose a port of an MSTP switch on a switching network is connected to an STP switch, the port will automatically transit to operate in STP-compatible mode. However, the port stays in STP-compatible mode and cannot automatically transit back to MSTP mode when the STP switch is removed. In this case, you can perform mCheck operation to transit the port to MSTP mode by force.

You can use the following measure to perform mCheck operation on a port.

step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port <1-MAX_PORT_NUM>**	Enter physical port mode
3	**spanning-tree mcheck**	force the port to MSTP
4	**Exit**	Back to global configuration mode
5	**Exit**	Back to privileged EXEC MODE
6	**show spanning-tree**	Show MST configuration information

Example:
Raisecom**#config**
Raisecom(config)**#interface port 2**
Raisecom(config-port)**#spanning-tree mcheck**
Raisecom(config-port)**#exit**
Raisecom(config)**#exit**

Raisecom#show spanning-tree

You can configure mCheck variable on a port with either of the earlier-mentioned measures. Note that the command can be used only if the switch runs MSTP. The command does not make any sense when the switch runs in STP-compatible mode.

13.4.15 Clearing information of port

MSTP statistics of each MSTP port includes: input STP packet, input RSTP packet, input MSTP packet, output STP packet, output RSTP packet, output MSTP packet.

step	Command	Description
1	**Config**	Enter global configuration mode
	interface port <1-MAX_PORT_NUM>	Enter physical port mode
2	**spanning-tree clear statistics**	clear statistics
4	**Exit**	Back to global configuration mode
5	**Exit**	Back to privileged EXEC MODE
6	**show spanning-tree**	Show MST configuration information

Example:

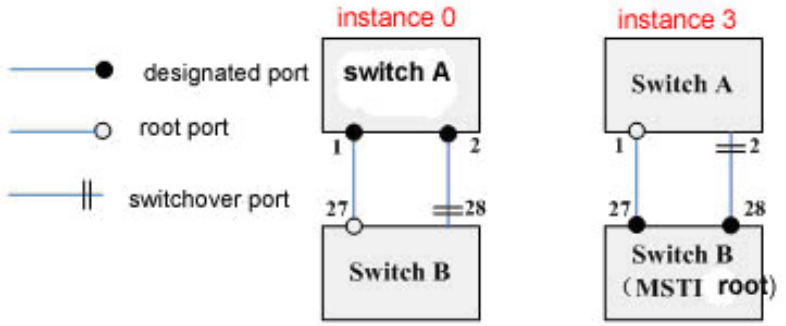
Raisecom**#config**
Raisecom(config)**#interface port 2**
Raisecom(config-port)**#spanning-tree clear statistics**
Raisecom(config-port)**#exit**
Raisecom(config)**#exit**
Raisecom**#show spanning-tree**

13.5 Monitor and maintainece

- ✧ show spanning-tree region-configuration show the configuration of MST region
- ✧ show spanning-tree [instance instance-id] show basal information of MSTP
- ✧ show spanning-tree [instance instance-id] show detail information of MSTP
- ✧ show spanning-tree [instance instance-id] port-list [portlist]show MSTP interface information
- ✧ show spanning-tree [instance instance-id] port-list [portlist] show detail MSTP interface information

13.5.1 Show Example

1. Topology and configuration



basal configuration:

switch	instance 0	instance 3
Switch A	4096	8192
Switch B	8192	4096

2. MST command configuration

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

13.5.2 Show basal MSTP information

- Command: **show spanning-tree region-configuration**
- Function: show MSTP region configuration information.

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

Configured:

Name: aaa

Revision level: 2 Instances configured: 2

Instance Vlans Mapped

-------- ---

```
    0               1-10,21-4094
    3               11-20

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

13.5.3 Show basal MSTP information

- ✧ Command: **show spanning-tree [instance instance-id]**
- ✧ Function: show basal information of one or all the STP instantces

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
```

13.5.4 Show detail MSTP information

- ✧ Command: **show spanning-tree [instance instance-id]**
- ✧ Function: show basal information of one or all the STP instantces

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

13.5.5 Show basal information of the portlist MSTP

- ✧ Command: **show spanning-tree [instance instance-id] port-list [portlist]**
- ✧ Function: show basal portlist information of one or all the STP instantces

```
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
```

13.5.6 Show detail information of the portlist MSTP

- ✧ Command: **show spanning-tree [instance instance-id] port-list [portlist]**
- ✧ Function: Function: show basal portlist information of one or all the STP instantces

```
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
```

Chapter 14 RSTP Configuration

This chapter introduces how to configure RSTP on the switch, including following parts:

- ✧ About RSTP
- ✧ RSTP configuration list
- ✧ Step by step introduction
- ✧ Maintenance

14.1 About RSTP

The RSTP takes advantage of point-to-point wiring and provides rapid convergence of the spanning tree. Reconfiguration of the spanning tree can occur in less than 1 second (in contrast to 50 seconds with the default settings in the 802.1D spanning tree), which is critical for networks carrying delay-sensitive traffic such as voice and video.

14.2 RSTP configuration list

- ✧ RSTP globally enable and disable.
- ✧ Switch system priority configuration.
- ✧ RSTP Hello Time configuration
- ✧ RSTP Maximum Aging time setting
- ✧ RSTP Forward Delay setting
- ✧ Switch RSTP running mode
- ✧ RSTP the setting of maximum send packet by the protocol within hello time
- ✧ RSTP port enable and disable
- ✧ RSTP port priority setting
- ✧ RSTP path cost setting
- ✧ RSTP edge port setting
- ✧ RSTP the setting for the type of port link
- ✧ configure current Ethernet port in RSTP mode
- ✧ Clear RSTP port statistical information

14.3 Enable and disable RSTP globally

Default setting: RSTP is enabled. The following steps can disable or enable RSTP.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**spanning-tree {enable | disable}**	Enable or disable RSTP globally
3	**exit**	Exit to privileged EXEC mode.

4	**show spanning-tree**	Show spanning tree configuration information.

Following is an example for disabling RSTP:

```
Raisecom#config
Raisecom(config)#spanning-tree disable
Raisecom(config)#exit
Raisecom#show spanning-tree
```

14.4 Switch system priority setting

The RSTP topology of a network is determined by the following elements:

- ✧ The unique bridge ID (switch system priority and MAC address)
- ✧ The spanning-tree path cost to the root switch
- ✧ The port identifier (port priority and MAC address) associated with each Layer 2 interface

The bridge ID decides whether the switch can be a root switch and combines 8 byte: 2 bytes of switch system priority and 6 bytes of switch MAC address. The smaller bridge ID has higher priority, and the switch which has the smallest bridge ID will be selected as root switch of the network.

The value of system priority must be the multiple of 4096.

Change RSTP system priority as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**spanning-tree priority** <1-61440>	Set RSTP system priority
3	**exit**	Exit to privileged EXEC mode
4	**show spanning-tree**	Show spanning tree configuration

Set RSTP system priority to 4096:

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

14.5 RSTP Hello Time configuration

Switch sends Bridge Protocol Data Unit (BPDU) periodically, and the default interval time value is 2 seconds. Users can configure the interval between the generations of configuration messages by the root switch by changing the hello time.

Change the RSTP hello time as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**spanning-tree hello-time** <1-10>	Set RSTP Hello Time
3	**exit**	Exit to privileged EXEC mode
4	**show spanning-tree**	Show RSTO configuration information

Example: Set RSTP hello time as 3 seconds:

Raisecom#config

Raisecom(config)#spanning-tree hello-time 3

Raisecom(config)#exit

Raisecom#show spanning-tree

14.6 RSTP Maximum aging time setting

The maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration. Users use **no spanning-tree max-age** command to recover the default value.

Change the RSTP Mac age as following steps:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**spanning-tree max-age** <6-40>	Set RSTP Maximum Aging time
3	**exit**	Exit to privileged EXEC mode
4	**show spanning-tree**	Show RSTP configuration information

Example: Set RSTP Max Age to 6 seconds:

Raisecom#config

Raisecom(config)#spanning-tree max-age 6

Raisecom(config)#exit

Raisecom#show spanning-tree

14.7 RSTP Forward Delay setting

The forward delay is the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state. User can use **no spanning-tree forward-delay** command to recover default value. Change RSTP Forward Delay as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**spanning-tree forward-delay** <4-30>	Set the forward delay of RSTP

3	**exit**	Exit to privileged EXEC mode.
4	**show spanning-tree**	Show RSTP configuration information

Example: Set RSTP Forward Delay to 5 seconds:

Raisecom#config

Raisecom(config)#spanning-tree forward-delay 5

Raisecom(config)#exit

Raisecom#show spanning-tree

14.8 Switch RSTP running mode

IEEE 802.1w protocol defines two modes: STP mode and RSTP compatible mode.

Under the STP mode, switch does not execute fast forwarding of designated port and fast changing from designated port to root port. RSTP only send STP BPDU and topology changing notification. The received RST BPDU will be dropped.

Raisecom series switch supports both STP and RSTP mode:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**spanning-tree mode {stp|rstp}**	Set RSTP running mode.
3	**exit**	Exit to privileged user mode.
4	**show spanning-tree**	Show RSTP configuration information.

The configuration of RSTP running mode as following:

Set RSTP running mode to RSTP mode:

Raisecom#config

Raisecom(config)#spanning-tree mode rstp

Raisecom(config)#exit

Raisecom#show spanning-tree

14.9 The maximum packets sent within hello time.

Use this command to set the BPDU packet transmission limitation of RSTP within hello time. The higher transmit speed is, the more packets can be sent in each time unit.

The following commands configure the maximum packets sent within hello time:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**spanning-tree transit-limit** <1-10>	Set the maximum BPDU packet by RSTP protocol within hello time.

3	**Exit**	Back to privileged user mode.
4	**show spanning-tree**	Display RSTO configuration situation.

Set the maximum BPDU packets sent within hello time to 6:

Raisecom#config

Raisecom(config)#spanning-tree transit-limit 6

Raisecom(config)#exit

Raisecom#show spanning-tree

14.10 Enable and disable RSTP function based on port

To control RSTP flexibly, user can enable/disable the RSTP function based on per port. This will make some ports not take part in the STP calculating. Use following commands to enable/disable the RSTP function based on designated Ethernet port.

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** <1-26>	Enter Ethernet physical interface mode.
3	**spanning-tree {enable | disalbe}**	Enable or disable the RSTP function on that port
4	**Exit**	Exit to global configuration mode.
5	**Exit**	Exit to privileged EXEC mode
6	**show spanning-tree**	Show RSTP configuration situation

Example: Shutdown RSTP protocol of port

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)#spanning-tree disable

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show spanning-tree

14.11 RSTP port priority setting

If a loop occurs, spanning tree uses the port priority when selecting an interface to put into the forwarding state. You can assign higher priority values (lower numerical values) to interfaces that you want selected first and lower priority values (higher numerical values) that you want selected last. If all interfaces have the same priority value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Step	Command	Description

1	**Config**	Enter global configuration mode
2	**interface port** <1-26>	Enter Ethernet physical interface mode.
3	**spanning-tree priority** <0-240>	Set RSTP port priority
4	**Exit**	Exit to global configuration mode.
5	**Exit**	Exit to privileged EXEC mode.
6	**show spanning-tree**	Show RSTP configuration information

Example: Set the RSTP port priority of physical port 2 as 16:

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)#spanning-tree priority 16

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show spanning-tree

14.12 The path cost configuration

The spanning-tree path cost default value is derived from the media speed of an interface. If a loop occurs, spanning tree uses cost when selecting an interface to put in the forwarding state. You can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, spanning tree puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

Default path cost of different media speed is:

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

The steps to change RSTP port expense:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** <1-26>	Enter Ethernet physical port mode.
3	**spanning-tree path-cost** <0-200000000>	Set RSTP port expense
4	**Exit**	Exit to global configuration mode.
5	**Exit**	Exit to privileged EXEC mode.
6	**show spanning-tree**	Show RSTP configuration situation.

Set the RSTP port expense of Ethernet physical interface 2 to 1000000.

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)#spanning-tree path-cost 1000000

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show spanning-tree

14.13 RSTP edge port setting

If you configure a port as edge port on an RSTP switch, the edge port immediately changes to the forwarding state. So please enable it only on ports that connect to a single end station. The steps of how to set the edge ports as following:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** <1-26>	Enter Ethernet physical interface mode.
3	**spanning-tree edged-port**	Set edge port.
4	**Exit**	Exit to global configuration mode.
5	**Exit**	Exit to privileged EXEC mode.
6	**show spanning-tree**	Show RSTP configuration information.

Example: Set the Ethernet physical port 2 as edge port.

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)#spanning-tree edged-port

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show spanning-tree

14.14 Setting of RSTP port link

If you connect a port to another port through a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port by using the proposal-agreement handshake to ensure a loop-free topology.

By default the switch determines the link type from the port duplex mode: a full-duplex port is considered to have a point-to-point connection; a half-duplex port is considered to have a shared connection.

Set the link type of RSTP port as following:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** <1-26>	Enter Ethernet physical interface mode.
3	**spanning-tree link-type** {**point-to-point** | **shared**}	Set the point-to-point link type
4	**Exit**	Exit to global configuration mode
5	**Exit**	Exit to privileged EXEC mode.
6	**show spanning-tree**	Show RSTP configuration

Example: Set Ethernet physical interface 2 to point-to-point link.

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)#spanning-tree link-type point-to-point

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show spanning-tree

14.15 Force the current Ethernet port in RSTP mode

If the network is stable, even though the bridge (which LAN runs STP) is disconnected, the switch which runs RSTP and connects to the bridge is still in STP compatible mode. Use **spanning-tree mcheck** command to set mCheck variables and force the port to be in RSTP mode. When the port is in RSTP mode, if it receives new STP packets, the port will be back to STP compatibility mode.

The steps that Ethernet port moves back to port RSTP mode as following:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** <1-26>	Enter Ethernet physical interface configuration mode.
3	**spanning-tree mcheck**	Force the port to RSTP mode.
4	**Exit**	Exit to global configuration mode.
5	**Exit**	Exit to privileged EXEC mode.
6	**show spanning-tree**	Show RSTP configuration mode.

Example: Force physical port 2 to RSTP mode.

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)#spanning-tree mcheck

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show spanning-tree

14.16 Clear RSTP port statistical information

The switch will count the BPDU message quantity of each RSTP port: received STP detection messages, sent notification messages, received RSTP messages, sent RSTP detection messages, sent notification messages and received RSTP message.

Clear RSTP port statistical information:

Step	Command	Description
1	**Config**	Enter global configuration mode.
2	**interface port** <1-26>	Enter Ethernet interface mode.
3	**spanning-tree clear statistics**	Clear port statistical information.
4	**Exit**	Exit to global configuration mode.
5	**Exit**	Exit to privileged user mode.
6	**show spanning-tree**	Display RSTP configuration situation.

Example: Clear the statistical information at physical port 2:

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)#spanning-tree clear statistics

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show spanning-tree

14.17 Maintenance

In privileged EXEC mode, use **show spanning-tree** command to check the current spanning tree configuration status. This command is used to display all the configuration information of spanning-tree of the switch.

Raisecom#show spanning-tree

RSTP Admin State: Enable

Protocol Mode: RSTP

Bridge ID: 32768-000E5E1A2B3C(priority-MAC)

Root ID: 32768-000E5E1A2B3C(priority-MAC)

Root Port: none

Root Cost: 0

Max Age: 20 Bridge Max Age: 20

Hello Time: 2 Bridge Hello Time: 2

Forward Delay: 15 Bridge Forward Delay: 15

Max Transmission Limit:3 per hello time

In privileged EXEC mode, use **show spanning-tree port** command to check current port status and configuration of RSTP. This command can display all the port configuration information of the switch.

```
Raisecom#show spanning-tree port 8
RSTP Admin State: Enable
Protocol Mode:      RSTP
Bridge ID:            32768-000E5E1A2B3C(priority-MAC)
Root ID:              32768-000E5E1A2B3C(priority-MAC)
Root Port:            none
Root Cost:            0
Max Age:              20      Bridge Max Age:           20
Hello Time:           2       Bridge Hello Time:        2
Forward Delay:      15      Bridge Forward Delay: 15
Max Transmission Limit:3    per hello time

---------------------------------------------
Port Index:8
---------------------------------------------
Port RSTP:            Enable
State:                Disable
Port Role:            Disable
Priority:             128
PortPathCost:         admin:          Auto          oper:       200000
Point2Point:          admin:          Auto          oper:           Y
Edge:                 admin:             N          oper:           N
Partner RSTP Mode:        RSTP
BPDU Received:        RST:0,Config:0,TCN:0
BPDU Sent:            RST:0,Config:0,TCN:0
```

Chapter 15 DHCP Configuration

DHCP Relay is NOT AVAILABLE ON L2 Switches.

15.1 DHCP Relay configuration

- ✧ About DHCP Relay
- ✧ Configure the task list
- ✧ Introduction step by step
- ✧ Monitoring and maintenance
- ✧ DHCP Relay trouble shooting

15.2 About DHCP Relay

The DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and a mechanism for allocating network addresses to devices. DHCP is built on a client-server model, in which designated DHCP servers allocates network addresses and deliver configuration parameters to dynamically configured devices (DHCP client).

DHCP Relay agent locates between DHCP server and client to realize the transmission of DHCP messages across different sub-nets, that is to say, network administrators do not need to set DHCP server on every sub-network. DHCP clients in different sub-nets can get IP address from one DHCP server, enabling a flexible network organization.

15.3 DHCP Relay configuration task list

The configuration of DHCP includes following setting:

- ✧ Enable and disable DHCP Relay
- ✧ DHCP Server address configuration

15.4 DHCP Relay configuration

15.4.1 Enable and disable DHCP Relay globally

DHCP Relay is disabled on the switch by default. When enable or disable DHCP relay function globally (in globally configuration mode), all the VALN will enable or disable DHCP relay function.

Enable and disable the DHCP relay function according to the following commands:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**dhcp-relay enable**	Enable DHCP Relay

3	**exit**	Exit privileged EXEC mode.
4	**show dhcp-relay**	Show DHCP Relay configuration information

To disable DHCP Relay, use **dhcp-relay disable** command.

To disable DHCP Relay function of a particular VLAN, use the following commands in global configuration mode:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**no dhcp-relay listen vlan-list {***1-4094***}**	Disable the DHCP Relay function in a particular VLAN
3	**exit**	Exit to privilege EXEC mode
4	**show dhcp-relay listen** [**vlan** *vlan-id*]	Show VLAN configuration information

Use dhcp-relay listen command in global configuration mode to enable DHCP relay function in a particular VLAN.

DHCP Relay function does not work in a particular VLAN unless it is enabled globally.

Use show command to check the DHCP relay configuration information:

ISCOM2826# show dhcp-relay listen

the VLAN that enabled the DHCP Relay include:

VLAN ID = 1,2

The total enabled VLAN num is 2

Check the DHCP relay configuration information of a particular VLAN:

ISCOM2826# show dhcp-relay listen vlan 3

VLAN 3 disabled DHCP Relay

15.4.2 DHCP Server address configuration

Administrators should configure the DHCP server address to realize the relay of DHCP messages. Configuration steps like following:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**dhcp-relay server-ip** *ip-address*	Set the IP address of DHCP server
3	**exit**	Exit to privileged EXEC mode
4	**show dhcp-relay server-ip**	Display the address configuration information of DHCP server

In order to clear the configured server address, use **no dhcp-relay server-ip** *ip-address* command in global configuration mode.

*Note: the maximum quantity of Server IP address is 8. Please make sure that the IP address you configured is correct.

Example

ISCOM2826#config
ISCOM2826(config)**#dhcp-relay server-ip** 10.0.0.1
ISCOM2826(config)**#exit**

ISCOM2826#show dhcp-relay server-ip

Command execution echo:

index IP address Status
---
1 10.0.0.1 active
2 20.0.0.1 active

15.4.3 Monitor and maintenance

Use the following commands for the monitoring and maintenance of DHCP Relay:

Step	Command	Description
1	**show dhcp-relay**	Show DHCP Relay configuration information.
2	**show dhcp-relay listen** [**vlan** *vlanid*]	Show DHCP Relay configuration information in all the VLAN or a designated VLAN.
3	**show dhcp-relay server-ip**	Show the IP address information of DHCP server.

Use **show dhcp-relay** command to check DHCP relay configuration information.

ISCOM2826# show dhcp-relay

DHCP Relay enabled !

the VLAN that enabled the DHCP Relay include:

VLAN ID = 1,2

The total enabled VLAN num is 2

Statistics infomation of DHCP Relay:

DHCP StartUp time: 0 hours 4 munites 30 seconds

the Num of Bootps received: 1

the Num of Discover received: 1

the Num of Request received: 0

the Num of Decline received: 0

the Num of Offer received: 0

the Num of Ack received: 0

the Num of Nack received: 0

the Num of Decline received: 0

the Num of Information received: 0

the Num of Unknows received: 0

the total Num of Packets received: …2

If user just want to check the DHCP relay configuration in a particular VLAN, use show dhcp-relay listen [vlan *vlanid*], if the VLAN is not specified, show all the VLAN information, that is all the exist and active VLAN.

ISCOM2826# show dhcp-relay listen

the VLAN that disabled the DHCP Relay include:

VLAN ID = 1,2

The total disabled VLAN num is 2

Show designated VLAN configuration information, use following command:

ISCOM2826# show dhcp-relay listen vlan 2

VLAN 2 disabled DHCP Relay

Show DHCP server IP address, command and format as following:

index IP address Status

---

1 10.0.0.1 active

2 20.0.0.1 active

15.5 DHCP Relay trouble shooting

If the server IP address is not specified, the device cannot forward DHCP message correctly.

When configure the DHCP server IP address, the following reasons may cause unsuccessful configuration: there are already 8 DHCP server IP addresses, or the input IP address is not correct.

When delete the configured DHCP server IP address, the following reasons may cause failure: wrong IP address or the IP address does exist.

15.5.1 DHCP Relay command reference

Step	Command	Description
1	**dhcp-relay service**	Enable DHCP Relay function
2	**dhcp-relay listen vlan-list {1-4094}**	Enable DHCP Relay function of a designated VLAN.
3	**dhcp-relay server-ip** *ip-address*	Configure DHCP server IP address.
4	**show dhcp-relay**	Show DHCP Relay configuration information
5	**show dhcp-relay listen** [**vlan** *vlanid*]	Show DHCP Relay configuration information in designated or all the VLAN
6	**show dhcp-relay server-ip**	Show DHCP server IP address information.

15.6 DHCP Server configuration

- ✧ About DHCP Server protocol
- ✧ Configuration task list
- ✧ Step by step introduction
- ✧ Monitoring and maintenance
- ✧ Configuration example
- ✧ DHCP Server trouble shooting

15.6.1 About DHCP Server protocol

Dynamic Host Configuration Protocol (DHCP) lets network administrators centrally manage and

automate the assignment of IP addresses in a TCP/IP based network, it is an extension of earlier BOOTP protocol and DHCP can handle BOOTP client requests.

DHCP provides configuration parameter to network hosts and is made of two basic parts: one is transmitting special configuration information to host computer; the other is distributing network address to host computer. DHCP is based on client/server mode, under this mode, the designated host computer (DHCP server) distributes network address, and transmits configuration parameter to the host computer that needs this kind of configuration information, the specified host computer is called server. This chapter introduces system integrated DHCP server configuration. It is not necessary to maintain special DHCP server if use this kind of integrated DHCP server. The cost of network construction and maintenance will be reduced.

15.6.2 DHCP Server configuration task list

The configuration of DHCP server includes following functional configuration:

- ✧ Enable and disable DHCP Server.
- ✧ The configuration of address pool.
- ✧ Lease time configuration
- ✧ Neighbor agent address configuration

15.6.3 Enable and disable DHCP Server

DHCP server is disabled by default. When the DHCP server is enabled or disabled in global configuration mode, DHCP server function will be enabled or disable in all the VLAN.

Refer the following commands to enable DHCP server function:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**dhcp-server enable**	Enable DHCP Server
3	**exit**	Exit to privileged EXEC mode.
4	**show dhcp-server**	Show DHCP Server configuration information.

To enable DHCP Server function use command **dhcp-server disable** in global configuration mode.

Use the following commands to disable the DHCP server function in particular VLAN:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**dhcp-relay deactive vlan-list {***1-4094***}**	Disable the DHCP server function in this VLAN.
3	**exit**	Exit to privileged configuration mode.
4	**show dhcp-server**	Show DHCP server configuration information of a particular VLAN.

Use **dhcp-relay active** command to enable DHCP server function of a particular VLAN in global configuration mode.

DHCP server function does not work in a particular VLAN unless it is enabled globally.

Use show command to check DHCP server configuration:

ISCOM2826# show dhcp-server

DHCP server: Enable

Active VLAN: 1,2

The total enabled VLAN: 2

……

Only the created VLAN can be displayed.

15.6.4 DHCP server address pool configuration

To realize network address automatic assignment, DHCP server should be correctly configured the IP pool. Use the following commands to configure the IP pool for DHCP server:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**dhcp-sever ip-pool WORD……**	Set the IP pool of the DHCP server.
3	**exit**	Exit to privileged EXEC mode.
4	**show dhcp-server ip-pool**	Show the configuration information of DHCP server IP pool.

Use **no dhcp-server ip-pool** command in global configuration mode to clear the DHCP server pool configuration. If the IP address doesn't exist, the operation will fail.

*Note: the maximum quantity of IP pool is 20, and the maximum quantity of IP address is 1000. IP pool name is the only mark for each IP pool.

Example:

ISCOM2826#config

ISCOM2826(config)#**dhcp-server ip-pool** abcdefgh 192.168.1.100 192.168.1.200 255.255.255.0 **vlan** 10-20 **gateway** 192.168.1.1 **dns** 192.168.1.1 **secondary-dns** 10.168.0.1

ISCOM2826(config)#**exit**

ISCOM2826#show dhcp-server ip-pool

Command execution echo:

Name of ip pool table : abcdefgh

Status of IP pool table: active

IP address range: 192.168.1.100 - 192.168.1.200

Mask: 255.255.255.0

Including VLANs: 10-20

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

Alloted IP address count : 0

Gateway and DNS are optional, if they are not configured, the default Gateway and DNS will not be specified.

15.6.5 Lease time configuration

The DHCP server controls the IP address pool. It grants permission to DHCP client to use IP addresses on a lease basis. The IP address is leased to the client for a fixed amount of time. The administrator sets the lease time, which can last from 30 minutes to 10080 minutes on Raisecom series switches.

The default lease time of Raisecom series switches is 30 minutes.
The maximum lease time: 10080 minutes (7 days). When clients require a lease time longer than the maximum lease time, the switch will use the maximum lease time-10080 minutes.
The minimum lease time: 30 minutes, when clients require a lease time shorter than the minimum lease time; the switch will use the minimum lease time-30 minutes.

Configuration steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**dhcp-sever default-lease** *timeout*	Set the default lease time

3	**dhcp-sever max-lease** *timeout*	Set the maximum lease time
4	**dhcp-sever min-lease** *timeout*	Set the minimum lease time
5	**exit**	Exit to privilege mode.
6	**show dhcp-server**	Show the configuration information of DHCP server

Use **no dhcp-server default,no dhcp-sever max-lease,no dhcp-sever min-lease** command to restore the default value in global configuration mode.

*Note: the lease time will be applied to all the IP pool. And the maximum lease time should be longer than the minimum lease time.

Configuration example:

ISCOM2826#config

ISCOM2826(config)**#dhcp-server default-lease** 60

ISCOM2826(config)**#dhcp-server max-lease** 1440

ISCOM2826(config)**#dhcp-server min-lease** 45

ISCOM2826(config)**#exit**

ISCOM2826#show dhcp-server

Command execution echo:

DHCP server: Enable

Active VLAN: 1,2

The total enabled VLAN: 2

Max lease time: 1440 m

Min lease time: 40 m

Default lease time: 60 m

15.6.6 Neighbor DHCP Relay address configuration

When DHCP clients connect with DHCP relay agent, DHCP server should know the IP address of DHCP Relay agent. The IP address DHCP relay agent should be configured by administrators manually.

The configuration steps as following:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**dhcp-sever relay-ip** *ip-address ip-mask*	Set the IP address of DHCP relay agent.
3	**exit**	Exit to privileged EXEC mode.
4	**show dhcp-server relay-ip**	Show the IP address of DHCP relay agent

Use **no dhcp-server relay-ip** *ip-address* command to delete the DHCP relay IP address in global configuration mode.

*Note: DHCP relay IP address here is the IP address of the interface connects with the clients directly.

Configuration example:

ISCOM2826#config

ISCOM2826(config)**#dhcp-server relay-ip** 192.168.1.1 255.255.255.0

ISCOM2826(config)**#exit**

ISCOM2826#show dhcp-server relay-ip

Command execution echo:

index IP address IP Mask Status

---

1 192.168.1.1 255.0.0.0 active

15.7 DHCP Auto-Configuration Guide

Dynamic Host Configuration Protocol (DHCP) provides configuration information for hosts and other Internet devices. Using DHCP auto-configuration, switches (DHCP clients) will obtain IP address and configuration file automatically during their startup process.

15.7.1 DHCP Server Configuration

DHCP server should be configured with hardware address binding, otherwise the switches may obtain different IP address and configuration file every time.

The following items of DHCP server requires configuration:

- Client IP address (compulsory)
- Client IP address subnet mask (compulsory)
- Gateway address (compulsory)
- TFTP server address (compulsory)
- Configuration file name (recommended to be provided)

15.7.2 DHCP Client Configuration

The DHCP auto-configuration on switches is disabled by default. It can be enabled by using command "service config" under global configuration mode. The command will be automatically saved.

Optional parameters of the "service config" command are used to specify DHCP auto-configuration options.

***management-vlan*:**

Using "management" parameters to specify DHCP auto-configuration options. Switches communicate with DHCP server by sending "untag" packet by default. Users can specify a management-vlan for a switch, then, the switch with a specified management-vlan will communicate with the DHCP server by sending "tag" message within the specified management-vlan. Users can specify the ports within the management-vlan using "portlist" option. When the "portlist" option is configured, the client IP address obtained by the switch will be configured on interface ip 0, otherwise, it will be configured on VLAN 1. If a management-vlan has been configured, the mode of the ports within the management-vlan will be set to mixed mode.

config-filename:

The DHCP server will name the configuration file by default. Users can specigy the configuration file name on switches. If user specifies the configuration file name at local side, the switch will try to obtain the configuration file specified at the local side from TFTP server. If neither the local client nor the DHCP server has specified the configuration file name, the switch will obtain the file named "startup_confg.conf" from the TFTP server to overwrite the local configuration file.

By default, the switch will load the configuration file obtained from TFTP server directly and will not save it at local side. Users can choose to save the configuration file at local side. If there is any configuration file exists at the local side, it will be overwritten.

The Obtaining Process

When the DHCP auto-configuration function of a switch is enabled, the switch will start to search for DHCP server. If several servers responded, the switched will accept the server who responds the most quickly. If there is no response from any DHCP server, the switch will try at most 4 times before it informs the failure. The switch will try at most 3 times for obtaining configuration file from TFTP server; otherwise it will load the local configuration file.

Management-vlan, IP address and gateway will be conserved during the process. However, they may be overwritten by the configurations in the loaded configuration file.

15.8 Monitoring and maintenance

Use the following **show command** for monitoring and maintenance:

Step	Command	Description
1	**show dhcp-server**	Show configuration and statistical

		information of DHCP Server.
2	**show dhcp-server ip-pool**	Show DHCP server IP pool information
3	**show dhcp-server relay-ip**	Show DHCP relay agent address information.

Use **show dhcp-server** command to check DHCP server configuration information:

ISCOM2826#show dhcp-server

DHCP server: Enable

Active VLAN: 1,2

The total enabled VLAN: 2

Max lease time: 1000 m

Min lease time: 32 m

Default lease time: 300 m

Statistics infomation:

Running time: 0 hours 7 munites 33 seconds

Bootps: 0

Discover: 0

Request: 0

Release: 0

Offer: 0

Ack: 0

Nack: 0

Decline: 0

Information: 0

Unknows: 0

Total: 0

Use show dhcp-server ip-pool to show configured address pool information

ISCOM2826#show 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 VLANs: 1

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

Alloted IP address count: 0 1

Use show dhcp-server relay-ip command to show address information of neighbouring agent.

ISCOM2826#show dhcp-server relay-ip

Index	IP Address	IP Mask	Status
1	11.1.1.34	255.255.255.0	active

15.8.1 Typical application

Following are the typical DHCP Relay and Server configuration examples:

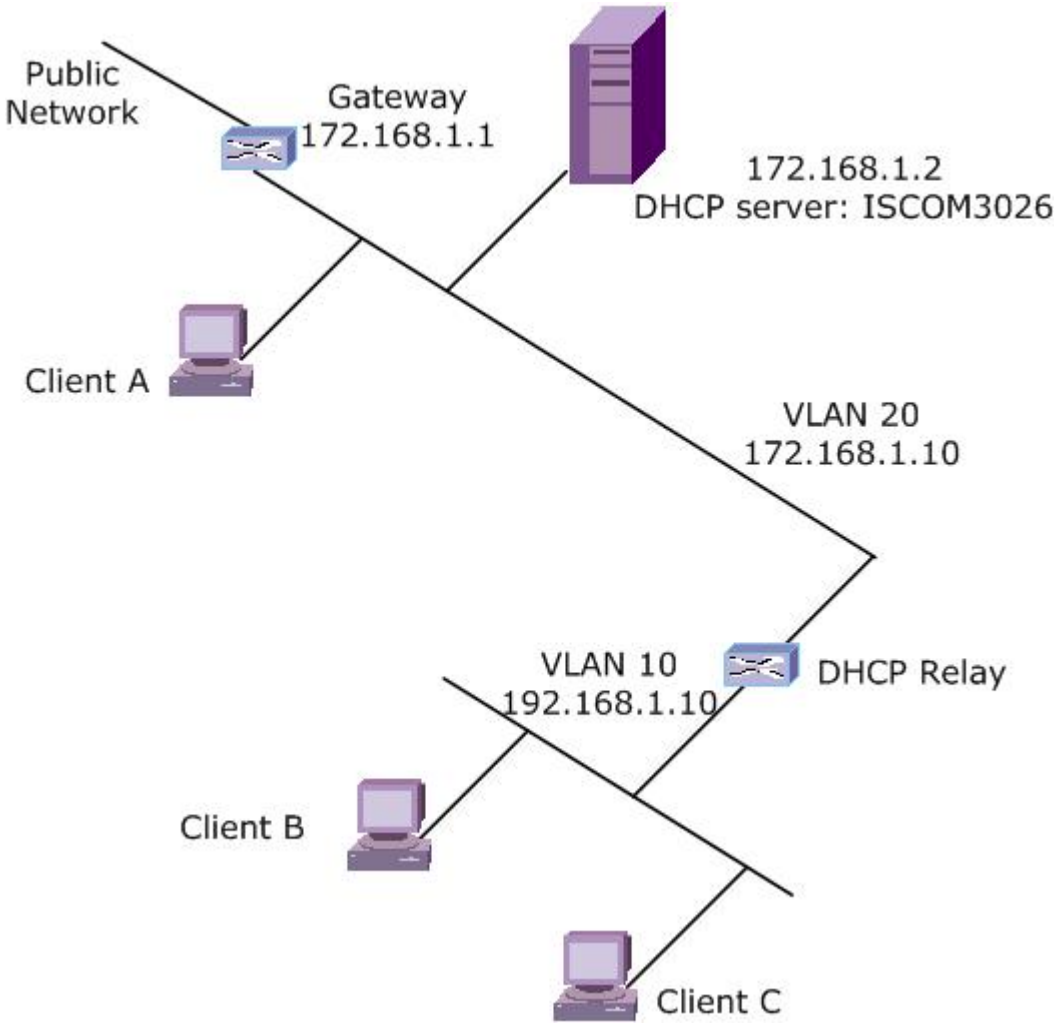
- ✧ Directly connecting client obtains IP address.
- ✧ Remote client obtains IP address through a DHCP relay agent.

1) Introduction

This is a typical application of DHCP protocol:

The ISCOM2826 has two VLAN, VLAN 10 and VLAN 20, connects with two sub-nets: one is 192.168.1.10 and the other is 172.168.1.10. And DHCP server is enabled on ISCOM3026 (suppose that ISCOM3026 works just as a DHCP server here), the IP address is 172.168.1.2. DNS of the subnet is 172.168.1.3. Subnet 1 and subnet 2 access the public network by network gateway 172.168.1.1.

2) Topology



3) Configuration steps

- ✧ Configure DHCP SERVER:
- ✧ Configure VLAN and interface:

```
ISCOM3026(config)# vlan 20
ISCOM3026(config-vlan)# state active
ISCOM3026(config-vlan)# exit
ISCOM3026(config)# interface port 1
ISCOM3026(config-port)# switchport access vlan 20
ISCOM3026(config-port)# exit
```

ISCOM3026(config)# interface ip 2

ISCOM3026(config-ip)# ip address 172.168.1.2 255.255.0.0 20

- ✧ Configure DHCP IP pool

Configure IP pool for subnet 1 and subnet 2 respectively.

ISCOM3026(config)#dhcp-server ip-pool abcdefg1 172.168.1.100 172.168.1.200 255.255.0.0 vlan 20 gateway 172.168.1.1 dns 172.168.1.3

ISCOM3026(config)#dhcp-server ip-pool abcdefg2 192.168.1.100 192.168.1.200 255.255.255.0 vlan 20 gateway 172.168.1.1 dns 172.168.1.3

ISCOM3026(config)# exit

ISCOM3026#show dhcp-server ip-pool

- ✧ Start DHCP server

ISCOM3026 (config)#dhcp-server enable

/*DHCP is enabled on all the VLAN, if you only need to enable the DHCP server function on VLAN20, please disable the function in other VLAN*/

ISCOM3026 (config)#vlan 1

ISCOM3026 (config-vlan)#dhcp-server deactive

ISCOM3026 (config-vlan)#exit

ISCOM3026 (config)#exit

ISCOM3026 # show dhcp-server

- ✧ Set the IP address of DHCP relay agent

ISCOM3026 (config)#dhcp-server relay-ip 192.168.1.10 255.255.255.0

ISCOM3026 (config)#exit

ISCOM3026 # show dhcp-server relay-ip

- ✧ Set the routing to network 192.168.1.0 (subnet 2).

ISCOM3026 (config)#ip route 192.168.1.0 255.255.255.0 172.168.1.10

Configure DHCP Relay

- ✧ Create VLAN and interface

ISCOM3026 (config)# vlan 10

ISCOM3026 (config-vlan)# state active

ISCOM3026 (config-vlan)#exit

ISCOM3026 (config)# interface port 1

ISCOM3026 (config-port)# switchport access vlan 10

ISCOM3026 (config-port)#exit

ISCOM3026 (config)# interface ip 2

ISCOM3026 (config-ip)# ip address 192.168.1.10 255.255.255.0 10

ISCOM3026 (config)# vlan 20

ISCOM3026 (config-vlan)# state active
ISCOM3026 (config-vlan)#exit
ISCOM3026 (config)# interface port 2
ISCOM3026 (config-port)#exit
ISCOM3026 (config)# interface ip 3
ISCOM3026 (config-ip)# ip address 172.168.1.10 255.255.0.0 20

- ✧ Configure server IP address

ISCOM3026 (config)#dhcp-relay server-ip 172.168.1.2
ISCOM3026 (config)#exit
ISCOM3026 #show dhcp-relay server-ip

- ✧ Start DHCP Relay

ISCOM3026 (config)#dhcp-relay enable
ISCOM3026 (config)# vlan 1
ISCOM3026 (config-vlan)# no dhcp-relay listen
ISCOM3026 (config-vlan)#exit
ISCOM3026(config)#exit
ISCOM3026#show dhcp-relay listen

Client obtains IP address.

4) Check the result

- ✧ Check the statistics information and address pool information of DHCP server.

Use show dhcp-server and show dhcp-server ip-pool commands.

- ✧ Check DHCP Relay information

Use show dhcp-relay.

- ✧ Check 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. . . . . :2003.09.08 13:03:24

Lease Expires. . . . . :2003.09.08 13:33:24

✧ Check client end B

c:\>ipconfig /all

Ethernet adapter local network 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. . . . . :2003.09.08 13:03:24

Lease Expires. . . . . :2003.09.08 13:33:24

✧ Check client end C

The content of client C is similar with client B, its IP address is 192.168.1.101.

15.8.2 DHCP Server trouble shooting

- ✧ If DHCP relay IP address has not been specified, the device can not realize DHCP relay agent function normally;
- ✧ When configure the DHCP relay IP address unsuccessfully, the possible reason may be: wrong IP address or there are already 8 IP address (the maximum number);
- ✧ When configure the DHCP IP pool unsuccessfully, the possible reason may be: wrong IP address or there are already 20 IP pools (the maximum number);
- ✧ If it is failed to delete DHCP IP pool, the possible reason is that the address pool doesn't exist or the input parameter is incorrect.
- ✧ If DHCP still can not work normally, please check whether the default gateway or the routing to DHCP relay has been set.

15.8.3 DHCP Server command reference

Step	Command	Description
1	**dhcp-server enable**	Enable DHCP Server function
2	**dhcp-server disable**	Disable DHCP Server function
3	**dhcp-server active vlan-list {1-4094}**	Enable DHCP Server function on designated VLAN.
4	**dhcp-server deactive vlan-list {1-4094}**	Disable DHCP Server function on designated VLAN.
5	**dhcp-server relay-ip** *ip-address*	Configure the IP address of DHCP relay agent IP address.
6	**dhcp-server ip-pool** *name startip endip maskip* **vlan** *vlanlist* **gateway** *gtwip* **dns** *dnsip* **secondary-dns** *dnsip*	Configure DHCP IP pool.
7	**dhcp-server default-lease** *timeout*	Set the default lease time of DHCP table.
8	**dhcp-server max-lease** *timeout*	The maximum lease time
9	**dhcp-server min-lease** *timeout*	The minimum lease time
10	**show dhcp-server**	Show configuration and statistics information of DHCP server.
11	**show dhcp-server relay-ip**	Show the DHCP relay agent IP address of DHCP server.

Chapter 16 IGMP SNOOPING Configuration

16.1 IGMP Snooping function configuration

- ✧ About IGMP Snooping
- ✧ Configuration task list
- ✧ Monitoring and maintenance
- ✧ Typical application
- ✧ Trouble shooting

16.2 About IGMP Snooping protocol

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. IGMP snooping requires LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure MAC multicast groups by using the **ip igmp snooping static** command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings.

Raisecom series switches supports 256 (255 of ISCOM2826) IP multicasts groups, and support IGMPv1 and IGMP v2 version.

16.3 IGMP snooping configuration list

The configuration for IGMP snooping includes:

- ✧ 1 Enable and disable IGMP Snooping
- ✧ 2 IGMP Snooping aging time
- ✧ 3 Multicast Router port configuration
- ✧ 4 Configuring immediate-leave function
- ✧ 5 Manually configure multicast MAC address table.

16.3.1 IGMP Snooping enable and disable

IGMP snooping is disabled on the switch by default. If IGMP snooping is globally enabled/disabled, all the VLAN will enable or disable IGMP snooping function. The following commands are used to enable

IP IGMP Snooping:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip igmp snooping**	Enable IGMP Snooping
3	**exit**	Exit to privilege mode
4	**show ip igmp snooping**	Show configuration situation

Use **no ip igmp-snooping** command to disable IP IGMP Snooping.

This command is used to globally disable IGMP snooping function. In order to disable IP IGMP snooping function on particular VLAN, use the following commands under VLAN configuration mode.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**vlan** *vlan-id*	Enter VLAN configuration mode
3	**no ip igmp snooping**	Disable the IGMP snooping function for this VLAN.
4	**exit**	Exit to global configuration mode
5	**exit**	Exit to privileged EXEC mode
6	**show ip igmp snooping vlan** *vlan-id*	Show VLAN configuration information

In order to enable IGMP snooping function on the VLAN, use **ip igmp snooping** in VLAN configuration mode.

If IGMP snooping is disabled globally, IGMP snooping function can not be enabled on particular VLAN.

If user needs to enable or disable IGMP Snooping function on several VLANs, use **ip igmp-snooping vlan** command in global configuration mode according to the following table:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip igmp snooping vlan 1-100**	Enable IGMP snooping function on VLAN1-100
3	**exit**	Exit to privileged user mode
4	**show ip igmp snooping**	Show IGMP Snooping configuration information

Use **no ip igmp snooping vlan** command to disable IGMP snooping function on several VLAN at a time.

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

Raisecom#show ip igmp snooping

IGMP snooping: Enable

IGMP snooping aging time: 300s

IGMP snooping active VLAN: 1,2

IGMP snooping immediate-leave active VLAN: --

Raisecom#show ip igmp snooping vlan *2*

IGMP snooping: Enable

IGMP snooping aging time: 300s

IGMP snooping on VLAN 2: Enable.

IGMP snooping immediate-leave on VLAN 2: Disable.

16.3.2 IGMP snooping aging time configuration

If switch does detect IGMP Snooping Join or Query message within a period, the subscriber may have left already without sending any leaving message, so the switch needs to be deleted the multicast MAC address from the address table. The default aging time is 300 seconds. Configuration steps are showed as follows:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**ip igmp snooping timeout** *timeout*	Set IGMP overtime.
3	**exit**	Exit to privilege EXEC mode
4	**show ip igmp snooping**	Show IGMP Snooping configuration information

The range of aging time is 30 seconds to 3600 seconds, in order to recover default value, use following command: **no ip igmp snooping timeout**

Example:

Raisecom**#config**

ISCOM2826(config)# **ip igmp snooping timeout** *1200*

ISCOM2826(config)**#exit**

Raisecom#show ip igmp snooping

IGMP snooping: Enable

IGMP snooping aging time: 3000s

IGMP snooping active VLAN: 1, 2

IGMP snooping immediate-leave active VLAN: 1

16.3.3 Multicast Router port configuration

The Multicast Router port can be assigned by dynamically address learning (through IGMP request

message), or manually configured (that is to say, multicast report and leave message of downlink hosts can be forwarded to multicast router port). The manual configuration steps of multicast router port are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip igmp snooping mrouter vlan <1-4094> port <1-26>**	Configure router port
3	**exit**	Exit to privileged EXEC mode
4	**show ip igmp snooping mrouter**	Show Multicast Router port configuration information

Use following command to delete configured Multicast Router port: no ip igmp snooping mrouter vlan 1 port 2

Configuration example:

ISCOM2826#**config**

ISCOM2826(config)#ip igmp snooping mrouter vlan 1 port 2

ISCOM2826(config)#exit

ISCOM2826#show ip igmp snooping mrouter

Ip Address	Port	Vlan	Age	Type
224.0.0.0/8	2	1	--	USER

16.3.4 Immediate-leave function configuration:

When you enable IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port.

The settings are as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**vlan 1**	Enter VLAN configuration mode
3	**ip igmp snooping immediate-leave**	Set immediate-leave function on the VLAN.
4	**exit**	Exit to global configuration mode.
5	**exit**	Exit to privilege EXEC mode.

6	**show ip igmp snooping**	Show IGMP Snooping configuration information

In VLAN configuration mode, use **no ip igmp snooping immediate-leave** command to restore default setting:

Configuration example:

ISCOM2826**#config**

ISCOM2826 (config)**#vlan 1**

ISCOM2826 (config-vlan)# **ip igmp snooping immediate-leave**

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

ISCOM2826 (config)**#exit**

ISCOM2826**#**show ip igmp snooping vlan 1

IGMP snooping: Enable

IGMP snooping aging time: 300s

IGMP snooping on VLAN 1: Enable.

IGMP snooping immediate-leave on VLAN 1: Enable.

In order to configure the immediate-leave function in multiple VLAN, use following commands:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**ip igmp snooping vlan** *vlanlist* **immediate-leave**	Set immediate-leave function on the VLAN.
3	**exit**	Exit to privileged EXEC mode.
4	**show ip igmp snooping**	Show IGMP Snooping configuration information

In order to restore default settings, use following command: **no ip igmp snooping vlan** *vlanlist* **immediate-leave**

Example:

iscom2016**#config**

iscom2016(config)# **ip igmp snooping vlan 1-10 immediate-leave**

iscom2016(config)**#exit**

iscom2016**#show ip igmp snooping**

igmp snooping is globally Enabled

igmp snooping aging time is 1200(s)

IGMP snooping active vlan: 1

IGMP snooping immediate-leave active vlan:1-10

16.3.5 Configure the multicast MAC address

When a host connected to the switch wants to join an IP multicast group, it sends an IGMP join message. Alternatively, when the switch receives a general query from the router, it forwards the query to all ports in the VLAN. So the switch learns the multicast MAC address dynamically. Administrators also can manually configure the multicast MAC address according to the following commands:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mac-address-table static multicast** *mac-addr* **vlan** vlanid **port-list** *portlist*	Add the port to the multicast group
3	**exit**	Exit to privilege user mode
4	**show mac-address-table multicast**	Show multicast MAC address information

The MAC address is the multicast MAC address, and the format is HHHH.HHHH.HHHH. For example, multicast IP address 224.8.8.8 is mapped to multicast MAC address 0100. 5e08.0808; the range of the port is from 1 to 26. In order to delete the port from multicast group manually, use command no mac-address-table static multicast mac-addr vlan vlanid port-list portlist.

Configuration example:

```
Raisecom#config
ISCOM2826(config)# mac-address-table static multicast 0100.5e08.0808 vlan 2 port-list 1-6
ISCOM2826(config)#exit
ISCOM2826# show mac-address-table multicast
Multicast filter mode: Forward-all
Vlan    Group Address       Ports[Static](Hardware)
----------------------------------------------------------------
2       0100.5E08.0808      1-6[1-6](1-6)
```

16.4 Monitoring and maintenance

Use show command to check switch IGMP snooping running and configuration status:

Step	Command	Description
1	**show ip igmp snooping** [**vlan** *vlan-id*]	Show IGMP snooping configuration information in all the VLAN or designated VLAN of the

		switch.
2	**show ip igmp snooping multicast** [**vlan** *vlan-id*]	Show multicast router port information (dynamically learned or manually configured) of all the VLAN or a designated VLAN.
3	**show mac-address-table multicast** [**vlan** *vlan-id*] [**count**]	Show all the multicast MAC address; *Count*: indicates the total number of multicast MAC address

Use s**how ip igmp snooping** command to check configuration information, for example the timer, VLAN configuration information.

Show IGMP Snooping configuration information:

```
Raisecom# show ip igmp snooping
IGMP snooping: Enable
    IGMP snooping aging time: 300s
    IGMP snooping active VLAN: 1, 2
    IGMP snooping immediate-leave active VLAN: 1
```

Use **show ip igmp snooping vlan** *vlanid* command to show the IGMP snooping information in a particular VLAN. If you do not specify VLAN, all the VLAN information will be displayed, that is all the existent and active VLAN.

Show igmp-snooping multicast router information:

```
Raisecom# show ip igmp snooping mrouter
    Ip Address          Port    Vlan  Age       Type
    ------------------------------------------------
    224.0.0.0/8         4       3     --        USER
```

```
Raisecom#show mac-address-table multicast
Multicast filter mode: Forward-all
    Vlan  Group Address     Ports[Static](Hardware)
    ---------------------------------------------------------------
    2     0100.5E08.0808    1-6[1-6](1-6)
```

16.5 IGMP snooping trouble shooting

- ✧ If multicast router port has not been specified, all the IGMP reports will be transmitted to the port directly connected to the router;
- ✧ If it is failed to add port to a multicast group manually, the reason may be incorrect multicast MAC address format or the maximum layer 2 multicast router table (255) has been achieved;
- ✧ If it is failed to delete the port from multicast group manually, the possible reason may be incorrect multicast MAC address format or MAC address/VLAN/port are not existent in multicast router.

16.6 IGMP Snooping command reference

Step	Command	Description
1	**ip igmp snooping**	Enable IGMP Snooping
2	**ip igmp snooping timeout**	Configure the aging time of IGMP snooping
3	**ip igmp snooping**	Enable the IGMP snooping function of a particular VLAN.
4	**ip igmp-snooping vlan**	Enable IGMP snooping of multiple VLAN.
5	**ip igmp snooping immediate-leave**	Set immediate-leave function on the VLAN.
6	**ip igmp snooping vlan immediate-leave**	Set immediate-leave function on the VLAN.
7	**ip igmp snooping mrouter port**	Set multicast router port
8	**show ip igmp snooping**	Show IGMP snooping configuration information.
9	**show ip igmp snooping multicast**	Show dynamically learned or manually configured multicast router port information.
10	**show mac-address-table multicast**	Show multicast MAC address

Chapter 17 RMON Configuration

17.1 RMON Introduction

RMON is an Internet Engineering Task Force (IETF) standard monitoring specification that allows various network agents and console systems to exchange network monitoring data. You can use the RMON feature with the Simple Network Management Protocol (SNMP) agent in the switch to monitor all the traffic flowing among switches on all connected LAN segments.

The switch supports these RMON groups (defined in RFC 1757):

- ✧ Statistics (RMON group 1)—Collects Ethernet, Fast Ethernet, and Gigabit Ethernet statistics on an interface.
- ✧ History (RMON group 2)—Collects a history group of statistics on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces for a specified polling interval.
- ✧ Alarm (RMON group 3)—Monitors a specific management information base (MIB) object for a specified interval, triggers an alarm at a specified value (rising threshold), and resets the alarm at another value (falling threshold). Alarms can be used with events; the alarm triggers an event, which can generate a log entry or an SNMP trap.
- ✧ Event (RMON group 9)—Determines the action to take when an event is triggered by an alarm. The action can be to generate a log entry or an SNMP trap.

RMON relevant commands include configuration command and show information commands, they are:

Config statistics group

Config history group

Config alarm group

Config events group

Show the result

17.2 RMON configuration

Config statistics group

Statistics collects Ethernet, Fast Ethernet, and Gigabit Ethernet statistics on an interface. The statistics function is enabled by default; use **no** format to disable the function.

*note: disable the statistics function indicates that the user cannot get the statistics data any more, and this does not mean the switch will stop the statistics.

Step	Command	Description

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

Disable RMON statistics function, use **no rmon statistics** {**ip** *l3_interface* | **port** *port_list*} command.

Example:
Set the statistics group function for physical port 1-5, the owner name is Raisecom.
Raisecom#config
Raisecom(config)#rmon statistics port 1-5 owner raisecom
Raisecom(config)#exit
Raisecom#show rmon statistics port

Example:
Set the statistics group function of layer 3 interface 1, 5-10, owner name is config.
Raisecom#config
Raisecom(config)# rmon statistics ip 1,5-10 owner config
Raisecom(config)#exit
Raisecom#show rmon statistics ip

Config history group:

History collects a history group of statistics on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces for a specified polling interval.
RMON history group function is enabled by default, including layer-3 management interface and physical interfaces. Use no format of the command to disable this function.

If the history statistics group is disabled, all the old history statistics data will be cleared and no more data will be collected.

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

Close the history group, use **no rmon history** {**ip** *l3_interface* | **port** *port_list*}

Example:

Set the RMON history function for physical port 1-5, owner name is Raisecom.

```
Raisecom#config
Raisecom(config)#rmon history port 1-5 owner raisecom
Raisecom(config)#exit
Raisecom#show rmon history port
```

Example:

Set the statistics function of layer 3 interface 1,5-10.

Raisecom#config

Raisecom(config)# rmon history ip 1,5-10

Raisecom(config)#exit

Raisecom#show rmon history ip

Configure Alarm group

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

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rmon alarm** *Number MIBVAR* [**interval** *time*] {**delta** | **absolute**} **rising-threshold** *value [event-number]* **falling-threshold** *value [event-number]* **owner** *string*	*Number* Alarm index number, range is <1-512〉; *MIBVAR* specify the MIB object that will be monitored. *time* unit is second, period for the monitoring of MIB object; **delta** get the sampling difference between two MIB variables. **absolute** get sampling MIB variable directly **rising-threshold** *value* rising threshold *event-number* the event number which will be triggered by the rising threshold **falling-threshold** *value* falling threshold *event-number* the event number which will be triggered by the falling threshold

		owner *string* specify the owner of Alarm.
3	**exit**	Exit from global configuration mode.
4	**show alarm** *number*	Show the configuration information

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

Example:

Set an alarm, monitor MIB variable 1.3.6.1.2.1.2.2.1.20.1 for every 20 seconds. Check the rising or falling of this variable. If the value increases 15, alarm will be triggered; the name of the owner is system.

Raisecom#config

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

Raisecom(config)#exit

Raisecom#show rmon alarm 10

Config event group

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

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

Use **no event *number*** to delete the event configuration

Example:

Create the event with an index 1, the community name of the trap is event trap, description string is High-ifOutErrors, owner is system.

Raisecom#config

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

Raisecom(config)#exit

Raisecom#show rmon event 1

Restore the default configuration:

Set all the function of RMON group to default status:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**clear rmon**	Restore to default status
3	**exit**	Exit from global configuration mode

17.3 Show RMON configuration information

Step	Command	Description
1	**show rmon**	Show all the information of RMON.
2	**show rmon alarms**	Show alarm information, including alarm number, name, threshold, sampling period and sampling value.
3	**show rmon events**	Show event information, including event number, name, description, log/trap etc.
4	**show rmon history**	Show port information which has enabled historical group
5	**show rmon statistics**	Show port information which has enabled statistics group.

Chapter 18 ARP Management

18.1 ARP address table introduction

To communicate with a device (over Ethernet, for example), the software first must determine the 48-bit MAC or the local data link address of that device. The process of determining the local data link address from an IP address is called *address resolution*.

The Address Resolution Protocol (ARP) associates a host IP address with the corresponding media or MAC addresses. Taking an IP address as input, ARP determines the associated MAC address. Once a MAC address is determined, the IP-MAC address association is stored in an ARP cache.

ARP address mapping table includes 2 types of MAC addresses:

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

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

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

18.2 Configuring ARP

18.2.1 Add static ARP entries

Static ARP entries must be manually added and do not age, must be manually deleted.
Refer to the following

Step	Command	Description
1	**arp** *ip-address mac-address*	Add a static ARP entry *ip-address:* IP address *mac-address:* MAC address

		related to the IP address, format is HHHH.HHHH.HHHH. For example: 0050.8d4b.fd1e.

18.2.2 Delete ARP address mapping term:

Step	Command	Description
1	**No arp** *ip-address*	Delete an entry in the ARP table.

Use **no arp** *ip-address* command to delete an entry from ARP address mapping table.

18.2.3 Set the aging time of ARP dynamic learned entries.

Step	Command	Description
1	**arp aging-time** *sec*	Set the aging time of ARP dynamic table.

This command is used to set the aging time of ARP dynamic address entries, the ARP dynamic learned address will be aged automatically according to this value. The range of aging time is 0, 30-2147483, If the aging time is 0, ARP dynamic learned address entries will not be aged.

18.2.4 Clear ARP address mapping table

Step	Command	Description
1	**clear arp**	Clear all the entries in ARP address mapping table.

Use clear arp command to delete all the entries in MAC address table.

18.3 Show ARP address mapping table

Step	Command	Description
1	**show arp**	Show all the entries in ARP address mapping table.

Use this command to show all the entries in ARP address mapping table.

Chapter 19 SNMP Configuration

19.1 SNMP protocol introduction

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a management information base (MIB). The SNMP manager can be part of a network management system (NMS). The agent and MIB reside on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

Raisecom series switches SNMP Agent support SNMPv1, SNMPv2 and SNMPv3.

19.2 SNMP configuration

SNMP management consists of two parts: one is that SNMP agent responses to manager's request and another is that SNMP agent sends traps. All the processes are based on users or communities. This chapter introduce SNMP configuration:

- ✧ SNMP user configuration
- ✧ SNMP communication configuration
- ✧ TRAP configuration

19.2.1 Configure SNMP user

SNMPv3 is based on user-based security model. No matter NMS sends request packets to SNMP Agent, or SNMP Agent sends Traps to NMS, the communication between NMS and SNMP Agent are based on particular user. SNMP NMS and agent maintain a local SNMP user table, which records user names; user associated engine ID, and other information like whether to be authenticate. No matter who gets message from other part, the receiving end will search the user table and encryption information, and then resolve it and give a proper response. Configure the SNMP user through the command line and switch will add an entry in the SNMP user table.

Table 19.1 configure SNMP user

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

Except *username*, all the other parameters are optional: ***engineid*** is the user associated SNMP engine ID, default is local engine ID; **md5** | **sha** is the authentication algorithm. Without the input parameter [**authentication**{**md5** | **sha**} *authpassword*], the user's password will not be authenticated; authpassword is authentication password.

Example 1:

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

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

Example 2:

Add a user *guestuser2* without engine ID:

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

Example 3:

Delete user *guestuser2*, without engine ID:

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

19.2.2 SNMP community configuration

SNMP protocol has several safety access control models.

1 The access control based on SNMP community

SNMP community strings authenticate access to MIB objects and function as embedded passwords. All the SNMP Get and Set operations of NMS should use the correct community strings; otherwise the SNMP agent will not response to the request. That is to say, SNMPv1 and SNMPv2 use community strings as operation passwords when access the switch.

A community string can have one of the attributes:

Read-only (RO): give read access to authorized management stations to all objects in the MIB, but does not allow write access;
Read-write (RW): give both read and write access to authorized management stations to all objects in the MIB.

Please refer to the following commands for the configuration of SNMP community:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server community** *community-name* [**view** *view-name*] { **ro** | **rw** }	Configure the community name and the relevant attributes. *view-name:* the view name ro: read-only rw: read-and-write
3	**exit**	Exit to privileged mode.
4	**show snmp community**	Show configuration information

Example 1:

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

Use this command to define the community name as Raisecom. This command does not specify the view. When the community name is configured, the network manager uses community name Raisecom to search all the MIB variables in Internet view of the switch.

Example 2:

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

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

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

The second command defines community name *guest*, and network management can use guest to search the MIB variable of *mib2* view in the switch.

2 Access control based on the user

SNMPV3 uses USM (user-based security model) for access control. USM uses **group** for the access control: One or more users belong to a group, each group is configured the relative read, write and notification view, the user in the group has the privilege within the view.

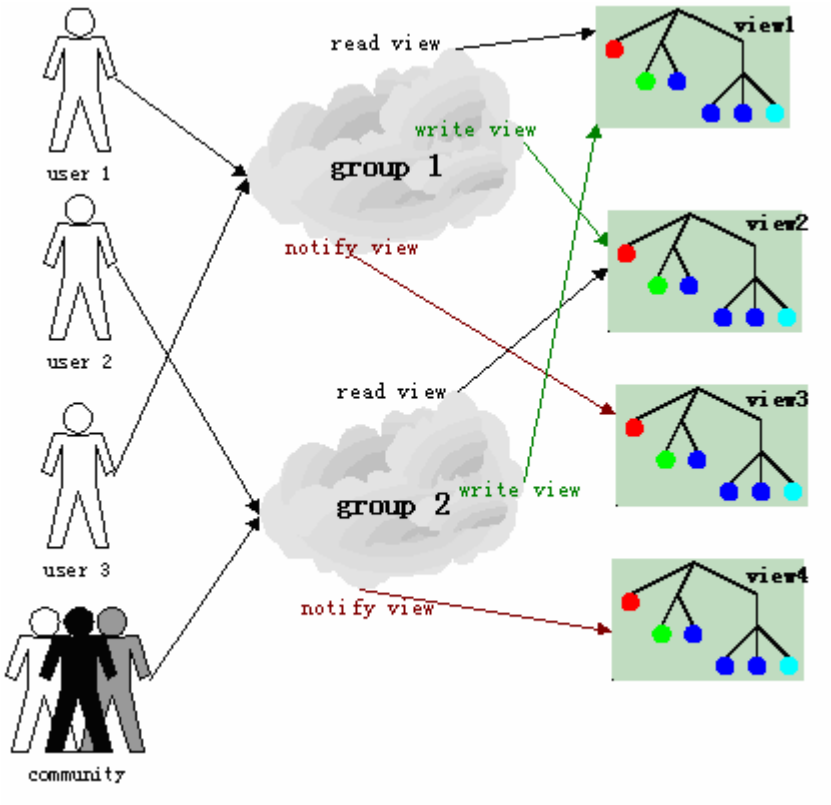


Figure 1 SNMPV3 access control model

From above figure, we know that if NMS wants to access the switch, there should be the user, the group which user belongs to, the view and the privilege of the view.

Please refer to the following commands for SNMPV3 group configuration:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server user** *username* [**remote** *engineid*] [**authentication**{**md5** | **sha**} *authpassword*]	Add a user
3	**snmp-server view** *view-name oid-tree* [*mask*] {**included** | **excluded**}	Define the view and its privilege of the MIB *view-name* specify the configured name of view ,*oid-tree* specify OID tree *mask* the mask of OID sub-tree, each bit corresponds to a note of the sub-tree **included** means that the scale of

		the view includes all the MIB variables under OID tree **excluded** means that the scale of the view includes all the MIB variables out of OID tree
4	**snmp-server group** *groupname* **user** *username* { **v1sm | v2csm | usm**}	Configure the group which the user belongs to
5	**snmp-server access** *groupname* **[read** *readview***] [write** *writeview***] [notify** *notifyview***] [context** *contextname* **[{exact | prefix}]]** { **v1sm | v2csm | usm**} { **noauthnopriv | authnopriv** }	Define the access privilege of the group *Groupname* is the name of access group; *readview* is the read view, default is internet; *writeview* is the write view, default is empty; *notifyview* is informational view, default is empty; *contextname* is the name of context or its prefix; **exact|prefix** stands for the match type of the context name: **exact** means the input should be fully matched with the name of context, **prefix** means that only the first several letters should match with the name of context; **v1sm|v2csm|usm** are the security model, stands for SNMPv1 security model,SNMPv2 is the security model based on community and SNMPv3 is the security model based on the user respectively; **noauthnopriv|authnopriv** is the security level, stands for no authentication and no encryption, or authentication without

		encryption respectively.
6	**exit**	Exit to privileged configuration mode
7	**show snmp group** **show snmp access** **show snmp view** **show snmp user**	Show SNMP configuration information

*note: when configure the view, for the parameter *mask,* 0 indicates does not need to match and 1 indicates must match. The maximum length of mask is 16 characters; that is to say, it supports the sub-tree of depth 128. For example: a view OID sub-tree is 1.3.6.1.2.1, mask is 1.1.1.1.0.1, and then real sub-tree belongs to the view is 1.3.6.1.x.1 (x can be any number). The default view of the switch is Internet; the view includes all the MIB variables under the tree 1.3.6. All bits of mask are 1 by default.

*note: When delete an access group, the name of group, name of context, security mode and security level should be specified

If the security model is v1sm or v2csm, security level is **noauthnopriv**, so there is no option of {**noauthnopriv | authnopriv**}, and at the same time, there is no option of **[context** *contextname* **[{exact | prefix}]].**

Example 1:

Create an access group “guestgroup”, security model is USM, security level is authentication without encryption, read view is mib2, both with view and information view are empty by default:

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

Example 2:

Delete access group guestgroup:

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

- ✧ **Configure the mapping from user to group**

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

Example 1:

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

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

Example 2:

Delete the mapping of *guestuser 1* with security level usm from access group *guestgroup.*

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

19.2.3 TRAP configuration

To configure the trap function of SNMP, user should configure the IP address of target SNMP server which will receive the Trap.

The user name, SNMP version information, security level (whether need to be authenticated or encrypted) should be configured for SNMPv3 Trap configuration.

Please refer to the following commands for the configuration of SNMP trap server:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server host** *A.B.C.D* version {1|2c} NAME [**udpport** *<1-65535>*] [bridge] [config] [interface] [rmon] [snmp] [ospf]	Configure the target host of SNMPv1/v2 Trap.
3	**snmp-server host** *A.B.C.D* version 3 { noauthnopriv | authnopriv } NAME [**udpport** *<1-65535>*] [bridge] [config] [interface] [rmon] [snmp] [ospf]	Configure Trap target host of SNMPv3
4	**exit**	Exit to privilege EXEC mode.

Example 1:

Add an SNMP trap server which IP address is *172.20.21.1*, user name is *raisecom*, and SNMP version is v3, authentication without encryption.

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

Example 2:

Delete the SNMP trap server:

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

19.3 Other configuration

- ✧ **Configure contact information of network administrators**

Please refer to the following commands for the configuration of the switch manager's contact information

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

Example:

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

✧ **Enable or disable SNMP trap function**

Traps are mainly used by SNMP agent to report some important events to the SNMP NMS. Please refer to the following command for the configuration of SNMP trap.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server enable traps**	Enable trap function
	no snmp-server enable traps	Disable trap function
3	**exit**	Exit to privilege EXEC mode
4	**show snmp config**	Show SNMP configuration information

✧ **Configure the position of the switch**

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

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

Example: set the physical position information of the switch to HaiTaiEdifice8th.

Raisecom(config)#snmp-server location HaiTaiEdifice8th

19.4 Show SNMP configuration information

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

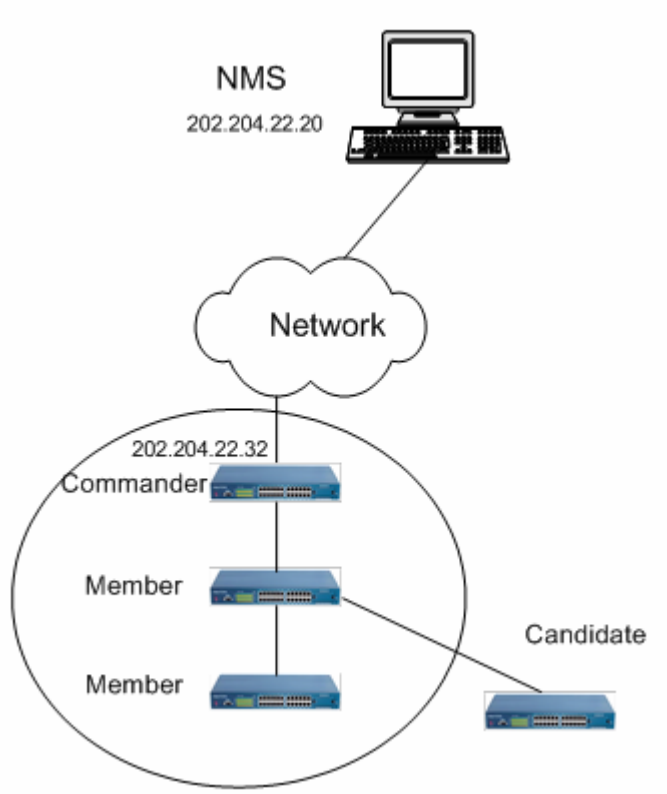
Chapter 20 Cluster Management

This chapter introduces the cluster configuration management function of the switch, including the following information:

- ✧ Cluster introduction
- ✧ Cluster management configuration list
- ✧ Monitoring and maintenance

20.1 Cluster introduction

A switch cluster is a group of connected ISCOM switches that are managed as a single entity. The command switch is the single point of access used to configure, manage, and monitor the member switches. Cluster members can belong to only one cluster at a time. Network administrators can use a public IP address of one switch to realize the management for several switches. The switch with IP address is the commander and other managed devices are members. Generally speaking, members do not need to set IP address. Realize the management and maintenance by device redirection. Typical application condition like following figure:



Cluster management includes three protocols: RNDP (Raisecom Neighbor Discover Protocol), RTDP

(Raisecom Topology Discover Protocol) and RCMP (Raisecom Cluster Management Protocol). RNDP is in charge of neighbor discovery and information collection, RTDP is in charge of the collecting and processing topology information, RCMP is in charge of the functions like adding, active, and deleting cluster members. RTDP and RCMP protocol communicate with each other in VLAN 2. So if there is no such a device that supports Raisecom cluster management functions between two cluster management devices. It needs proper configuration for VLAN2 to make sure normal communication between RTDP and RCMP.

The position and function of the switch are different in the cluster, so different switch has different role in the cluster. The switches can be commander, member and candidate.

- Commander: the commander has public IP address, provides the management interface for all the switches in the cluster. Commander uses command redirection to manage the members: users send the management command to the commander through public network, and the commander will handle the command, if the commander finds that this command is for other members it will send the commands to members. Commanders have the functions: discover neighbor Raisecom switches, collect the network topology, cluster management, maintaining cluster status, and support different proxy.
- Member: cluster members do not have IP address. User uses the command redirection function to manage the device. Member device has the functions including discovering neighbor, receiving the management info of commander, executing the proxy command, failure/log report function. Once the member is active, it can be managed by network commander.
- Candidate: the switch does not join any cluster but do have cluster capability, it can be member.
- Each cluster has to designate a commander. When commander is designated, it can discover candidates by RNDP and RTDP.
- When candidate is added to the cluster, it becomes a member; user has to active this switch by cluster management function, or by configuring automatically active function on the switch to active the cluster function.

20.2 Cluster management configuration list

1. Enable RNDP globally
2. Enable RNDP on a particular port
3. Enable RTDP
4. Configure RTDP collection range
5. Enable and disable cluster management function

6. Automatically active candidates
7. Add and active cluster member
8. Delete cluster member
9. Suspend cluster member
10. Add and active all the candidate
11. Remote management of cluster member

20.2.1 Globally enable RNDP

Enable or disable RNDP function globally in global configuration mode, RNDP is enabled by default; all the ports take part in RNDP report and discovery.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rndp** {**enable	disable**}	Globally enable or disable RNDP
3	**exit**	Exit to privilege EXEC mode
4	**show rndp**	Show RNDP configuration

Globally disable RNDP function

```
Raisecom#config
Raisecom(config)#rndp dis
Raisecom(config) #exit
Raisecom #show rndp
```

20.2.2 Enable RNDP on a particular port

In physical port configuration mode, user can enable or disable RNDP function, all the ports take part in RNDP report and discovery by default.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port <1-26>**	Enter port configuration mode
3	**rndp** {**enable	disable**}	Enable or disable RNDP
4	**exit**	Exit to privilege EXEC mode
5	**show rndp**	Show RNDP configuration

Following example is to deny RNDP function on port 1:

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

Raisecom(config-port)#rndp dis

Raisecom(config-port) #exit

Raisecom(config) #exit

Raisecom #show rndp

20.2.3 Enable RTDP

Under global configuration mode, user can enable or disable RTDP function, RTDP is disabled by default. If RTDP is enabled, RTDP will collect all the information of Raisecom switch which RNDP function is enabled.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rtdp** {**enable	disable**}	Enable or disable RTDP collection.
3	**exit**	Exit to privilege EXEC mode.
4	**show rtdp**	Show RTDP collection.

Following command is to enable RTDP collection function:

Raisecom#config

Raisecom(config)#rtdp enable

Raisecom(config) #exit

Raisecom #show rtdp

20.2.4 Configure RTDP collection range

Under global configuration mode, user can set the collection range of RTDP, RTDP can collect device information within 16 hops as the default.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rtdp max-hop <**1-16**>**	Configure RTDP collection range
3	**exit**	Exit to privilege EXEC mode
4	**show rtdp**	Show RTDP configuration information

Following example is to set the RTDP collection range to 1 hop:

Raisecom#config

Raisecom(config)#rtdp max-hop 1

Raisecom(config) #exit

Raisecom #show rtdp

20.2.5 Enable and disable cluster management

In default situation, the cluster management function of the system is disabled. User can use following command to disable or enable cluster management function:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**cluster**	Enable cluster management function
3	**exit**	Exit to global configuration mode
4	**exit**	Exit to privilege EXEC mode
5	**show cluster**	Show cluster relevant information

Following command is used to enable cluster management function:

Raisecom#config
Raisecom (config)#cluster
Raisecom (config-cluster)#exit
Raisecom (config) #exit
Raisecom #show cluster

Following command is used to disable cluster management function

Raisecom#config
Raisecom (config)#no cluster
Raisecom (config) #exit
Raisecom #show cluster

20.2.6 Automatically active function

Users can use cluster-autoactive command to enable automatic active function. No cluster-autoactive command will disable the function. When the autoactive function is enabled, and the commander MAC address is configured, the switch will set itself as an active member automatically.

By cluster-autoactive commander-mac command, the MAC address of commander switch can be configured. no cluster-autoactive commander-mac will recover to the commander address to 0000.0000.0000.

This MAC address is only available when the autoactive function is enabled.

User can use following commands to disable or enable automatic active function:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**[no] cluster-autoactive**	Enable or disable automatic active function
3	**[no] cluster-autoactive commander-mac** *HHHH.HHHH.HHHH*	Configure the MAC address of the commander.
4	**exit**	Exit to global configuration mode.
5	**exit**	Exit to privileged EXEC mode.
6	**show cluster**	Show cluster information

Following commands are used to enable autoactive active function and set the MAC address of the switch to 1111.2222.3333:

Raisecom#config
Raisecom(config)# cluster-autoactive
Raisecom(config)# cluster-autoactive commander-mac 1111.2222.3333
Raisecom(config)#exit
Raisecom#show cluster

20.2.7 Add and active cluster member

Use member command to add and active candidates of the cluster or active members; it also can delete some or all the members from the cluster. When the key word “active” is not used, the command will add the member to the cluster, but not active the member (but if auto-active function of this member is enabled, and the auto-active commander for this member is current switch’s MAC address, then the member will be auto activated when it is added).

Step	Command	Description
1	**config**	Enter global configuration mode
2	**cluster**	Enter cluster management mode
3	**member** *HHHH.HHHH.HHHH* [active *username password*]	Add member to the cluster; Active: active the switch that has been added to the cluster. Usrename: the user name for active the switch Password: the password for active the switch
4	**exit**	Exit to global configuration mode.

5	**exit**	Exit to privilege EXEC mode
6	**show cluster member** [*HHHH.HHHH.HHHH*]	Show cluster member relevant information.

Following example is to add cluster member 1111.2222.3333:

Raisecom#config
Raisecom(config)#cluster
Raisecom(config-cluster) #member 1111.2222.3333
Raisecom(config-cluster) #exit
Raisecom(config) #exit
Raisecom #show cluster member

20.2.8 Delete cluster member

In cluster management mode, user can delete the member that does not need the cluster management function.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**cluster**	Enter cluster management mode.
3	**no member** {*HHHH.HHHH.HHHH* | **all**}	Delete one or all the members; HHHH.HHHH.HHHHis the member's MAC address that will be deleted. All: delete all the members;
4	**exit**	Exit to global configuration mode.
5	**exit**	Exit to privilege EXEC mode
6	**show cluster member**	Show cluster member information

Follow example is to delete cluster member 1111.2222.3333:

Raisecom#config
Raisecom(config)#cluster
Raisecom(config-cluster) #no member 1111.2222.3333
Raisecom(config-cluster) #exit
Raisecom(config) #exit
Raisecom #show cluster member

20.2.9 Suspend Cluster member

In cluster management mode, user can suspend the member which is in active mode, but it has not

been deleted from the cluster. When the device is suspended, user cannot manage the device by cluster management any more. User following steps to active cluster member:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**cluster**	Enter cluster management mode
3	**member** *HHHH.HHHH.HHHH* **suspend**	Suspend cluster member. HHHH.HHHH.HHHH stands for the MAC address of the device that will be suspended. Suspend is the key word to be suspended.
4	**exit**	Exit to global configuration mode.
5	**exit**	Exit to privilege EXEC mode.
6	**show cluster member**	Show cluster member information.

Following example is to suspend cluster member 1111.2222.3333:

Raisecom#config
Raisecom(config)#cluster
Raisecom(config-cluster) #member 1111.2222.3333 suspend
Raisecom(config-cluster) #exit
Raisecom(config) #exit
Raisecom #show cluster member

20.2 10 Add and suspend all the members automatically

To make the operation of add and active members flexibly, this command allows user to use the same username and password to add and active all the members, or add and active the candidate members which autoactive function has been enabled.

User can also use following commands to add or active all the candidate members in the cluster:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**cluster**	Enter cluster management mode
3	**member auto-build** [{**active** *username password*}| {**active** *username password* **all**}]	Add all the candidate members. Active: active the candidates Username: the username that is used for active member. Password: the password that is

		used for active members. All: add and active all the members.
4	**exit**	Exit to global configuration mode
5	**exit**	Exit to privilege EXEC mode
6	**show cluster member**	Show cluster members information

Use member auto-build command to automatically add and active all the members that have enabled autoactive function.

Under command prompt, use member auto-build active username password command to add and active all the members step by step.

Use member auto-build active username password all command to automatically add and active all the candidates.

Use the following commands to add and active all the candidates:

Raisecom#config
Raisecom(config)#cluster
Raisecom(config-cluster) # member auto-build active *raisecom raisecom* all
Raisecom(config-cluster) #exit
Raisecom(config) #exit
Raisecom #show cluster member

20.2.11 Cluster member remote management

Under cluster management mode, user can remotely manage the members which have been active, refer following commands:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**cluster**	Enter cluster management mode
3	**rcommand** { *hostname* | *HHHH.HHHH.HHHH* }	Login cluster member, the hostname is the member name, HHHH.HHHH.HHHH is the MAC address of the member.

Login cluster member 1111.2222.3333:

Raisecom#config

Raisecom(config)#cluster

Raisecom(config-cluster) #rcommand 1111.2222.3333

Login the member with a cluster number name swA.

Raisecom#config

Raisecom(config)#cluster

Raisecom(config-cluster) #rcommand swA

20.3 Monitoring and maintenance

20.3.1 Show RNDP information

Step	Command	Description
1	**show rndp neighbor**	Show the information of the switches which are directly connected with current switch
2	**show rndp**	Show RNDP configuration

Show the information of the switches which are directly connected with current switch:

Raisecom# show rndp neighbor

Use show rndp command to check RNDP configuration:

Raisecom# show rndp

20.3.2 Show RTDP information:

Step	Command	Description
1	**show rtdp device-list** [*HHHH.HHHH.HHHH* | *WORD*] [**detailed**]	Show the information collected by RTDP
2	**show rtdp**	Show RTDP information

Use show rtdp device-list to check all the concise information for neighbor device:

Raisecom# show rtdp device-list

Use show rtdp device-list detailed to check detail information of all devices detected by RTDP:

Raisecom# show rtdp device-list detailed

Use show rtdp device-list HHHH.HHHH.HHHH to check the concise information with designated MAC

device:

Raisecom# show rtdp device-list HHHH.HHHH.HHHH

Use show rtdp device-list HHHH.HHHH.HHHH detailed to check the detail information of the device with the designated MAC address:

Raisecom# show rtdp device-list HHHH.HHHH.HHHH detailed

Use show rtdp device-list WORD to check information of the device with a designated name.

Raisecom# show rtdp device-list WORD

Use show rtdp device-list WORD detailed to check detail information of the device with a designated name:

Raisecom# show rtdp device-list WORD detailed

Use show rtdp to check RTDP configuration:

Raisecom# show rtdp

20.3.3 Show cluster management information

Step	Command	Description
1	**show cluster**	Show cluster information
2	**show cluster member** [*HHHH.HHHH.HHHH*]	Show cluster member information
3	**Show cluster candidate**	Show cluster candidate information

Use show cluster to check current cluster relevant information:

Raisecom# show cluster

Use show cluster member [HHHH.HHHH.HHHH] to check particular cluster member or all the member information:

Raisecom# show cluster member

Use show cluster candidate to check candidates' information:

Raisecom# show cluster candidate

Chapter 21 System Log Configuration

21.1 System log introduction

The log information of switch and some debugging will be exported to the log for process. This process will determine the destination where the log information will be sent: log file, console, TELNET, log host.

The system logging format is:

timestamp module-level- Message content

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

21.2 System log configuration

System log configuration mainly includes the functions below:

- system log on and off
- system log information time stamp configuration
- system log rate configuration
- system log information output configuration
- show log information

21.2.1 System log on and off

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging on**	Enable system log
3	**exit**	Back to privileged EXEC mode
4	**show logging**	Show the configuration

Example:

Raisecom**#config**

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

CONFIG-I:Configured from console ...

Raisecom(config)**#logging on**

set sucessfully!

Raisecom(config)#exit

Raisecom**#show logging**

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

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

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

Time-stamp logging messages: date-time

Log host information:

Target Address Level Facility Sent Drop

21.2.2 Log information time stamp configuration

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

Example:

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

set sucessfully!

21.2.3 Log rate configuration

Stem	Command	Description
1	**config**	Enter global configuration mode
2	**logging rate <1-1000>**	Log number sent every second
3	**exit**	Back to privileged EXEC mode

21.2.4 Log information output configuration

1. Log information output to console or TELNET

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

2. Log host setting

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

Instructions:

local0-local7 log host device name

- **<0-7>** Logging severity level
- **alerts** Immediate action needed (severity=1)
- **critical** Critical conditions (severity=2)
- **debugging** Debugging messages (severity=7)
- **emergencies** System is unusable (severity=0)
- **errors** Error conditions (severity=3)
- **informational** Informational messages (severity=6)
- **notifications** Normal but significant conditions (severity=5)
- **warnings** Warning conditions (severity=4)

Example:

Raisecom(config)**#logging console warnings**
set console logging information successfully

Raisecom(config)#logging host 10.168.0.16 local0 warnings

set log host logging information successfully
Raisecom(config)**#ex**
Raisecom**#show logging**
Syslog logging: enable, 0 messages dropped, messages rate-limited 0 per secon
d
Console logging: enable, level=warning, 18 Messages logged
Monitor logging: disable, level=info, 0 Messages logged
Time-stamp logging messages: enable

Log host Information:

Target Address	Level	Facility	Sent	Drop
10.168. 0. 16	warning	local0	1	0

3. Enable log output

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging file**	Enable log output
3	**exit**	Back to privileged EXEC mode
4	**show logging file**	Show log file

21.2.5 Show log configuration

Step	Command	Description
1	**show logging**	Show the configuration
2	**show logging file**	Show the log file contents

Chapter 22 System Clock

22.1 System clock

Two methods can be used for Raisecom system clock configuration: The first one, use SNTP protocol to make the switch time consistent to SNTP server, the switch time by using this method will be the Greenwich time, switch will make adjustment according to the time zone; The second one, manually set the time, the time by using this method is local time. The configuration of system clock includes

- SNTP service configuration
- Manually set switch time
- Summer time setting

22.1.1 SNTP service configuration

Step	Command	Description
1	**config**	Enter the global configuration mode
2	**sntp master**	Enable the SNTP service
3	**sntp server** A.B.C.D	SNTP service address setting
4	**exit**	Back to privileged EXEC mode
5	**show sntp**	Show the configuration

22.1.2 Manually set switch time

Step	Command	Description
1	**clock timezone** {+|-} <0-11> <0-59>	Switch timezone configuration ·+ Eastern Hemisphere timezone ·- western Hemisphere timezone ·<0-11> offset hours ·<0-59> offset minutes Default time is Beijing time, that is

		8 hours offset in Eastern Hemisphere.
2	**clock set** *<1-24> <0-60> <0-60> <2000-2199> <1-12> <1-31>*	Switch time setting: hour, minute, second, year, month, day in turns
3	**show clock**	Show the configuration

For example, set the local time zone as 10 hours 30 minutes offset to the east, the local time is March 28 2005, 11 o'clock 14 minutes 20 seconds

Raisecom**#clock timezone** – 10 30
set sucessfully!
Raisecom**#clock set** *11 14 20 2005 3 28*
set sucessfully!
Raisecom**#show clock**
Current system time: Mar-28-2005 11:15:05
Timezone offset: -10:30:00

Note that when manually setting the switch time, if you need to use summer time, for example the summer time begins from 2 o'clock in the morning on the second Sunday of April every year till 2 o'clock in the moring on the second Sunday of September, you need to switch the time one hours faster, which means the time offset is 60 minutes, therefore, the time between 2 o'clock and 3 o'clock in the morning on the second Sunday of April does not exist. You will fail to set the time as within this period (set fail).

22.1.3 Summer time configuration

Sun rise earlier in summber, so the daytime is long. In order to save energy and fully utilize the daytime, most countries in the world legally switch the time one hour faster when summer comes up, also half an hour or a couple of hours for that; when the winter comes, the time will be set back. This is called "summber time" which is a legal time.

When the summber time function is enabled, time synchronized by SNTP will be transferred to local summer time. The steps for summter time configuration are as follows:

Step	Command	Description
1	**clock summer-time enable**	Enable the summer time function.

		This function can also be shutdown if you do not need it
2	**clock summer-time recurring {**<1-4>| last**} {** sun | mon | tue | wed | thu | fri | sat **} {**<1-12> | MONTH **} <**0-23**> <**0-59**> {**<1-4> | last**} {** sun | mon | tue | wed | thu | fri | sat **} {**<1-12> | MONTH **} <**0-23**> <**0-59**> <**1-1440**>**	starting time and ending time for summber time ·**<1-4>** which week to begin the summber time in the month ·**last** the summber time begins from the last week in the month ·***week day*** which day to begin summer time in the week (Sunday: sun, Saturday: sat) ·**<1-12>** summer time starting month ·**MONTH** summer time starting month, input English word ·**<0-23>** summer time starting hour ·**<0-59>** summber time starting minute ·**<1-4>** which week to end the summer time in the month ·**last** summer time ends at the last week in the month ·***week day*** which day to end summer time in the week(Sunday: sun, Saturday: sat) ·**<1-12>** summer time ending month ·**MONTH** summer time ending month, input English words ·**<0-23>** summer time ending hour ·**<0-59>** summer time ending minute ·**<1-1440>** summer time offset minutes

3	**show clock summer-time recurring**	Show summer time configuration

For example, set the summer time as: starts at 2 0’clock in the morning in April of every year, ends at 2 o’clock in the morning in September. The time should be switched one hour faster within this period.

Raisecom#clock summer-time enable

set sucessfully!

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

set sucessfully!

Raisecom#show clock summer-time-recurring

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

Timezone offset: +08:00:00
Summer time recuuring: Enable
Summer time start: week 02 Sunday Apr 02:00
Summer time end: week 02 Sunday Sep 02:00
Summer time Offset: 60 min

Chapter 23 Loopback Detection

23.1 Loopback detection introduction

Loopback detection is to solve the network problem due to Loop (inner loop and outer loop), so as to enhance the network self-diagnostic capability, fault compatibility and robustness.

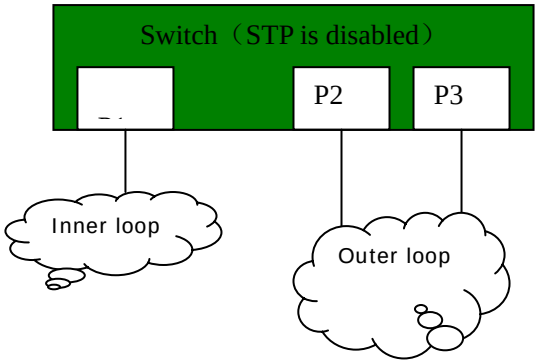


图 1

The loop discovery process:

1. Each port of the switch sends Loopback-detection packet periodically (the interval is configurable, generally as 4 seconds)
2. Switch will check the CUP MAC section of received packet, if the CPU MAC section has the same MAC as the switch, loop exsits on certain ports; otherwise, packet will be dropped;
3. If the port series number which sends out packed is the same with the port number which receives packets, self loopback exists; otherwise, outer loop exists;
4. When loop exists, port with bigger series number will be shutdown;

23.2 Loopback detection configuration

Configuration includes two parts:

- Loopback detection enable/disable;
- Loopback detection period configuration;

Loopback detection enable/disable configuration

Command	Description
config	Enter global configuration mode
loopback-detection { *enable* | *disable* **} port-list {** *port-list* | all **}**	Enable/disable loopback detection for port. Default status is enabled *enable*， enable the loopback detection； *disable*，disable the loopback detection；； *port-list is port series number, ranged 1-26, use "," and "-" for multiple ports input*; *all*, all the ports;
exit	Back to privileged EXEC mode
show loopback-detection	Show loopback detection status

Loopback detection period configuration

Command	Description
config	Enter global configuration mode
loopback-detection hello-time <1-65535>	Loopback detection interval configuration. 1-65535， parcket sending interval, unit is second, 4 seconds for default;
exit	Back to privileged EXEC mode
show loopback-detection	Show loopback detection status

You can use the command no loopback-detection hello-time for default configuration

Use show loopback-detection for showing the port loopback detection status.

For example: set the loopback detection period as 3 seconds. Enable all the loopback detecton function. Port 2 and port 6 construct a outer loop, port 9 constructs a self-loopback. STP function is disabled.

Raisecom# **config**

Raisecom(config)# **loopback-detection hello-time** 3

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

Raisecom(config)# **exit**

Raisecom# show loopback-detection

Period of loopback-detection: 3 s

VLAN: 1

Destination address: FFFF.FFFF.FFFF

Port	Detection State	Loop Flag	State/Time	Source Port
1	enable	no	--/infin	--
2	enable	no	--/infin	--
3	enable	no	--/infin	--
4	enable	no	--/infin	--
5	enable	no	--/infin	--
6	enable	yes	--/infin	2
7	enable	no	--/infin	--
8	enable	no	--/infin	--
9	enable	yes	--/infin	9
10	enable	no	--/infin	--

……

Chapter 24 Task Schedule Configuration

Task schedule function can realize periodical implementation for certain task and term maintenance. You can configure a list with time property, this list includes a starting time, a periodic time and an ending time. There are two sorts of time properties, one is that the task is timed from the startup of the switch, which is a relative time; the other one is that the switch is timed according to the strandard time regarding hour, minute, second, year, month and day, which is an absolute time.

This chapter includes the following parts:

1. Task schedule time list setting
2. Task schedule configuration based on command line

24.1 Task schedule time list configuration

Command	Description
schedule-list *list-no* **start** { **up-time** *days time* [**every** *days time* [**stop** *days time*]] | **date-time** *date time* [**every** { **day** | **week** | *days time* } [**stop** *date time*]]}	Add or modify schedule-list term, this command is for setting the starting time, ending time, and periodical interval for the task. You can use “no”to delete a schedule list *list-no* ：schedule list number, range is <0-99>； **up-time** ：start from the switch startup time, which is a relative time; **date-time** ：start according to the system time which is a absolute time; *days time* ：a time period, format input, days: <0-65535>，time: HH:MM:SS, such as 3 3:2:1 *date time* ：a time point, format input is MMM-DD-YYYY HH:MM:SS, such as jan-1-2003 or 1-1-2003，rang of YYYY is from 1970 to 2199
show schedule-list	Show the schedule-list configuration

24.2 task schedule configuration based on command line

Command	Description
config	Enter global configuration mode
command-string **schedule-list** *list-no*	Add tasks into schedule-list
show schedule-list	Show schedule-list configuration

Chapter 25 Malfunction Located

25.1 Malfunction location

When switch has malfunctions or works abnormally, you can view the running information for locating the malfunction. The viewed contents include:

- ✧ memory using status;
- ✧ port drive pool using status
- ✧ process and its stacking status
- ✧ port UP/DOWN statistical information;
- ✧ Information accumulation for locating malfunction

25.1.1 Memory using status

Step	Command	Description
1	**show memory**	View the memery using status

Example:

Raisecom#show memory

FREE LIST:

num	addr	size
1	0x27db148	9120
2	0x3483100	16904
3	0x27ddd50	160
4	0x916220	32017512
5	0x3e00000	2077144

SUMMARY:

status	bytes	blocks	avg block	max block
current				
free	34120840	5	6824168	32017512

alloc 23460160 62554 375 -

cumulative

alloc 23591248 64754 364 -

25.1.2 Port drive pool using status

Step	Command	Description
1	**show buffer [port** <1-26>**]**	View port drive pool using status

Example:

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

Port 2

Total mBlks: 500 Free mBlks: 500 DATA: 0

HEADER: 0 SOCKET: 0 PCB: 0

RTABLE: 0 HTABLE: 0 ATABLE: 0

SONAME: 0 ZOMBIE: 0 SOOPTS: 0

FTABLE: 0 RIGHTS: 0 IFADDR: 0

CONTROL: 0 OOBDATA: 0 IPMOPTS: 0

IPMADDR: 0 IFMADDR: 0 MRTABLE: 0

25.1.3 Process and its stacking status

Step	Command	Description
1	**show processes**	View the process and its stacking status

Example:

Raisecom#**show processes**

Task Information :

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

Task STATUS: RDY- ready ; SUP- suspended; POS-pend on sem;
TSD- task delay;DTS-dead task

taskid	task Name	stk(B)	prio	status	Ecode	Rtime(sws /ticks%)
3bfe9e0	tExcTask	7744	0	POS	3d0001	(0 / 0.0%)
3bfc058	tLogTask	4760	0	POS	0	(0 / 0.0%)
348bd78	tWdbTask	7656	3	POS	0	(0 / 0.0%)
2c71c38	tED	8024	20	POS	3d0002	(0 / 0.0%)
6c9a38	tStpTm	2796	30	TSD	0	(0 / 0.0%)
2a055c0	tSch	8056	30	TSD	0	(0 / 0.0%)
29e5188	tRmonTm	1896	30	TSD	0	(0 / 0.0%)
2a4aa00	tStpRecv	4832	35	POS	0	(0 / 0.0%)
34e22d0	tNetTask	9792	50	POS	3d	(4 / 0.0%)
2e7d9d8	tDPC	15928	50	POS	0	(0 / 0.0%)
2e2a988	tARL.0	15928	50	POS	0	(0 / 0.0%)
2da6710	tLINK.0	15912	50		3d0004	(3 / 0.0%)
2db3bd0	tCOUNTER.0	15896	50		3d0004	(3 / 0.0%)
27d9500	tScrnBg_0	13888	50	RDY	30067	(28 / 0.0%)
27d1c78	tScrnBg_1	16192	50	POS	0	(0 / 0.0%)
27ca4e0	tScrnBg_2	16192	50	POS	0	(0 / 0.0%)
27c2d48	tScrnBg_3	16192	50	POS	0	(0 / 0.0%)
27bb5b0	tScrnBg_4	16192	50	POS	0	(0 / 0.0%)
27b3e18	tScrnBg_5	16192	50	POS	0	(0 / 0.0%)
2a6ba58	tRndpRecv	7944	51	POS	0	(0 / 0.0%)
2a632d0	tRtdpRecv	7912	51	POS	0	(1 / 0.0%)
2907680	tCcomTm	840	55	TSD	0	(2 / 0.0%)
348df68	tSntpS	4344	56	POS	0	(0 / 0.0%)
2a7c008	tDhcpS	19464	56		0	(0 / 0.0%)
2a6f480	tLoopD	3944	60	TSD	0	(10 / 0.0%)
2906408	tCcom	3848	60	POS	0	(2 / 0.0%)
2a1e7f0	tRmon	32632	75	TSD	81000c	(15 / 0.0%)
2a11358	tPortStats	3632	75	TSD	0	(6 / 0.0%)
2a0aeb8	tLinkTrap	8040	75	TSD	0	(2 / 0.0%)
2a06868	tColdTrap	3944	75	TSD	0	(1 / 0.0%)
2a23a38	tIgmpTm	2848	100	TSD	0	(0 / 0.0%)
2a22c20	tIgmpSnoop	3816	100	POS	0	(0 / 0.0%)
2a21a08	tSnmp	11816	100	POS	0	(0 / 0.0%)
2a16590	tIpBind	3904	100	TSD	81000c	(1 / 0.0%)

```
2a08b78      tEndStat      7832   100            3d0004   (      0 /   0.0%)
29e2558      tRmonAlrm     7976   100      POS          0   (      2 /   0.0%)
27aea90 tTelnetdOut0       3336   100      POS          0   (      0 /   0.0%)
27ad878   tTelnetdIn0      3384   100      POS          0   (      0 /   0.0%)
27ac610 tTelnetdOut1       3336   100      POS          0   (      0 /   0.0%)
27ab3f8   tTelnetdIn1      3384   100      POS          0   (      0 /   0.0%)
27aa190 tTelnetdOut2       3336   100      POS          0   (      0 /   0.0%)
27a8f78   tTelnetdIn2      3384   100      POS          0   (      0 /   0.0%)
27a7d10 tTelnetdOut3       3336   100      POS          0   (      0 /   0.0%)
27a6af8   tTelnetdIn3      3384   100      POS          0   (      0 /   0.0%)
27a5890 tTelnetdOut4       3336   100      POS          0   (      0 /   0.0%)
27a4678   tTelnetdIn4      3384   100      POS          0   (      0 /   0.0%)
27a3460      tTelnetd      3640   100      POS          0   (      0 /   0.0%)
3489320      tSyslog       7968   105      POS          0   (      0 /   0.0%)
2daaac8        tx_cb      15912   110      POS          0   (      0 /   0.0%)
348f558    tSntpCLsn       4760   150      TSD          0   (      1 /   0.0%)
2a52d20      tRelay        3880   151      POS          0   (      0 /   0.0%)
2da0958        rx0       15888   200            3d0004   (     29 /   0.0%)
2cc1c98    tArlAging       1896   200      TSD          0   (      0 /   0.0%)
2b38248      tSnmpTm       3856   200      POS          0   (      0 /   0.0%)
2c25d60      tRosInit      5912   250      POS    81000e   (      0 /   0.0%)
27af260        tIdle        568   251      RDY          0   (    281 /   0.0%)
```

Each column above indicates: task ID, task name, statcking size, priority, status, error code, running time and CPU usage

25.1.4 Port UP/DOWN statistical information

Step	Command	Description
1	**show diags link-flap**	View port UP/DOWN statistical information

Example:

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

This example indicates that, after the startup of the switch, port 19 UP/DONW for twice, no UP/DOWN in the latest 1 minute; port 21 UP/DOWN for twice, UP/DOWN twice in the latest 1 minute;

25.1.5 Information accumulation for locating malfunction

Step	Command	Description
1	**show tech-support**	View information accumulation for locating malfunction

This command will show the information accumulation for locating malfunction, which includes:

1. version information（show version）
2. current configuration information(show running-config)
3. current CUP utilization(show cpu-utilization)
4. memory usage information(show memory)
5. port drive pool using status(show buffer)
6. process information(show processes)
7. files in flash(dir)
8. system current time(show clock)
9. port status information(show interface port)
10. port statistical information(show interface port statistics)
11. port UP/DOWN statistical information(show diags link-flap)
12. SNMP statistical information(show snmp statistics)
13. spanning tree status(show spanning-tree)
14. static VLAN information(show vlan static)
15. ARP information(show arp)
16. trunk information(show trunk)
17. TCP link status

Chapter 26 VLAN Configuration

This chapter mainly discusses how to configure VLAN on a switch, which includes the following contents:

1. VLAN summarization;
2. VLAN configuration list;
3. Monitoring and maintenance;

26.1 VLAN summarization

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:

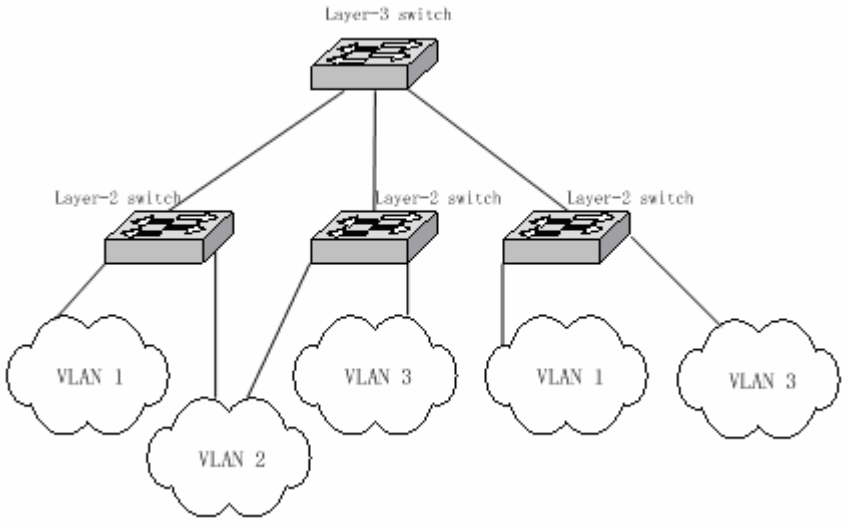


Figure 9-1 VLAN topology

In practical network application, VLAN always corresponds to a specified IP subnet, as in figure 9-1 above, VLAN 1 may correspond to network 10.0.0.0/24, VLAN 2 may corresponds to network

20.0.0.0/24, though they are isolated on layer 2, they can realize communication via Layer-3 switch.

26.2 VLAN member port mode

Port member mode	**VLAN member attributes**
Access	Under this mode, the port can be allocated to a single VLAN, packet sent from Access port does not have no 802.1Q tag, Access ports within different VLANs cannot communicate with each other.
Hybrid	Under this mode, the port can be allocated to multiple VLANs, you can also determine if packet sent out from Hybrid port carries related 802.1Q tag or not. Meanwhile, you can also classify the non-802.1Q packets that enter the port into different VLANs by setting the Native attribute of the port.
Trunk	Trunk port can be allocated with different VLANs by default, packet forwarded from it carries 802.1Q tag expect for Native VLAN. However, you can limit the packets through which VLAN they are forwarded by using *allowed vlans*

26.3 VLAN configuration list

Configuration for VLAN includes:

- ✧ VLAN creation and deletion
- ✧ VLAN name setting
- ✧ VLAN status configuration
- ✧ Port VLAN mode and the relative attributes configuration
- ✧ Monitoring and maintenance

26.3.1 VLAN creation and deletion

Under default situation, two VLANs exist, which are default VLAN (VLAN 1) and cluster VLAN (VLAN 2), all ports are Access mode and belong to the default VLAN. The default VLAN cannot be deleted. When you want to create a new VLAN, the steps below need to be followed:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**vlan** <*3-4094*>	Create new VLAN and enter the associated configuration mode
3	**exit**	Back to global configuration mode
4	**exit**	Back to privileged EXEC MODE
4	**show vlan**	Show the VLAN configuration status

The status of newly-created VLAN is suspended, if you want it to take effect, you still need to use the command *state*.

If you want to delete a VLAN, you should follow the steps below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**no vlan** <*3-4094*>	Deleting VLAN
3	**exit**	Back to global configuration mode
4	**show vlan**	Show the VLAN configuration status

The example below show how to create VLAN 3, and view the configuration status by using command *show*

Raisecom#(config)**#vlan** *3*
Raisecom#(config-vlan)**#exit**
Raisecom#(config)**#exit**
Raisecom**#show vlan**

VLAN	Name	Status	Ports
1	Default	active	1-26
2	Cluster-Vlan	active	n/a
3	VLAN0003	suspend	n/a

26.3.2 VLAN name setting

You can set the VLAN name for managing the users conveniently. By default, the name of default VLAN (VLAN 1) is “default”, “Cluster-Vlan” for the cluster VLAN (VLAN 2), and string “VLAN” appended with 4-bit digitals for the names of other VLANs. For example, the default name for VLAN 1

is “VLAN0001”, “VLAN4096” for VLAN 4096. The configuration is as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**vlan** <*3-4094*>	Enter the corresponding VLAN configuration mode
3	**Name** *WORD*	Nominating VLAN
4	**Exit**	Back to global configuration mode
5	**Exit**	Back to privileged EXEC mode
6	**show vlan**	Show VLAN configuration status

The example below nominates VLAN 2 as “Raisecom”

Raisecom#config

Raisecom#(config)#**vlan** *2*

Raisecom#(config-vlan)# **name** *Raisecom*

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

Raisecom#(config)# **exit**

Raisecom#**show vlan**

VLAN Name Status Ports

---- ---------- ------- ----------

1 Default active 1-26

2 raisecom active n/a

3 VLAN0003 suspend n/a

26.3.3 VLAN status configuration

All VLAN settings will not take effect until being activated. When VLAN status is suspend, you can still configure it, such as delete/add port, VLAN name and so on. Switch will save these configurations. Once the VLAN is active, these configurations will take effects. VLAN status configuration is as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**vlan** <*3-4094*>	Enter the corresponding VLAN configuration mode
3	**state** {**active	suspend**}	Set VLAN status
4	**exit**	Back to global configuration mode

5	**exit**	Back to privileged EXEC mode
6	**show vlan**	Show VLAN configuration status

The example below show how to activate VLAN 2:

Raisecom#config

Raisecom#(config)#**vlan** *2*

Raisecom#(config-vlan)# **state active**

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

Raisecom#(config)# **exit**

Raisecom#**show vlan**

VLAN	Name	Status	Ports
----	----------	-------	----------
1	Default	active	1-26
2	Cluster-Vlan	active	n/a
3	Raisecom	active	n/a

26.3.4 Port VLAN mode and the relative attributes configuration

VLAN mode for the port should be configured under the physical port configuration mode, the steps are as follows:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface port** <1-26>	Enter the corresponding physical port configuration mode
3	**switchport mode {access | hybrid | trunk }**	Set VLAN mode for the port
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show interface port** [{*1-26*}] **swithport**	Show port VLAN attributes configurations

Configure port VLAN mode as the default Access mode, the steps are as follows:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**interface port** <*1-26*>	Enter the corresponding physical port configuration mode
3	**no switchport mode {access | hybrid | trunk }**	Configure the port VLAN mode as default mode
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show vlan**	Show the port VLAN attributes configuration

The example below shows how to configure physical port 2 as Trunk mode:

Raisecom#**config**
Raisecom#(config)#**interface port** *2*
Raisecom#(config-port)# **switchport mode trunk**
Raisecom#(config-port)# **exit**
Raisecom#(config)# **exit**

Raisecom#show interface port *2* switchport

Port 2:
Administrative Mode: trunk
Operational Mode: trunk
Access Mode VLAN: 1(default)
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: 1-3
Administrative Hybrid Allowed VLANs: 1-4094
Operational Hybrid Allowed VLANs: n/a
Administrative Hybrid Untagged VLANs: n/a
Operational Hybrid Untagged VLANs: n/a
Native Mode VLAN: 1(default)

Configure Access VLAN for the Access、Extend-access、Tunnel ports, the steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <1-26>	Enter the corresponding physical port configuration mode
3	**switchport access vlan** <*1-4094*>	Configure the Access VLAN for the port

4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show interface port** [{*1-26*}] **switchport**	Show the port VLAN attributes configuration

Configure the Access VLAN as default VLAN 1, the steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <*1-26*>	Enter the corresponding physical port configuration mode
3	**no switchport access vlan**	Delete the port Access VLAN
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show interface port** [{*1-26*}] **switchport**	Show the port VLAN attributes configuration

The example below shows how to set the Access VLAN as 4096 for physical port 24:

Raisecom#config

Raisecom#(config)#**interface port** *24*
Raisecom#(config-port)# **switchport access vlan** *4094*
Raisecom#(config-port)# **exit**
Raisecom#(config)# **exit**

Raisecom#show interface port *24* switchport

Port 24:
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 1(default)
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

Configure the allowed VLAN for 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	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show interface port** [{*1-26*}] **switchport**	Show the port VLAN attributes configuration

Configure the allowed VLAN for Hybrid port as 1-4096, the steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <*1-26*>	Enter the corresponding physical port configuration mode
3	**no switchport hybrid allowed vlan**	Configure the allowed VLANs to default for Hybrid port
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show interface port** [{*1-26*}] **swithport**	Show the port VLAN attributes configuration

The example below shows the allowed VLANs (VLAN 1-100) for the physical port 3 under hybrid mode:

Raisecom#config

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

Raisecom#(config-port)# **switchport hybrid allowed vlan** *1-100*

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

Raisecom#(config)# **exit**

Raisecom#show interface port *3* switchport

Port 3:
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 1(default)
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: n/a
Administrative Hybrid Allowed VLANs: 1-100
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

Configure the allowed untagged VLAN for hybrid port:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <1-26>	Enter the corresponding physical port configuration mode
3	switchport hybrid untagged vlan { all | *vlan-list* | add *add-vlan-list* | remove *remove-vlan-list*}	Configure the allowed untagged VLAN for 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	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show interface port** [{*1-26*}] **swithport**	Show the port VLAN attributes configuration

Configure the allowed Untagged VLANs for Hybrid port as 1-4094:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <*1-26*>	Enter the corresponding physical port configuration mode
3	**no switchport hybrid untagged vlan**	Configure the allowed untagged VLAN for hybrid port
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show interface port** [{*1-26*}] **swithport**	Show the port VLAN attributes configuration

The example below show how to configure the allowed Untagged VLAN as 3-100 for physical port 3 under the Hybrid mode:

Raisecom#config

Raisecom#(config)**#interface port** *3*
Raisecom#(config-port)**# switchport hybrid untagged vlan** *3-100*
Raisecom#(config-port)**# exit**
Raisecom#(config)**# exit**

Raisecom#show interface port *3* switchport

Port 3:
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 1(default)
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: n/a
Administrative Hybrid Allowed VLANs: 1-100
Operational Hybrid Allowed VLANs: n/a
Administrative Hybrid Untagged VLANs: 1,3-100
Operational Hybrid Untagged VLANs: n/a
Native Mode VLAN: 1(default)
VLAN Ingress Filtering: Enabled

Configure the allowed VLAN for trunk port:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**interface port** <1-26>	Enter the 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 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: remove vlan base on the existent vlan
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show interface port** [{*1-26*}] **switchport**	Show the port VLAN attributes configuration

Configure the allowed VLAN as 1-4094 for trunk port:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <*1-26*>	Enter the corresponding physical port configuration mode
3	**no switchport trunk allowed vlan**	Configure the allowed VLAN as 1-4094 for trunk port
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show interface port** [{*1-26*}] **switchport**	Show the port VLAN attributes configuration

The example below shows how to configure the allowed VLAN as 1-100 for physical port 3 under trunk mode:

Raisecom#config

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

Raisecom#(config-port)# **switchport trunk allowed vlan** *1-100*

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

Raisecom#(config)# **exit**

Raisecom#show interface port *3* switchport

Port 3:

Administrative Mode: access

Operational Mode: access

Access Mode VLAN: 1(default)

Administrative Trunk Allowed VLANs: 1-100

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-100

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1,3-100

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

Configure the Native VLAN for Trunk and Hybrid port:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <1-26>	Enter the corresponding physical port configuration mode
3	**switchport native vlan** *<1-4094>*	Configure the Native VLAN for Trunk and Hybrid port
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show interface port** [{*1-26*}] **swithport**	Show the port VLAN attributes configuration

Configure the Native VLAN for Trunk and Hybrid port as default:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** *<1-26>*	Enter the corresponding physical port configuration mode
3	**no switchport native vlan**	Configure the Native VLAN for Trunk and Hybrid port as default
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show interface port** [{*1-26*}] **swithport**	Show the port VLAN attributes configuration

The example below shows how the configure Native VLAN as VLAN 100 for the physical port 3:

Raisecom#config

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

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

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

Raisecom#(config)# **exit**

Raisecom#show interface port *3* switchport

Port 3:
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 1(default)
Administrative Trunk Allowed VLANs: 1-100
Operational Trunk Allowed VLANs: n/a
Administrative Hybrid Allowed VLANs: 1-100
Operational Hybrid Allowed VLANs: n/a
Administrative Hybrid Untagged VLANs: 1,3-100
Operational Hybrid Untagged VLANs: n/a
Native Mode VLAN: 100
VLAN Ingress Filtering: Enabled

26.3.5 Monitoring and maintenance

You can use two “show” commands to check the VLAN and relative configurations to realized VLAN monitoring and maintenance:

Command	Description
show vlan [{*1-4094*}]	Show VLAN configurations
show interface port [{*1-26*}] **swithport**	Show the VLAN relative configuration for physical port

You can use *show vlan* to view the VLANs that are created by using CLI or SNMP manner, including the current active and suspended VLANs:

Raisecom#**show vlan**

VLAN	Name	Status	Ports
1	Default	active	1-26
2	Cluster-Vlan	active	n/a

You can use ***show interface port*** *[{1-26}]* ***swithport*** to view the port VLAN attributes configured by using CLI or SNMP:

Raisecom#show interface port 24 switchport

Port 3:
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 1(default)
Administrative Trunk Allowed VLANs: 1-100
Operational Trunk Allowed VLANs: n/a
Administrative Hybrid Allowed VLANs: 1-100
Operational Hybrid Allowed VLANs: n/a
Administrative Hybrid Untagged VLANs: 1,3-100
Operational Hybrid Untagged VLANs: n/a
Native Mode VLAN: 100
VLAN Ingress Filtering: Enabled

Chapter 27 Interface Statistics

27.1 Port statistics introduction

The configurations introduced in this chapter are only for ISCOM2026 switch.

ISCOM2026 switch supports packet statistics based on port. You can configure the statistical packet type by using command lines. You can configure the packet types on the ingress of a specified port which include: ingress good packet, ingress bad packet, ingress local packet, default statistical ingress packet; you can also configure the packet types on the egress of a specified port which included: ingress good packet, egress bad packet, dropped packet, and default statistical egress packet:

27.2 Interface statistics configuration

Statistics configuration of packet type on specified port

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <1-26>	Enter Ethernet interface configuration mode
3	**statistic packet ingress {good |bad |local} egress {good |bad |abort}**	Configure the packet statistic type
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show interface port [<1-26>] statistics**	Show interface statistics information

The example below shows how to statistic egress bad packets and ingress bad packets:

```
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)#statistic packet ingress bad egress bad
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show interface port 2 statistics
```

27.3 Monitoring and maintenance

You can use command *show* to view the packet statistical information on the port:

Command	Description
show interface port [{*1-26*}] **statistics**	Show physical port packet statistical information

Example:

Statistic the egress bad packets and ingress bad packets on port 2, show the packet statistical information on port 2:

```
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)#statistic packet ingress bad egress good
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show interface port 2 statistics
  Statistics for the interface of switch:
  port No.          number of recv-pkts          number of send-pkts
  ------------------------------------------------------------------------------------
  2                 9(bad-pkt )                  78 (good-pkt )
```

Chapter 28 ACL and Network Security Configuration

28.1 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.

28.2 ACL configuration

Relevant configurations include:

1、MAC access control list configuration

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.

Command	Description
config	Enter global configuration mode
mac-access-list *list-number* {**deny** | **permit**} [*protocol* | **any**] {*source-MAC-address* **| any**} {*destination-MAC-address* | **any**}	MAC access control list configuration *list-number* access control list series number, range 0-399. **deny|permit** indicates deny/permit access [*protocol* | **any**] indicates bonded protocol type, **any** indicates unrestricted protocol type.

	source-MAC-address 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. *destination-MAC-address* 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.
exit	Exit global configuration mode and enter privileged EXEC mode
show mac-access-list *list-number*	Show MAC access control list *list-number* is the series number for the MAC access control list to be shown, rang is 0-399.
no mac-access-list *list-number*	Delete configured MAC access control list *list-number* is the list series number to be deleted

Example：Configure the source MAC address as 1234.1234.1234, destination MAC address as 5678.5678.5678, protocol as IP, access type as deny. Configure the source MAC address as 1111.2222.3333, destination MAC address as 4444.5555.6666, protocol as ARP, access type as permit.

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

2、IP access control list 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.

Command	Description
config	Enter global configuration mode
ip-access-list *list-number* {**deny** | **permit**} *protocol* {*source-address mask* | **any**} [*source-protocol-port*] {*destination-address mask* | **any**}	**ip-access-list** set IP address control list. *list-number* list series number for IP address control list, range is 0-399 **deny|permit** indicates deny/permit access

[*destination-protocol-port*]	*protocol* indicates bonded protocol type *source-address mask* | **any** is source IP address with its mask, format is dotted decimal in the form of A.B.C.D, **any** indicates arbitrary address. *source-protocol-port* is source port for TCP/UDP protocol *destination -address mask* | **any** is the destination address and its mask, the format is dotted decimal as A.B.C.D; **any** indicates arbitrary address. *destination -protocol-port* is the destination port of TCP/UPD.
exit	Exit global configuration mode and enter privileged EXEC mode
show ip-access-list *list-number*	Show IP access control list relevant information *list-number* is the series number for the IP access control list to be shown, rang is 0-399.
no ip-access-list *list-number*	Delete IP access control list *list-number* is the list series number to be deleted

Example: configure the source IP address as in 192.168.1.0 network segment, destination IP address as arbitrary address, protocol as IP, access type as deny. Configure the source IP address as 10.168.1.19, mask as 255.255.255.255, source protocol port as 80, destination IP address as arbitrary, protocol as TCP, access type as deny. Configure the source IP address as 10.168.1.19, mask as 255.255.255.255, destination address as segment 10.168.0.0, protocol as TCP, and access type as permit. .

raisecom#config

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

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

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

raisecom(config)#exit

raisecom#show ip-access-list

Src Ip: Source Ip Address

Dest Ip: Destination Ip Address

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

3、Access list map configuration

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. Note that: **Rules should be even hexadecimal, offset includes segment of 802.1Q VLAN TAG even if what the switch receives is untagged packet.**

Command	Description
config	Enter global configuration mode
access-list-map *list-number* {**deny** | **permit**}	*list-number*：list series number, rang is 0-399 **deny|permit** deny or permit data packets to go through when matching
match mac {destination|source} *HHHH.HHHH.HHHH*	**destination|source** match source mac address or destination address

	HHHH.HHHH.HHHH mac address
match cos <0-7>	<0-7> match cos
match ethertype *HHHH [HHHH]*	*HHHH[HHHH]* match Ethernet type [mask]
match {arp | eapol | flowcontrol | ip | ipv6 | loopback | mpls | mpls-mcast | pppoe | pppoedisc | x25 | x75}	**arp**——match ARP protocol **eapol**——match eapol protocol **flowcontrol**——match flowctrol protocol **ip**——match ip protocol **ipv6**——match ipv6 protocol **loopback**——match loopback protocol **mpls**——match mpls singlecast protocol **mpls-mcast**——match mpls multicast protocol **pppoe**——match pppoe protocol **pppoedisc**——match pppoe discovery protocol **x25**——match x25 protocol **x75**——match x75 protocl
no match mac {destination|source}	Donot match MAC address **destination|source** match source mac or destination mac
no match cos	Donot match cos
no match ethertype	Donot match Ethernet frame type
match arp opcode {request | reply}	Match arp protocol type **request | reply** arp protocol request/reply packet
match arp {sender-mac| target-mac} *HHHH.HHHH.HHHH*	Match arp protocol hardware address **sender-mac| target-mac** match arp sender/target mac address *HHHH.HHHH.HHHH* MAC address
match arp {sender-ip| target-ip} *A.B.C.D [A.B.C.D]*	Match arp protocol IP address **sender-ip| target-ip** sender/target ip address *A.B.C.D [A.B.C.D]* IP address [mask]
no match arp opcode	Donot match arp protocol type
no match arp {sender-mac| target-mac}	Donot match arp hardware address **sender-mac| target-mac** match arp sender/target mac address
no match arp {sender-ip| target-ip}	Donot match arp protocol IP address **sender-ip| target-ip** sender/target IP address
match ip {destination-address | source-address} *A.B.C.D [A.B.C.D]*	Match IP protocol address **destination-address | source-address** IP protocol destination/source address *A.B.C.D [A.B.C.D]* IP address [mask]
match ip precedence {<0-7> **| routine| priority| immediate| flash| flash-override | critical | internet | network}**	Match IP precedence <0-7>—— IP precedence **routine**—— IP precedence 0 **priority**—— IP precedence 1

	immediate—— IP precedence 2 **flash**—— IP precedence 3 **flash-override**—— IP precedence 4 **critical**—— IP precedence 5 **internet**—— IP precedence 6 **network**—— IP precedence 7
match ip tos {<0-15> **| normal | min-monetary-cost | min-delay | max-reliability | max-throughput}**	Match IP precedence ToS <0-15>——TOS value **normal**——normal TOS value (0) **min-monetary-cost**——minimum monetary cost TOS value（1） **min-delay**——minimum delay TOS value（8） **max-reliability**——maximum reliability TOS value（2） **max-throughput**——maximum throughput TOS value（4）
match ip dscp {<0-63> **| af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41| af42 |af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | default}**	Match IP dscp value <0-63>——ip dscp value **af11**——AF11 dscp value（001010） **af12**——AF12 dscp value（001100） **af13**——AF13 dscp value（001110） **af21**——AF21 dscp value（010010） **af22**——AF22 dscp value（010100） **af23**——AF23 dscp value（010110） **af31**——AF31 dscp value（011010） **af32**——AF32 dscp value（011100） **af33**——AF33 dscp value（011110） **af41**——AF41 dscp value（100010） **af42**——AF42 dscp value（100100） **af43**——AF43 dscp value（100110） **cs1**——CS1(precedence 1) dscp value（001000） **cs2**——CS2(precedence 2) dscp value（010000） **cs3**——CS3(precedence 3) dscp value（011000） **cs4**——CS4(precedence 4) dscp value（100000） **cs5**——CS5(precedence 5) dscp value（101000） **cs6**——CS6(precedence 6) dscp value（110000） **cs7**——CS7(precedence 7) dscp value（111000） **default**——default dscp value（000000） **ef**——EF dscp value（101110）
match ip no-fragments	Match no-fragment ip packet
match ip protocol <0-255>	Match ip protocol value

	<0-255>——IP protocol type value
**match ip { ahp	esp	gre	icmp	igmp	igrp	ipinip	ospf	pcp	pim	tcp	udp}**	Match ip protocol value **ahp**——authorization header protocol **esp**——Encapsulation Security Payload **gre**——Generic Routing Encapsulation **icmp**——Internet Control Message Protocol **igmp**——Internet Group Message Protocol **igrp**——Interior Gateway Routing Protocol **ipinip**——IP in IP tunneling **ospf**——Open Shortest Path First routing **pcp**——Payload Compression Protoco **pim**——Protocol Independent Multicast **tcp**——Transmission Control Protocol **udp**——User Datagram Protocol
**no match ip {destination-address	source-address}**	Donot match IP protocol address **destination-address	source-address** IP protocol destination/source address
no match ip precedence	Donot match IP precedence
no match ip tos	Donot match IP ToS value
no match ip dscp	Donot match IP dscp value
no match ip no-fragments	Donot match IP no-fragments
no match ip protocol	Donot match IP protocol value
**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 **destination-port	source-port** TCP protocol destination/source port <0-65535>——tcp port number **bgp**——Border Gateway Protocol（179） **domain**——Domain Name Service protocol（53） **echo**——echo protocol（7） **exec**——Exec (rsh, 512) **finger**——Finger (79) **ftp**——File Transfer Protocol（21） **ftp-data**——FTP data connections（20） **gopher**——Gopher (70) **hostname**——NIC hostname server (101) **ident**——Ident Protocol (113) **irc**——Internet Relay Chat protocol (194) **klogin**——Kerberos login (543) **kshell**——Kerberos shell (544) **login**——Login (rlogin, 513) **lpd**——Printer service (515) **nntp**——Network News Transport Protocol **pim-auto-rp**——PIM Auto-RP (496)

	pop2——Post Office Protocol v2 (109) **pop3**——Post Office Protocol v3 (110) **smtp**——Simple Mail Transport Protocol (25) **sunrpc**——Sun Remote Procedure Call (111) **syslog**——system log (514) **tacacs**——TAC Access Control System (49) **talk**——Talk (517) **telnet**——Telnet (23) **time**——Time (37) **uucp**——Unix-to-Unix copy program(540) **whois**——Nicname(43) **www**——*world wide* web (HTTP, 80)
match ip tcp {ack | fin | psh | rst | syn | urg }	Match TCP protocol bit **ack**——match on ACK bit **fin**——match on FIN bit **psh**——match on PSH bit **rst**——match on RST bit **syn**——match on SYN bit **urg**——match on URG bit
no match ip tcp { destination-port | source-port}	Donot match Tcp protocol port number **destination-port | source-port** TCP protocol destination/source port
no match ip tcp {ack | fin | psh | rst | syn | urg }	Donot match TCP protocol bit **ack**——match on ACK bit **fin**——match on FIN bit **psh**——match on PSH bit **rst**——match on RST bit **syn**——match on SYN bit **urg**——match on URG bit
match ip udp { destination-port | source-port } {<0-65535> **| biff | bootpc | bootps | domain | echo | mobile-ip | netbios-dgm | netbios-ns | netbios-ss | ntp | pim-auto-rp | rip | snmp | snmptrap | sunrpc | syslog | tacacs | talk | tftp | time | who }**	Match udp protocol port number **destination-port | source-port** TCP protocol destination/source port **<**0-65535>——udp port number **biff**——Biff (mail notification, comsat, 512) **bootpc**——Bootstrap Protocol (BOOTP) client（68） **bootps**——Bootstrap Protocol (BOOTP) server（67） **domain**——Domain Name Service（53） **echo**——echo protocol（7） **mobile-ip**——Mobile IP registration (434) **netbios-dgm**——NetBios datagram service（138） **netbios-ns**——NetBios name service（137）

	netbios-ss——NetBios session service（139） **ntp**——Network Time Protocol (123) **pim-auto-rp**——PIM Auto-RP (496) **rip**——Routing Information Protocol (520) **snmp**——Simple Network Management Protocol (161) **snmptrap**——SNMP Traps (162) **sunrpc**——Sun Remote Procedure Call (111) **syslog**——system log (514) **tacacs**——TAC Access Control System (49) **talk**——Talk (517) **tftp**——Trivial File Transfer Protocol 69) **time**——Time (37) **who**——Who service (rwho, 513)
no match ip udp { destination-port | source-port}	Donot match udp protocol port number **destination-port | source-port** TCP protocol destination/source port
match ip icmp <0-255> [<0-255>]	match icmp protocol information type <0-255> [<0-255>] information type [information code]
match ip igmp {<0-255> **| dvmrp | query | leave-v2 | report-v1 | report-v2 |report-v3 | pim-v1 }**	Match igmp protocol information type <0-255>——IGMP information type **dvmrp**——Distance Vector Multicast Routing Protocol **leave-v2**——IGMPv2 Leave Group **pim-v1**——Protocol Independent Multicast version 1 **query**——IGMP member query **report-v1**——IGMPv1 member report **report-v2**——IGMPv2 member report **report-v3**——IGMPv3 member report
match user-define *rule-string rule-mask* <0-64>	Match user-defined segment *rule-string:* user-defined regular string, must be combined of hexadecimal, no more than 64 bytes. *rule-mask*：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
no match user-define	Donot match user-defined segment
exit	Exit global configuration mode and enter privileged EXEC mode
show access-list-map [*list-number*]	Show port access-list-map *list-number* is the port access-list-map series number to show, range is 0-399

no access-list-map *list-number*	Delete user-defined access-list-map *list-number* is the list number to delete

Example:

To filter bytes 123456 from the 40th bytes in the data frame, access type is “deny”. ARP protocol request packet is filtered.

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

28.3 Using ACL on Layer-2 physical port or VLAN

Steps for using ACL on Layer-2 physical port or VLAN are as follows:

一、 Define ACL

Described in the previous section.

二、 Set the 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.

Filtering rules on a physical port or VLAN 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.

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.

1、Based on switch

Command	Description
config	Enter global configuration mode
[no] filter (**ip-access-list | mac-access-list | access-list-map**) {*acllist* | **all**}	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 *acllist* | **all** access control list series number, **all** means all the configured access control lists
exit	Exit global configuration mode and enter privileged EXEC mode
show filter	Show all filter status

2、Based on port

Command	Description
config	Enter global configuration mode
[no] filter (**ip-access-list | mac-access-list | access-list-map**) {*acllist* | **all**} {**ingress | egress** } **port-list** {*portlist* }	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* Phsical port list range
exit	Exit global configuration mode and enter privileged EXEC mode
show filter	Show all filter status

3、Based from ingress port to egress port

Command	Description
config	Enter global configuration mode
[no] filter (ip-access-list | mac-access-list | access-list-map) {**all**| *acllist*} **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 *acllist* | **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
exit	Exit global configuration mode and enter privileged EXEC mode
show filter	Show all filter status

4、Based on VLAN

Command	Description
config	Enter global configuration mode
[no] filter (ip-access-list | mac-access-list | access-list-map) {**all**| *acllist*} **vlan** *vlanid*	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
exit	Exit global configuration mode and enter privileged EXEC mode
show filter	Show all filter status

三、Activating filter

This command is to enable or to disable the related access control lists. The default situation is “disable”. All filtering rules including those previously configured and being configured after that will take effect as soon as the command is configured successfully.

Command	Description
config	Enter global configuration mode
filter (enable | disable)	**enable** filter function is enabled **disable** filter function is disabled
exit	Exit global configuration mode and enter privileged EXEC mode
show filter	Show all filter status

Example:

1. The switch does not allow TCP packet to pass through with destination port 80

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

2. The switch does not allow ARP packets with the MAC address 000e.3842.34ea to pass through on port 2 to 8.

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
3. The switch allows IP packets with the source address in network segment 10.0.0.0/8 to pass through in VLAN 3.
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

28.4 Using ACL on Layer-3 interface

The steps below show how to use ACL on Layer-3 interface:

- ✧ Define access control list

As described in chapter 28.2.

- ✧ 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.

Command	Description
config	Enter global configuration mode
interface ip <0-14>	Enter Layer-3 interface configuration mode
[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
exit	Exit Ethernet Layer-3 interface configuration mode and enter global configuration mode
exit	Exit global configuration mode and enter privileged EXEC mode

show ip-access-list	**interface**	**ip**	Show filters status for all interfaces

Example:

1、The switch allows IP access from only 10.0.0.0/8 network segment.

raisecom#config

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

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

raisecom(config)#interface ip 0

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

raisecom(config-ip)#exit

raisecom(config)#exit

Chapter 29 QoS configuration

This chapter introduces ISCOM series switch QoS function and the configuration method. By using QoS function, user can realize traffic management, it also provide end-to-end service quality assurance for customers' business.

29.1 QoS introduction

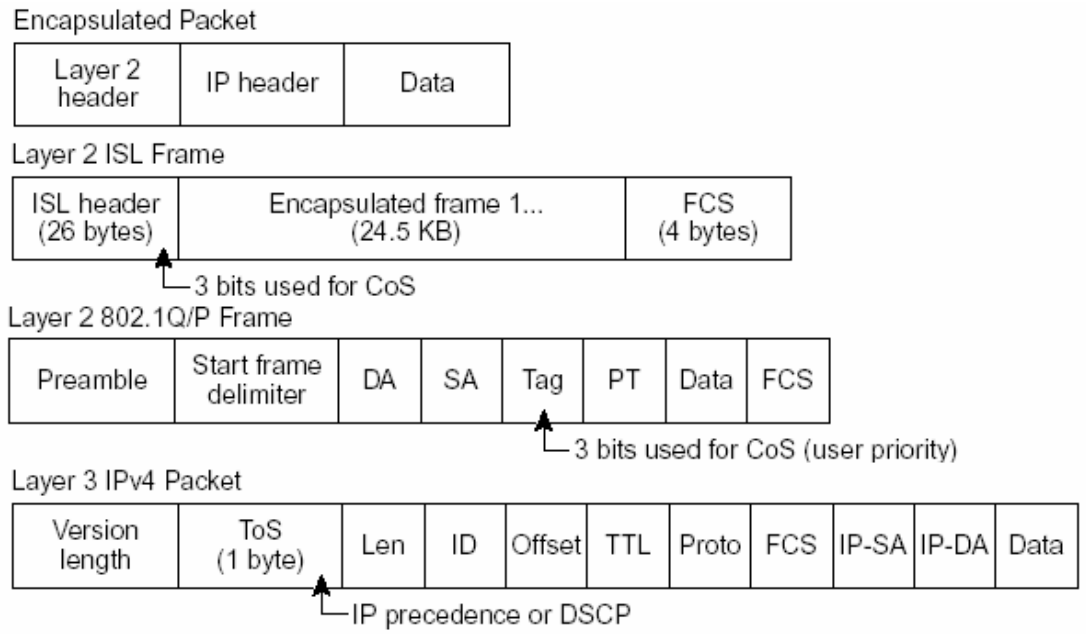
Generally speaking, Internet (Ipv4 standard) provides users only "best effort" service, cannot guarantee a real-time and complete packets transmission, and the quality of services either. Since user always has different requirements for the transmission quality of separate multi-media applications, network 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.

ISCOM2800 mechanism realizes layer-2 packets classification based on 802.1P and 802.1Q standards.

802.1Q defines VLAN, though QoS is not defined in this standard, the given mechanism which mention than the frame precedence can be modified configures a strong groundwork to realize QoS.

802.1P standard defines priority mechanism. If packets with high priority have not been transmitted, packets with low priority will not be transmitted.

In Layer-2 802.1Q frame header, there are 2 bytes of TAG control information string, the first 3 bits carry CoS (Class of Service) value, the values is from 0 to 7, shown in the figure below:



The 8 priority defined by CoS can be considered as the following 8 kinds of packets:

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

Normally level 7 is applied to important network data traffic such as routing information and so on; lever 6 or 5 is applied to interactive video and audio traffics that are sensitive to delay; level 4~1 aims at multi-media data or important enterprise-classs data information; lever 0 is applied to best-effort transmitted information by default. Therefore, user can classify output data traffic according to the CoS value, or implement relevant processings.

The figure below shows the basic module of QoS:

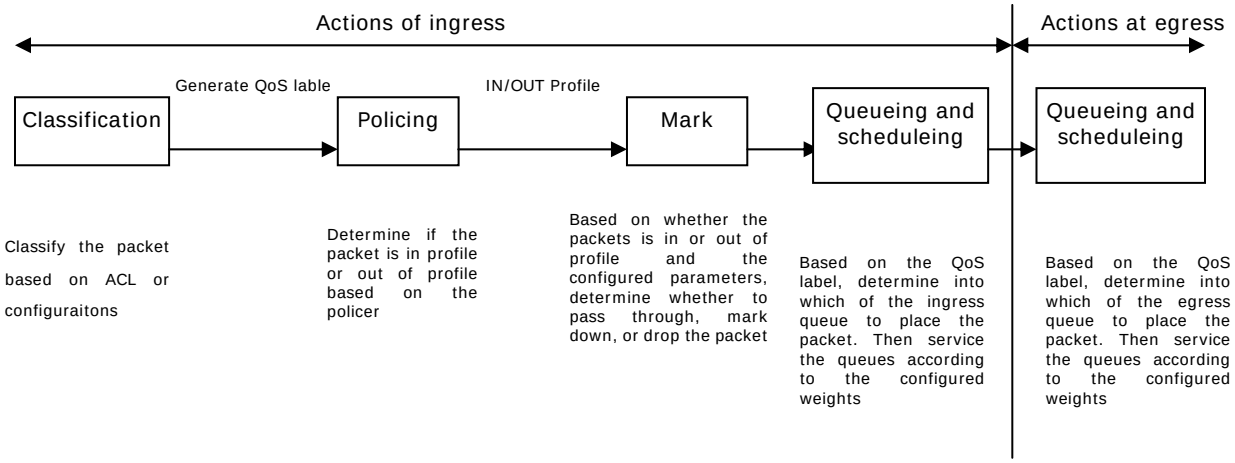
Actions at ingress include traffic classification, policing and marking.

1. Classifying: to classify the traffc. This process generates a inner DSCP to identify the data's QoS characterstics.
2. 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.
3. Marking: Evaluates the policer 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:

1、 Queueing: evaluates the QoS packet label and the corresponding DSCP before selecting which queues to use. The DSCP value is mapped to an inner COS value for the seletion of an output queue.

2、 Scheduling: based on configured WRR (Weighted round robin) and threshold to provide service for output qu



29.1.1 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. For none-IP traffic, the classification procedure is as follows:

1. 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.
2. 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.
3. 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:

1. 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.
2. Trust IP precedence of incoming packet (configure the port as trust IP precedence): use IP-precedence-to-DSCP mapping table to generate DSCP value.
3. Trust CoS value of incoming packets: use CoS-to-DSCP mapping table to generate DSCP value.
4. 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.

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.

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.

Classification based on class maps and policy maps:

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; the criteria can include matching the access group defined by the ACL or specified DSCP, IP precedence and so on.

If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. After a packet is matched against the class-map criteria, you further classify it through the use of a policy map.

A policy map specifies which traffic class to act on. Actions can include trusting CoS, DSCP or IP precedence, setting DSCP or IP precedence, specifying the traffic bandwidth limitations and the action to take when the traffic is out of profile. Before a policy map can be effective, you must attach it to an interface.

The policy map contains the features below:

1. One policy map can include multiple traffic definition;
2. Policy map trust status and port trust status are mutually exclusive, later configuration will take effects.

29.1.2 Policing and marking

You can create this type of policer:

1. individual policer

QoS applies the bandwidth limits specified in the policer separately to each matched traffic class. Since each traffic may generate multiple rules, every rule shoud use this policer.

2. shared policer

QoS applies the bandwidth limits specified in the policer separately to each matched traffic class. Since each traffic may generate multiple rules, all the traffics should use this policer, which means multiple rules share with each other.

You configure this type of policer within a policy map by using the **policy-map** configuration command

3. Aggregation policer

QoS applies the bandwidth limits defined in aggregation policer to all matched traffics. Aggregation poicy is shared by multiple traffic classifications.

Policy uses token bucket algorithm. When switch receives a frame, it will add one token to the bucket. According to specified average traffic rate (bps), every time you add one token to the bucket, the switch will check if there is enough space in the bucket. If there is no enough space, the packet will be marked as nonconforming, and policer actions will then follow (drop or mark down). In addition, burst may also trigger actions.

When configuring policing and policers, note:

1. no policers are configured by default;
2. policers can be configured on only on port, but cannot support VLAN and virtual interface;
3. on policer must be applied on only one direction;
4. policers may occur at both egress and ingress, ingress policer can be individual or aggregated;
5. Once QOS is configured on a port, all traffics received at the port will be classified, policied and marked according to policing maps.

After configuring policing map and policer actions, bond the policer to ingress or egress.

29.1.3 Mapping table

During QoS processing, switch describes the inner DSCP precedence for all traffics:

1. During the classification procedure, QOS use configured map table (CoS-to-DSCP、IP-precedence-to-DSCP), based on the COS or IP precedence value in the incoming packet to obtain an inner DSCP value; To configure DSCP trust status on port, if the DSCP values are different in the two QOS domains, use can use DSCP-to-DSCP-mutation map to modify DSCP value.
2. During the policing procedure, QOS can assign new DSCP values to IP or non-ip packets (if the packet is out of profile and the policer has indicated mark down action), this map is called policed-DSCP mapping.
3. Before traffics go into the scheduling, QOS use DSCP-to-CoS map to obtain COS value according to inner DSCP value, and then use CoS-to-egress-queue map to select the egress queueing.

CoS-to-DSCP、DSCP-to-CoS and IP-precedence-to-DSCP maps have default settings;
DSCP-to-DSCP-mutation and policed-DSCP maps are blank, the default situation is using DSCP value in the incoming packet;
DSCP-to-DSCP-mutation map is for the application on port while the other maps are for the application on the switch.

29.1.4 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 policer is effective only when the rules are configured as relying on TOS value, that is to say: modify the packet's native COS value according to TOS value.

ISCOM series switches support 4 kinds of priority output queues, the priority values are 0-3. The highest priority is level 3; the switch also supports 3 kinds of queue scheduling policies: strict priority scheduling, control forward weight scheduling and control forward delay scheduling.

ISCOM serises switches also support the processing of untagged Layer-2 frame. Every port has default priority which is COS value. When the port receives an untagged packet, the switch will consider the port default priority as the packet's COS value for queue dispatching and scheduling. After the packet goes out of the switch, it will recover to the original format.

29.2 QoS configuration list

- ✧ QoS configurations include:
- ✧ QoS enable and disable
- ✧ QoS trust status and COS default value configuration
- ✧ QoS map configuration
- ✧ QoS class configuration
- ✧ QoS policer map configuration
- ✧ QoS traffic classification configuration
- ✧ Policer application on port
- ✧ scheduling mode configuration for output queue
- ✧ monitor and maintenance

29.2.1 QOS default configuration

Attributes	Default configuration
QoS function	Disabled
Port trust status	UNTRUST
Port default COS	0
Port default DSCP	0
Port default DSCP OVERRIDE	Disable
DSCP Mutation Map	default-dscp
Queue scheduling policy	Strict priority scheduling 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

29.2.2 QOS enable and disable

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**.

Use command **show** to check if the configuration is correct:

Raisecom#show mls qos

QoS is enabled.

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.

29.2.3 Configuration for QOS trust status and default COS value

Under default situation, port trust status is UNTRUST, COS value is 0, DSCP is 0. You canconfirgure these parameters under port configuration mode:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**interface port 1**	Enter port configuration mode
3	**mls qos default-cos** *cos-value*	Default COS value configuration
4	**mls qos default-dscp** *dscp-value*	Default DSCP value configuration
5	**mls qos default-dscp override**	Enale DSCP override
6	**exit**	Back to global configuration mode
7	**exit**	Back to privileged EXEC mode
4	**show mls qos port 1**	Show QOS port configuration status

Example:

Raisecom#config

Raisecom(config)#inter port 1

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

Raisecom(config-port)#mls qos default-dscp 3

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom# show mls qos port 1

In order to check if the configurations are correct, use command **show:**

Raisecom#show mls qos port 1

port 1:

trust state: untrust

default COS: 2

default DSCP: 3

DSCP override: enable

DSCP Mutation Map: default-dscp

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

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port 1**	Enter the port configuration mode
3	**no mls qos default-cos**	Recover the default configuration of COS value as 0
4	**no mls qos default-dscp**	Recover the default configuration of DSCP value as 0
5	**no mls qos default-dscp override**	Recover the DSCP override as default configuration
6	**exit**	Back to global configuration mode

7	**exit**	Back to privileged EXEC mode
4	**show mls qos port 1**	Show QOS port configuration mode

In order to check if the configurations are correct, use command **show**:

Raisecom#show mls qos port 1

port 1:

trust state: not trusted

default COS: 0

default DSCP: 0

DSCP override: disable

DSCP Mutation Map: default-dscp

29.2.4 QoS map configuration

1、COS-DSCP map

COS-DSCP map table maps the COS value of incoming packet to a DSCP value, which is used for the QOS description of data traffic priority. The map relationship is :

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

If user wants to modify the map, you should follow the steps below:

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

Example:

Configure cos-dscp map as 2 3 4 5 6 7 8 9:

Raisecom#config

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

Raisecom(config)#exit

Raisecom# show mls qos maps cos-dscp

In order to check if the configurations are correct, use command **show:**

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

In order to recover COS-DSCP map to default setting, use command **no**:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**no mls qos map cos-dscp**	Recover to the default mapping status
3	**exit**	Back to privileged EXEC mode
4	**show mls qos maps cos-dscp**	Show COS-DSCP map

In order to check if the configurations are correct, use command **show**:

```
Raisecom#show mls qos maps cos-dscp
    Cos-dscp map:
        cos:    0   1   2   3   4   5   6   7
    ------------------------------------------------------------
       dscp:    0   8   16  24  32  40  48  56
```

2、IP-Procedence-DSCP map

IP-Procedence-DSCP map table maps the TOS value of incoming packet to a DSCP value, which is used for the description of data traffic priority. The default mapping status is:

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

If use wants to modify this mapping stauts, you should follow the steps below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mls qos map ip-prec-dscp** *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Configure new mapping status
3	**exit**	Back to privileged EXEC mode
4	**show mls qos maps ip-prec-dscp**	Show IP-Procedence-DSCP map

Example：

Configure the ip-prec-dscp map status as 2 4 6 8 10 12 14 16：

Raisecom#config

Raisecom(config)# mls qos map ip-prec-dscp 2 4 6 8 10 12 14 16

Raisecom(config)#exit

Raisecom# show mls qos maps ip-prec-dscp

In order to check if the configurations are correct, use command **show**

Raisecom#show mls qos maps ip-prec-dscp

Ip Precedence-dscp map:

ipprec: 0 1 2 3 4 5 6 7

---

dscp: 2 4 6 8 10 12 14 16

In order to recover the IP-Procedence-DSCP map to default status, use command **no**:

Step	Command	Descriptioin
1	**config**	Enter global configuration mode
2	**no mls qos map ip-prec-dscp**	Recover to the default mapping status
3	**exit**	Back to privileged EXEC mode
4	**show mls qos maps ip-prec-dscp**	Show IP-Procedence-DSCP map

In order to check if the configurations are correct, use command **show**:

Raisecom#show mls qos maps ip-prec-dscp

Ip Precedence-dscp map:

ipprec: 0 1 2 3 4 5 6 7

---

dscp: 0 8 16 24 32 40 48 56

3、DSCP-COS map

DSCP-COS map table maps the dscp value of incoming packet to a cos value, which is used for the description of data traffic priority. The default mapping stauts is:

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

If you want to modify this mapping status, you can follow the steps below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mls qos map dscp-cos** *dscplist* **to** *cos*	Set new mapping stauts
3	**exit**	Back to privileged EXEC mode
4	**show mls qos maps dscp-cos**	Show DSCP-COS map

Example:

Configure **dscp-cos** map, map the value 1－10 to 7

Raisecom#config

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

Raisecom(config)#exit

Raisecom# show mls qos maps dscp-cos

In order to check if the configurations are correct, use command **show**:

Raisecom#show mls qos maps dscp-cos

Dscp-cos map:

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

In order to recover the DSCP-COS map to the default mapping status, use command **no**:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**no mls qos map dscp-cos**	Recover to the default mapping stauts
3	**exit**	Back to privileged EXEC mode
4	**show mls qos maps dscp-cos**	Show DSCP-COS map

In order to check if the configurations are correct, use command **show**:

Raisecom#show mls qos maps dscp-cos

Dscp-cos map:

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

4、DSCP-MUTATION map

If you want to realize QOS feature-based IP trafficb between two individual QOS domains, you can configure the port at the domain egdge as trust DSCP status, as a result, the port will accept the trusted DSCP value to avoid QOS classification processing. If the DSCP values of the two domains are different, you can use DSCP-to-DSCP map for conversion

DSCP-MUTATION map table maps the dscp value of incoming packets to a new dscp value, which is used for the QOS description of data traffic priority. There is a default map default-dscp in the switch, this map cannot be modified or deleted.

If you want to modify the mapping status, you should follow the steps below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mls qos map dscp-mutation** *dscpname dscplist* **to** *dscp*	Create new DSCP mapping status
3	**exit**	Back to privileged EXEC mode
4	**show mls qos maps dscp-mutation**	Show DSCP-MUTATION map

Example:

Configure **dscp-mutation** map, map the value 1－10，20－30 to 30：

Raisecom#config

Raisecom(config)# mls qos map dscp-mutation aaa 1-10 to 30

Raisecom(config)# mls qos map dscp-mutation aaa 20-30 to 30

Raisecom(config)#exit

Raisecom# show mls qos maps dscp-mutation

In order to check if the configurations are correct, use command **show**:

Raisecom#show mls qos maps dscp-mutation

Dscp-dscp mutation map:

default-dscp:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0 :	0	1	2	3	4	5	6	7	8	9
1 :	10	11	12	13	14	15	16	17	18	19
2 :	20	21	22	23	24	25	26	27	28	29
3 :	30	31	32	33	34	35	36	37	38	39
4 :	40	41	42	43	44	45	46	47	48	49
5 :	50	51	52	53	54	55	56	57	58	59
6 :	60	61	62	63						

Dscp-dscp mutation map:

aaa:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0 :	0	30	30	30	30	30	30	30	30	30
1 :	30	11	12	13	14	15	16	17	18	19
2 :	30	30	30	30	30	30	30	30	30	30
3 :	30	31	32	33	34	35	36	37	38	39
4 :	40	41	42	43	44	45	46	47	48	49
5 :	50	51	52	53	54	55	56	57	58	59
6 :	60	61	62	63						

In order to delte DSCP-MUTATION map, use the command **no**:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**no mls qos map dscp-mutation** *dscpname*	Delete DSCP mapping status
3	**exit**	Back to privileged EXEC mode
4	**show mls qos maps dscp-mutation**	Show DSCP-COS map

If you want to apply the DSCP-mutation map, you need to operate under the port configuration mode.

The default por configuration use default-dscp map:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port 1**	Enter port configuration mode
3	**mls qos dscp-mutation** *dscpname*	Use DSCP map
4	**exit**	back to port configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show mls qos port 1**	Show QOS port configuration status

example：

Raisecom#config

Raisecom(config)#interface port 1

Raisecom(config-port)# **mls qos dscp-mutation aaa**

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

Raisecom(config)#exit

Raisecom#show mls qos port 1

In order to check if the configurations are correct, use command **show**:

Raisecom#show mls qos port 1

port 1:

trust state: not trusted

default COS: 0

default DSCP: 0

DSCP override: disable

DSCP Mutation Map: aaa

Note: DSCP-MUTATION map is realized by using the hardware filtering function on the switch. Port 1-8 use the same filter table in the hardware (similar for port 9－16、17－24. port 25 and port 26 use one filter table, 5 tables in all). Therefore when any port in port 1-8 uses DSCP-MUTATION map, the other ports in port 1-8 use the same DSCP-MUTATION map.

In order to cancel the application of DSCP-MUTATION map on the port, use the command **no**:

Step	Command	description
1	**config**	Enter global configuration mode
2	**interface port 1**	Enter port configuration mode
3	**no mls qos dscp-mutation**	Cancel applying DSCP mapping

	dscpname	status
4	**exit**	Back to port configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show mls qos port 1**	Show QOS port configurations

In order to check if the configurations are correct, use command **show**:

Raisecom#show mls qos port 1

port 1:

trust state: not trusted

default COS: 0

default DSCP: 0

DSCP override: disable

DSCP Mutation Map: default-dscp

Note: when the dscp-mutation map is applied to a port, this map cannot be deleted; this map can be deleted only if it is not applied.

5、Configuration for COS value and output queue

Cos-queue map determine which queue to send packets according to COS value in them, QOS use this map to define data traffic priority. The default mapping status is:

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

If you want to modify the mapping status, follow the steps below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**queue cos-map** *queueid coslist*	Create new mapping status, which means packets with cos value 1－4 will be sent to queue 1
3	**exit**	Back to privileged EXEC mode
4	**show mls qos queuing**	Show QOS queue mapping status

Example：

Raisecom#config

Raisecom(config)# queue cos-map 1 1-4

Raisecom(config)#exit

Raisecom#show mls qos port 1

In order to check if the configurations are correct, use command **show**:

Raisecom#show mls qos queueing

the queue schedule mode: strict priority(SP)

Cos-queue map:

cos-queueid

0 - 1

1 - 1

2 - 1

3 - 1

4 - 1

5 - 3

6 - 4

7 - 4

In order to recover the Cos-queue map to default status, use command **no**:

Steps	Command	Desciption
1	**config**	Enter global configuration mode
2	**no queue cos-map**	Recover to the default mapping status
3	**exit**	Back to privileged EXEC mode
4	**show mls qos queuing**	Show QOS queue map

In order to check if the configurations are correct, use command **show**:

Raisecom#show mls qos queueing

the queue schedule mode: strict priority(SP)

Cos-queue map:

cos-queueid

0 - 1

1 - 1

2 - 2

3 - 2

4 - 3

5 - 3

6 - 4

7 - 4

29.2.5 QoS class map configuration

1、create, delete class-map

Use command **class-map** to isolate specified traffic. Matching conditions include ACL, IP precedence, DSCP, VLAN and class.

Create **class-map** according to the steps below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**class-map** *class-map-name* **[match-all | match-any]**	Create class-map named aaa, and enter config-cmap mode
3	**description WORD**	Description information
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode
6	**show class-map [WORD]**	Show CLASS MAP

There are two matching types for class-map, match-all carries out AND operation, which means multiple match demonstrations involve in the “and” operation, if congestion occurs, match demonstration will fail; match-any carries out “or” operation. Defalut status is match-all.

Example:

Raisecom#config

Raisecom(config)# **class-map** *aaa* **match-all**

Raisecom(config-cmap)# description this-is-test-class

Raisecom(config-cmap)#exit

Raisecom(config)#exit

In order to check if the configurations are correct, use command **show**:

Raisecom#show class-map

Class Map match-all aaa (id 0)

Description:this-is-test-class

Match none

If you want to delete a **class-map**, use command **no**, **no class-map** *class-map-name*。

Note: when deleting a class-map, if the map has been applied to a port, it cannot be deleted.

2、Match demonstration configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**class-map** *class-map-name*	enter config-cmap mode
3	**match** { **ip-access-list** | **mac-access-list** | **access-list-map**} *acl-index*	Match ACL
4	**match ip dscp {0-63}**	Match dscp value
5	**match ip precedence {0-7}**	Match TOS value
6	**match vlan {1-4094}**	Match VLAN
7	**match class-map WORD**	Match class map
8	**exit**	Back to global configuration mode
9	**exit**	Back to privileged EXEC mode
10	**show class-map [WORD]**	Show CLASS MAP

When matching ACL, ACL should be created firstly.

When matching class map, class-map should be created firstly.

If the matching condition type of class-map is match-all, configuration may fail due to congestion of matching information.

If the class-map has been applied to a port, match demonstration cannot be modified.

Example:

Raisecom#config

Raisecom(config)# ip-access-list 1 permit ip any 192.168.1.1 255.255.255.0

Raisecom(config)# class-map *aaa*

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

In order to check if the configurations are correct, use command **show**:

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

If you want to delete a match demonstration:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**class-map** *class-map-name*	Enter config-cmap mode
3	**no match { ip-access-list | mac-access-list | access-list-map }** *acl-index*	Match ACL
4	**no match ip dscp {0-63}**	Match dscp value
5	**no match ip precedence {0-7}**	Match TOS value
6	**no match vlan {1-4094}**	Match VLAN
7	**no match class-map WORD**	Match class map
8	**exit**	Back to global configuration mode
9	**exit**	Back to privileged EXEC mode
10	**show class-map [WORD]**	Show CLASS MAP

If this class-map has been applied to a port, deleting the match demonstration is not allowed.

29.2.6 QoS policy map configuration

1、create and delete policy-map

Use command **policy-map** to encapsulate and classify the data traffic defined by class-map for further applications.

Create policy-map:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**policy-map** *policy-map-name*	Create policy-map named bbb and enter config-pmap mode
3	**description WORD**	Description information
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode

6	**show policy-map [WORD]**	show POLICY MAP

Example：

Raisecom#config

Raisecom(config)# **policy-map** *bbb*

Raisecom(config)# **exit**

In order to check if the configurations are correct, use command **show**:

Raisecom#show policy-map

Policy Map bbb

Description:this-is-test-policy

If you want to delete a **policy-map**, use command **no**, **no policy-map** *policy-map-name***.**

Note: when deleting a policy-map, if it has already been applied to a port, it cannot be deleted.

29.2.7 QoS traffic classification

1、create and delete policer

Policer is used for the traffic rate-limiting and shaping, meanwhile, DSCP in the traffic may be modified, or bytes may be drop. Thress types of policers are available currently:

single-policer：every rule in the class-map uses this policer;

class-policer：all rules in the class-map share the using of this policer;

aggregate-policer：All the class-maps in a policy-map use this policer;

when the traffic rate exceeds the configured value（out profile）, two actions are supported: drop or mutate dscp value（marked down）..

Create policer：

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mls qos single-policer** *policer-name rate burst* **exceed-action {drop | policed-dscp-transmit** *marked-dscp* **}**	Create single type plicer
3	**mls qos class-policer** *policer-name rate burst*	Create class type policer

	exceed-action {drop | policed-dscp-transmit *marked-dscp* **}**	
4	**mls qos aggregate-policer** *policer-name rate burst* **exceed-action {drop | policed-dscp-transmit** *marked-dscp* **}**	Create aggregate type policer rate—traffic average rate, range is 8－2000000kbps。 burst—traffic burst value, range is 8－512000k bytes marked-dscp—new dscp value
5	**exit**	Back to global configuration mode
6	**show mls qos policer [single-policer | class-policer | aggregate-policer]**	show policer

Example：

Raisecom#config

Raisecom(config)# mls qos single-policer aaa 44 44 exceed-action policed-dscp-transmit 4

Raisecom(config)# exit

In order to check if the configurations are correct, use command **show**:

Raisecom#show mls qos policer

single-policer aaa 44 44 exceed-action policed-dscp-transmit 4

Not used by any policy map

If aaa is used to a port:

Raisecom#show mls qos port policers

Port id 1

policymap name: aaa

policer type: Single, name: aaa

rate: 44 kbps, burst: 44 kbyte, exceed action: policed-dscp-transmit, dscp: 4

if you want to delete a **policer**, use command **no**, **no {single-policer | class-policer | aggregate-policer }** *placer-name*。

Note: when deleting a **policer**, if it has been quoted by a policy and applied to a port, it cannot be deleted.

2、Defining traffci classification

If you want to add one or more class-map to a policy, follow the steps below:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**policy-map** *policy-map-name*	Enter config-pmap mode
3	**class-map** *class-map-name*	Add class-map aaa to policy aaa, and enter config-pmap-c mode
4	**exit**	Back to global configuration mode
4	**exit**	Back to privileged EXEC mode
5	**show policy-map [WORD]**	Show POLICY MAP

One class can be applied to multiple policies.

Example：

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**

In order to check if the configurations are correct, use command **show**:

Raisecom#show policy-map

Policy Map aaa

Class aaa

If you want to delete a class-map from a policy:

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**policy-map aaa**	Enter config-pmap mode
3	**no class-map aaa**	Delete class-map from a policy
4	**Exit**	Back to privileged EXEC mode
5	**show policy-map [WORD]**	Show POLICY MAP

If this policy-map has been applied to a port, it is not allowed to delete the class-map.

3、Define traffic actions

Currently 3 types of traffic actions are supported:

trust：traffic trust status, which is to trust COS、DSCP or TOS；

set：modify the COS、DSCP and TOS value in the data traffic;

police：for traffic rate-limiting and shaping.

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**policy-map** *policy-name*	Enter config-pmap mode
3	**class-map** *class-name*	Add class-mapto policy and enter config-pmap-c mode
4	**police** *policer-name*	Apply policer to traffic of this policy
5	**trust** [**cos** | **dscp** | **ip-precedence**]	Traffic trust status, trust dscp by defalut
6	**set** {**ip dscp** *new-dscp* | **ip precedence** *new-precedence* | **cos** *new-cos* }	New values for setting traffic
7	**Exit**	Back to config-pmap mode
8	**Exit**	Back to global configuration mode
9	**Exit**	Back to privileged EXEC mode
10	**show policy-map [WORD]**	Show POLICY MAP

Note: command “trust” is not supported by now. Commands “set” and “trust” are mutually exclusive. In addition, only one “set” item can be configured in a class-map, configuration closer to the back will take effect.

Example:

```
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)#exit
Raisecom(config-pmap)#exit
Raisecom(config)#exit
Raisecom# show policy-map aaa
```

To check if the configurations are correrct, use command **show**:

```
Raisecom#show policy-map
  Policy Map aaa
      Class aaa
```

police aaa

set ip precedence 4

If you want to delete or modify the traffic actions:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**policy-map aaa**	Enter config-pmap mode
3	**class-map aaa**	add class-map aaa to policy aaa, and enter config-pmap-c mode
4	**no police** *policer-name*	Apply policer on the traffic of this policy
5	**no trust** [**cos** | **dscp** | **ip-precedence**]	Traffic trust status, trust dscp by defalut
6	**no set** {**ip dscp** | **ip precedence** | **cos** }	New values for setting traffic
7	**exit**	Back to config-pmap mode
8	**exit**	Back to global configuration mode
9	**exit**	Back to privileged EXEC mode
10	**show policy-map [WORD]**	Show POLICY MAP

If the policy-map has been applied to a port, it is not allowed to modify actions.

29.2.8 Apply policy on port

Policy will note take effect before applied to a specified port.

Policy application steps are as follows:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service-policy** *policy-name* **ingress** *portid* **[egress** *portlist* **]**	Apply policy on egress or ingress
5	**exit**	Back to privileged EXEC mode
6	**show mls qos port** *portid*	Show qos port information

Note: before applying policy, QOS should be enabled; Trust status of policy and port are mutually exclusive, if the port tust status is not “UNTRUST” before application, the status will changed to “UNTRUST” after that.

Example:

Raisecom#config

Raisecom(config)#service-policy aaa ingress 2 egress 1-5

Raisecom(config)#exit

Raisecom#show mls qos port 2

In order to check if the configurations are correct, use command **show**:

Raisecom#show mls qos port 2

port 2:

Attached policy-map: aaa

trust state: untrust

default COS: 0

default DSCP: 0

DSCP override: disable

DSCP Mutation Map: aaa

If you want to cancel policy application, use command **no**, **no service-policy** *policy-name* **ingress** *portid***.**

29.2.9 Output queueing scheduling mode

Currently, the switch supports four types of queue scheduling modes: strict-priority (SP), Weighted Round Robin (WRR), BOUND-DELAY mode and SP+WRR hybrid mode. SP mode is the default status.

Configuration steps:

Step	Command	Descrption
1	**config**	Enter global configuration mode
2	**queue strict-priority**	Configure it as strict priority
3	**queue wrr-weight** *weight0 weight1 weight2 weight3*	Configure the port scheduling mode as WRR mode
4	**queue bounded-delay** *weight0 weight1 weight2 weight3 delaytime*	Configure the port scheduling mode as BOUNDDELAY mode delaytime——delay
5	**queue preemp-wrr** *weight1 weight2 weight3*	Configure the port scheduling mode as PREEMP-WR mode, which means queue 1 is under SP mode with the other queues depending on weights.
6	**exit**	Back to privileged EXEC mode

7	**show mls qos queuing**	Show qos queueing information

Currently, SP+WRR hybrid mode **preemp-wrr** is not supported.

Example：configure the queue as WRR mode with weights being 1:2:4:8：

Raisecom#config

Raisecom(config)# queue wrr-weight 1 2 4 8

Raisecom(config)#exit

Raisecom#show mls qos queuing

Results:

Raisecom#show mls qos queuing

the queue schedule mode: weighted round robin(WRR)

wrr queue weights:

Queue ID - Weights - Delay

1 - 1 - 0

2 - 2 - 0

3 - 4 - 0

4 - 8 - 0

Configure the queueing as BOUNDDELAY mode with weights being 1:3:5:7, delay being 100ms:

Raisecom#config

Raisecom(config)# queue bounded-delay 1 2 4 8 100

Raisecom(config)#exit

Raisecom#show mls qos queuing

Results:

Raisecom#show mls qos queueing

the queue schedule mode: bounded delay

wrr queue weights:

Queue ID - Weights - Delay

1 - 1 - 100

2 - 3 - 100

3 - 5 - 100

4 - 7 - 100

29.3 QOS monitor and maintenance

User can also use command **show** to view the switch QOS status and configurations for monitoring and maintenance.

Command, mode	The commands below need to be carried out under ENABLE mode
show mls qos	Show Qos enable/disable status
show mls qos policer [*policename* **| aggregate-policer |class-policer | single-policer]**	Show policer information
show mls qos maps [**cos-dscp** | **dscp-cos** | **dscp-mutation** | **ip-prec-dscp**]	Show the configurations for the maps
show mls qos queueing	Show input/output queueing information
show mls qos port *portid* [**policers**]	Show port policy configuration, policer information and so on
show class-map [*class-map-name*]	Show class-map information
show policy-map [*policy-map-name* | [**port** *portId*] [**class** *class-name*]	Show policy information

29.3.1 Show QOS enable/disable information

Raisecom#show mls qos
QoS is enabled.

29.3.2 Show QOS policer information

Raisecom#show mls qos policer
single-policer aaa 44 44 exceed-action policed-dscp-transmit 4
Used by policy map aaa

Use the commands below if you want to view which port uses policer:
Raisecom#show mls qos port policers
Port id 1
policymap name: aaa
policer type: Single, name: aaa
rate: 44 kbps, burst: 44 kbyte, exceed action: policed-dscp-transmit, dscp:4

29.3.3 Show QOS maps information

Raisecom#show mls qos maps

Dscp-cos map:

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

Cos-dscp map:

cos:	0	1	2	3	4	5	6	7
dscp:	0	8	16	24	32	40	48	56

Ip Precedence-dscp map:

ipprec:	0	1	2	3	4	5	6	7
dscp:	0	8	16	24	32	40	48	56

Dscp-dscp mutation map:

default-dscp:

d1 : d2	0	1	2	3	4	5	6	7	8	9
0 :	0	1	2	3	4	5	6	7	8	9
1 :	10	11	12	13	14	15	16	17	18	19
2 :	20	21	22	23	24	25	26	27	28	29
3 :	30	31	32	33	34	35	36	37	38	39
4 :	40	41	42	43	44	45	46	47	48	49
5 :	50	51	52	53	54	55	56	57	58	59
6 :	60	61	62	63						

Dscp-dscp mutation map:

aaa:

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

1 :	30	30	30	30	30	30	30	30	30	30
2 :	30	21	22	23	24	25	26	27	28	29
3 :	30	31	32	33	34	35	36	37	38	39
4 :	40	41	42	43	44	45	46	47	48	49
5 :	50	51	52	53	54	55	56	57	58	59
6 :	60	61	62	63						

29.3.4 Show QOS queueing information

Raisecom#show mls qos queueing
the queue schedule mode: bounded delay

wrr queue weights:

queueid-weights-delay

1	-	1	-	100
2	-	3	-	100
3	-	5	-	100
4	-	7	-	100

Cos-queue map:

cos-queueid

0	-	1
1	-	1
2	-	2
3	-	2
4	-	3
5	-	3
6	-	4
7	-	4

29.3.5 Show port QOS information

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

To view all port QOS information:
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

29.3.6 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 none

To show the designated class-map:

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

29.3.7 Show QOS policy-map information

Raisecom#show policy-map

Policy Map aaa

Class aaa

police aaa

set ip precedence 4

Class bbb

police aaa

To show designated policy-map information:

Raisecom#show policy-map aaa

Policy Map aaa

Class aaa

police aaa

set ip precedence 4

Class bbb

police aaa

To show designated policy-map name with the related class-map:

Raisecom#show policy-map aaa class-map aaa

Policy Map aaa

Class aaa

police aaa
set ip precedence 4

29.3.7 Show QOS policy-map application information

To view policy-map information applied on a port:
Raisecom#show policy-map port 1
port 1:
Policy Map aaa:
Egerss:1-5
Class Map :aaa (match-all)
Class Map :bbb (match-all)

To view 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)

29.4 QOS trouble shooting

- ✧ Port TRUST status and policy configuration are mutually exclusive;
- ✧ Traffic TRUST status and SET actions are mutually exclusive;
- ✧ When deleting class-map、policy-map、policer, if these maps have already been applied on a port, the deletion will fail;
- ✧ When class-map、policy-map have already been applied on port, to modify the matched and to modify the traffic actions such as the set actions will fail;
- ✧ If you want to apply a traffic policy, QOS should be enabled in advance; traffic policy will fail to take effects if QOS is disabled;
- ✧ If the matching type of class-map is match-all, since the matched information may have collision, the configuration may fail.
- ✧ When matching an ACL, the ACL should be defined first, and the type should be permit;
- ✧ When matching a class-map, the type of sub class-map should be match-all;
- ✧ When configuring massive traffics, the configuration may fail during applications. The possible reason is that rules have exceeded 256 rules in all that supported for 8 ports;
- ✧ When enabling QOS policy, the flow control function is suggested to shutdown;

29.5 QOS command references

Command	Description
[no] mls qos	Enable and disable QOS
[no] mls qos trust [**cos** | **dscp | ip-precedence**]	Port TRUST status configuration
mls qos default-cos *default-cos*	QOS default COS value of port
no mls qos default-cos	Recover port default COS value
mls qos default-dscp { *default-dscp* | **override }**	Configure QOS port defalult DSCP value
no mls qos default-dscp [override]	Recover QOS port default DSCP value
mls qos map dscp-mutation *dscp-name dcp-list* **to** *dscp*	Create dscp-mutaion map
no mls qos map dscp-mutation *dscp-name*	Delete dscp-mutaion map
[no] mls qos dscp-mutation *dscp-name*	Apply or cancel applying dscp-mutaion map
class-map *class-map-name* **[match-any | match-all]**	Create class-map
no class-map *class-map-name*	Delete class-map
[no] policy-map *policy-map-name* **description** *WORD*	Create/delete policy map Set description information for policy mapand class-map
[no] class *class-map-name*	Apply class map to a policy
match { **ip-access-list** *acl-index* **| mac-access-list** *acl-index* **| access-list-map** *acl-index* | **ip dscp** *dscp-list* | **ip precedence** *ip-precedence-list* | **class** *calss-name* | **vlan** *vlanlist*}	Set match demonstration
no match { **ip-access-list** *acl-index* **| mac-access-list** *acl-index* **| access-list-map** *acl-index* | **ip dscp** | **ip precedence | class** *calss-name* | **vlan** *vlanlist* }	Delete match demonstration
[no] trust [**cos** | **dscp |**	Traffic TRUST status configuration

ip-precedence]	
set {**ip dscp** *new-dscp* | **ip precedence** *new-precedence* | **cos** *new-cos* }	Set action
no set {**ip dscp** | **ip precedence** | **cos** }	Delete set value
mls qos {aggregate-policer |class-policer | single-policer } *policer-name rate burst* **[exceed-action { drop | policed-dscp-transmit** *dscp* **}]**	Create policer
no mls qos {aggregate-policer |class-policer | single-policer } *policer-name*	Delete policer
[no] police *policer-name*	Apply policer
service-policy *policy-map-name* **ingress** *portid* **[egress** *portlist*]	Apply policy
no service-policy *policy-map-name* **ingress** *portid*	Cancel applying policy
mls qos map cos-dscp *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Configure the mapping from cos to dscp
no mls qos map cos-dscp	reover the mapping from cos to dscp
mls qos map ip-prec-dscp *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Configure the mapping from TOS to dscp
no mls qos map ip-prec-dscp	Recover the mapping from TOS to dscp
mls qos map dscp-cos *dscp-list* **to** *cos*	Configure the mapping from dscp to switch inner priority
no mls qos map dscp-cos	Recover the mapping from dscp to switch inners priority
queue cos-map *queue-id cos-list*	Configure the mapping from switch inner priority to quequeing
no queue cos-map	Recover the mapping from switch inner priority to queue 恢复交换机内部优先级到队列的映射
queue wrr-weight *weight0 weight1*	Configure the switch queueing scheduling

weight2 weight3	mode as WRR
queue bounded-delay *weight0 weight1 weight2 weight3 delaytime*	Configure the port scheduling mode as BOUNDDELAY
queue preemp-wrr *weight1 weight2 weight3*	Configure the port scheduling mode as PREEMP-WRR
queue strict-priority	Configure the port scheduling mode as strict-priority
show mls qos	Show Qos enable/disable status
show mls qos policer [*policename* **| aggregate-policer |class-policer | single-policer]**	Show policer information
show mls qos maps [**cos-dscp** | **dscp-cos** | **dscp-mutation** | **ip-prec-dscp**]	Show configuration contents of every map
show mls qos queueing	Show input/output queueing configuration information
show mls qos port *portid* [**policers**]	Show port policy configuration, policer information and so on
show class-map [*class-map-name*]	Show class-map information
show policy-map [*policy-map-name* | [**port** *portId*] [**class** *class-name*]	show policy information

Chapter 30 MVR configuration

This chapter introduces MVR function and IGMP filter function of ISCOM series switches with the relevant configurations.

30.1 MVR introduction

Multicast VLAN registration is applied as traffic multicast in the network of service provider, such as TV programme ordering. MVR allows subscriber on the port to order or cancel the multicast traffic in VLAN, allows data traffic sharing for different VLANs. There are two MVR aims:

- ✧ By using simple configurations, use can transmit multicast among different VLANs safely and effectively;
- ✧ Support multicast group joining and leaving dynamically;

The operation manner of MVR is similar to that of IGMP snooping. These two functions can be enabled simultaneously. MVR only processes the joining and leaving of configured multicast groups, the other multicast groups are managed by IGMP snooping. The difference between these two is that: with IGMP snooping, the multicast traffic can be transmitted within only one VLAN, while with MVR the multicast traffic can be transmitted within different VLANs.

There are two operation modes:

- ✧ Compatible mode: all multicast data received at the source port (port connected with multicast router) will be forwarded to the other ports, no matter whether these source ports have members to join in or not. Simultaneously, multicast data are only forwarded to those receiving ports (ports connected with subscribers) which are specified to have already joined in the MVR group, the joining can be in the form of IGMP report or MVR static configuration. IGMP report will not be forwarded to the source port of switch. Therefore, the switch dose not support source port joining dynamically. Under this mode, multicast router should be configured as forwarding all multicast data to the source port, since switch will not send IGMP joining information to the router.
- ✧ Dynamic mode: Received multicast data are only forwarded to those ports which have member to join (source port or receiving port), the joining can be in the form of IGMP report information or MVR static configurations. All received IGMP information is forwarded to the source port of the switch. This method could save much bandwidth.

MVR are operative only on Layer-2. It dose not work on Layer-3. One switch can configure only one multicast VLAN, support 256 multicast groups at most.

30.2 IGMP filter introduction

Administrator needs to limit the multicast users under some circumstances, such as to allow which ports to receive multicast on a switch, which ports to reject multicast data. Use can realize this kind of control on the port by configuring IGMP profile. One IGMP profile includes one or multiple multicast groups, and permit/deny items to access these groups. If one “deny” type IGMP profile is applied to the port, when the port receives IGMP joining information of this group, it will drop and do not allow receiving multicast data from this group. IGMP profile can be applied to dynamic multicast group, not suitable for static group.

The maximum multicast group can be configured on port.

30.3 MVR configuration list

Configuration includes:

- ✧ MVR global configuration
- ✧ MVR port information
- ✧ MVR monitor and maintenance

30.3.1 MVR default configuration

Attributes	Default configuration
MVR enable/disable	disabled
Multicast address	Not configured
MVR timeout	600 seconds
Multicast VLAN	1
MVR mode	compatible
Port MVR enable/disable	disabled
Port default configuration	Non MVR（neither source port, nor receiving port）
Intermediate leave	disabled

The steps below should be followed:

- ✧ Receiving port can be only ACCESS port, but cannot be TRUNK port. Receiving port can belong to different VLANs, but cannot belong to multicast VLAN;

- ✧ The maximum MVR multicast address is 256;
- ✧ Since ISCOM28 series switches support Layer-2 multicast, which means multiple IP multicast addresses correspond to one MAC multicast address, MVR multicast address is not allowed using repetitive names during configuration.
- ✧ MVR and IGMP snooping can coexist；
- ✧ Source port should be in the multicast VLAN;

30.3.2 MVR global configuration

Under the default situation, MVR is disabled. User can carry out the commands below to enable MVR under global configuration mode. Multicast VLAN, multicast address, operation modes can be configured as well. If MVR has not been enabled yet, it is allowed to configure MVR. Once MVR is enabled, these configurations will take effect at once.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mvr enable**	Enable MVR
3	**mvr group** *ip -address* [*count*]	Configure IP multicast address, if the parameter count is specified, you can configure a consecutive MVR group addresses (the range for count is from 1 to 256, 1 by default)
4	**mvr timeout** *timeout*	optional， MVR multicast entity timeout, unit is second, range is from 60 to 36000, 600 seconds by deflault.
5	**mvr vlan** *vlanid*	optional，to specify the VLANs for receiving multicast, all source ports should belong to this VLAN. Range is from 1 to 5094. 1 by default.
6	**mvr mode { dynamic | compatible }**	optional，MVR operation modes: Dynamic——Dynamic mode Compatible——Compatible mode
7	**exit**	Back to privileged EXEC mode
8	**show mvr**	Show MVR configuration

9	**show mvr members**	Show MVR group address

To disable MVR, carry out command **mvr disable** under global configuration mode. To set the other configurations back to default status, use command **no mvr {mode | group** *ip-address* **| timeout | vlan}.**

Command **mvr group** *ip –address* indicates which multicast traffic can be received. If this parameter is not specified, all traffics will be received.

The example below shows how to enable MVR, how to configure multicast address, timeout and multicast vlan:

raisecom(config)**# mvr enable**

raisecom (config)**# mvr group** 234.5.6.7

raisecom (config)**# mvr timeout** 180

raisecom (config)**# mvr vlan** 22

raisecom (config)**# mvr mode dynamic**

To check if the configurations are correct, use command **show**:

Raisecom#show mvr

MVR Running: Enable

MVR Multicast VLAN: 22

MVR Max Multicast Groups: 256

MVR Current Multicast Groups: 1

MVR Timeout: 180 (second)

MVR Mode: dynamic

To view MVR group address configurations:

Raisecom#show mvr members

MVR Group IP Status Menbers

234.5.6.7 Inactive none

30.3.3 MVR port information configuration

Under default situation, ports on switch are neither receiving port, nor source ports. User can configure them under interface configuration mode;

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

2	**mvr**	enable MVR
3	**interface port 3**	Enter interface configuration mode
4	**mvr**	Enable interface MVR
5	**mvr type { source | receiver }**	Mvr type configuration: Source——uplink port can be configured as souce port for receiving multicast data, this port cannot be connect directly to subscribers, all source ports should belong to multicast VLAN. Receiver——configured as to connect subscribers straightforward, cannot belong to multicast VLAN.
6	**mvr vlan** *vlanid* **group** *ip-address*	Optional, set the port to join multicast group statically. Under compatible mode, this command can applied to receiving port, and can be applied to source port or receiving port dynamically.
7	**mvr immediate**	Enable automatic leaving function onthis port, this command can be only applied on receiving port
8	**exit**	Back to global configuration mode
9	**exit**	Back to privileged EXEC mode
10	**show mvr**	Show MVR configuration status
11	**show mvr port [***portid***]**	Show port mvr configuration information
12	**show mvr port [***portid***] members**	Show port member information

To set port MVR configuration back to default status, use command **no mvr** [**type** | **immediate** | **vlan** *vlan-id* **group**]. Use command **no mvr vlan** *vlan-id* **group** to delete all static multicast group, you can specify a multicast address if you want to delete only one group. The example below shows how to configure port 3 as MVR receiving port, and how to enable intermediate leaving function and how to join into the static multicast group:

Raisecom#config

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

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

Raisecom(config-port)**#mvr type receiver**

Raisecom(config-port)**#mvr immediate**

Raisecom(config-port)**#mvr vlan** 1 **group** 234.5.6.7

Raisecom(config-port)#exit

Raisecom(config)#exit

To check if the configurations are correct, use command **show**:

Raisecom#show mvr port 3

Running: Enable

Type: Receiver

Status: Inactive/down

Immediate Leave: Enable

Raisecom#show mvr port 3 members

MVR Group IP Type Status

234.5.6.7 static Inactive

30.3.4 MVR monitor and maintenance

You can use some “show” commands to view the MVR running status and configurations for the switch in which way you can achieve a better monitor and maintenance:

Command, mode	Commands below need to run under ENABLE mode
show mvr	Show MVR global configuration information
show mvr members	show MVR group information
show mvr port [*portid* **]**	show MVR port configuration information
show mvr port *portid* **members**	Show MVR static or dynamic group information

Show MVR global configuration information

Raisecom#show mvr

MVR Running: Enable

MVR Multicast VLAN: 1

MVR Max Multicast Groups: 256

MVR Current Multicast Groups: 0

MVR Timeout: 600 (second)

MVR Mode: Compatible

Show MVR group information

Raisecom#show mvr members

MVR Group IP Status Menbers

234.5.6.7 Active 1

234.5.6.8 Active 1

234.5.6.9 Inactive None

234.5.6.10 Inactive None

show MVR port configuration information

Raisecom#show mvr port

Port Running Type Status Immediate Leave

---

1 Enable Receiver Inactive/down Enable

2 Disable Non-MVR Inactive/down Disable

3 Disable Non-MVR Inactive/down Disable

4 Disable Non-MVR Inactive/down Disable

5 Disable Non-MVR Inactive/down Disable

6 Disable Non-MVR Inactive/down Disable

7 Disable Non-MVR Inactive/Up Disable

……

25 Disable Non-MVR Inactive/down Disable

26 Disable Non-MVR Inactive/down Disable

To show designated port information:

Raisecom#show mvr port 1

Running: Enable

Type: Receiver

Status: Inactive/down

Immediate Leave: Enable

Show MVR port group information

Raisecom#show mvr port 1 members

MVR Group IP Type Status

```
-------------------------------------------
234.5.6.7          static      Inactive
234.5.6.8          static      Inactive
```

30.4 IGMP filter configuration

- ✧ IGMP profile configuration
- ✧ Applying IGMP profile
- ✧ port maximum group configuration
- ✧ IGMP filter monitoring and maintenance

30.4.1 IGMP filter default configuration

Attribute	Default configuration
IGMP filter enable/disable	Enabled
Port application	No application
Maximum group	No limit
Maximum group action	Reject
IGMP profile	Not defined
IGMP profile action	reject

30.4.2 Profile configuration

Use command **ip igmp profile** under global configuration mode, you can create IGMP profile and enter profile configuration mode. Parameters such as range, actions and etc. can be configured under this mode.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip igmp profile** *profile-number*	Create profile and enter profile configuration mode, series number of profile is from 1 to 65535.
3	**permit | deny**	Optional, actions configuration including permit or deny multicast group access, the default status is deny.
4	**range** *start-ip* [*end-ip*]	IP multicast address or address range configurations. If inputting

		address range, the starting address, blanks and ending address should be within the group address.
5	**exit**	Back to global configuration mode
6	**exit**	Back to privileged EXEC mode
8	**show ip igmp profile [** *profile-number*]	Show IGMP profile configuration information

To delete profile, carry out **no ip igmp profile** under global configuration mode. To delete a multicast address of profile, use command **no range** *start-ip*.

The example below shows how to create profile 1 and configure single multicast address:

raisecom(config)**# ip igmp profile 1**
raisecom (config-profile)**# range** 234.5.6.7
raisecom (config-profile)**# range** 234.5.6.9
raisecom (config-profile)**# permit**
raisecom (config-profile)**#exit**
raisecom (config)**#exit**

To check if the configurations are correct, use command **show**:

Raisecom#show ip igmp profile 1
IGMP profile 1
permit
range 234.5.6.7
range 234.5.6.9

30.4.3 Applying IGMP profile

Use command **ip igmp filter** under interface configuration mode to apply the created IGMP profile on a specified port. One IGMP profile can be applied to multiple ports, but one port can have only one IGMP profile.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port 1**	Enter interface configuration mode
3	**ip igmp filter** *profile-number*	Apply IGMP profile on port, profile series number is from 1 to 65535
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC mode

6	**show ip igmp filter port [** *portid* **]**	Show IGMP profile applied on port

To cancel applying IGMP profile, use command **no ip igmp filter** under interface configuration mode. If no IGMP profile is applied to port, no result will be shown.

The example below shows how to apply IGMP profile 1:

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

raisecom (config-port)# **ip igmp filter 1**

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

raisecom (config)**#exit**

To check if the configurations are correct, use command **show**:

Raisecom#show ip igmp filter port

Port	Filter	Max Groups	Current Groups	Action
1	1	20	0	Deny
2	0	20	0	Deny
3	0	0	0	Deny
……				
25	0	0	0	Deny
26	0	0	0	Deny

To view port 1 information:

Raisecom#show ip igmp filter port 1

IGMP Filter: 1

Max Groups: 20

Current groups: 0

Action: Deny

30.4.4 Port maximum multicast group configuration

Use command **ip igmp max-groups** under interface configuration mode to limit the group number for the port.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port 1**	Enter interface configuration mode
3	**ip igmp max-groups** *group-number*	Configure maximum groups for the port, range is from 0 to 65535，0 means no limit.

4	**ip igmp max-groups action { deny | replace }**	Optional, actions when the joining groups exceed the configured value. The default status is denied. **Replace** is not supported currently.
5	**exit**	Back to global configuration mode
6	**exit**	Back to privileged EXEC mode
7	**show ip igmp filter port [** *portid* **]**	Show port configuration information

To recover to the default configurations, use commands **no ip igmp max-groups [action]** under interface configuration mode.

The example below shows how to configure the maximum-group limit:

raisecom(config)**# interface port 1**
raisecom (config-port)**# ip igmp max-groups 20**
raisecom (config-port)**# ip igmp max-groups action deny**
raisecom (config-port)**#exit**
raisecom (config)**#exit**

To check if the configurations are correct, use command **show**:

Raisecom#show ip igmp filter port

Port	Filter	Max Groups	Current Groups	Action
1	1	20	0	Deny
2	0	0	0	Deny
3	0	0	0	Deny
……				
25	0	0	0	Deny
26	0	0	0	Deny

To view port 1 information:

Raisecom#show ip igmp filter port 1
IGMP Filter: 1
Max Groups: 20
Current groups: 0
Action: Deny

30.4.5 IGMP filter monitoring and maintenance

User can use some “show” commands to view the IGMP running status and configurations.

Command, mode	Commands below should be used under ENABLE mode
show ip igmp filter	Show IGMP filter global configuration information
show ip igmp profile [*profile-number***]**	Show IGMP profile information
show ip igmp filter port [*portid* **]**	Show IGMP filter port configuration information

To show IGMP filter global configuration information

Raisecom# show ip igmp filter

IGMPfilter: Enable

To show IGMP profile information

Raisecom#show ip igmp profile

IGMP profile 1
permit
range 234.1.1.1 234.2.2.2
range 234.5.1.1 234.5.2.2
IGMP profile 2
Deny
range 234.1.1.1 234.2.2.2
range 234.5.1.1 234.5.2.2

To show designated profile information:
Raisecom#show ip igmp profile 1
IGMP profile 1
permit
range 234.1.1.1 234.2.2.2
range 234.5.1.1 234.5.2.2

To show IGMP filter port configuration information

Raisecom#show ip igmp filter port

Port	Filter	Max Groups	Current Groups	Action
1	1	20	0	Deny
2	2	20	0	Deny
3	0	0	0	Deny
◦ ◦ ◦ ◦ ◦ ◦				
25	0	0	0	Deny
26	0	0	0	Deny

To show designated port information:

Raisecom#show ip igmp filter port 1

IGMP Filter: 1

Max Groups: 20

Current groups: 0

Action: Deny

30.5 MVR typical application configuration

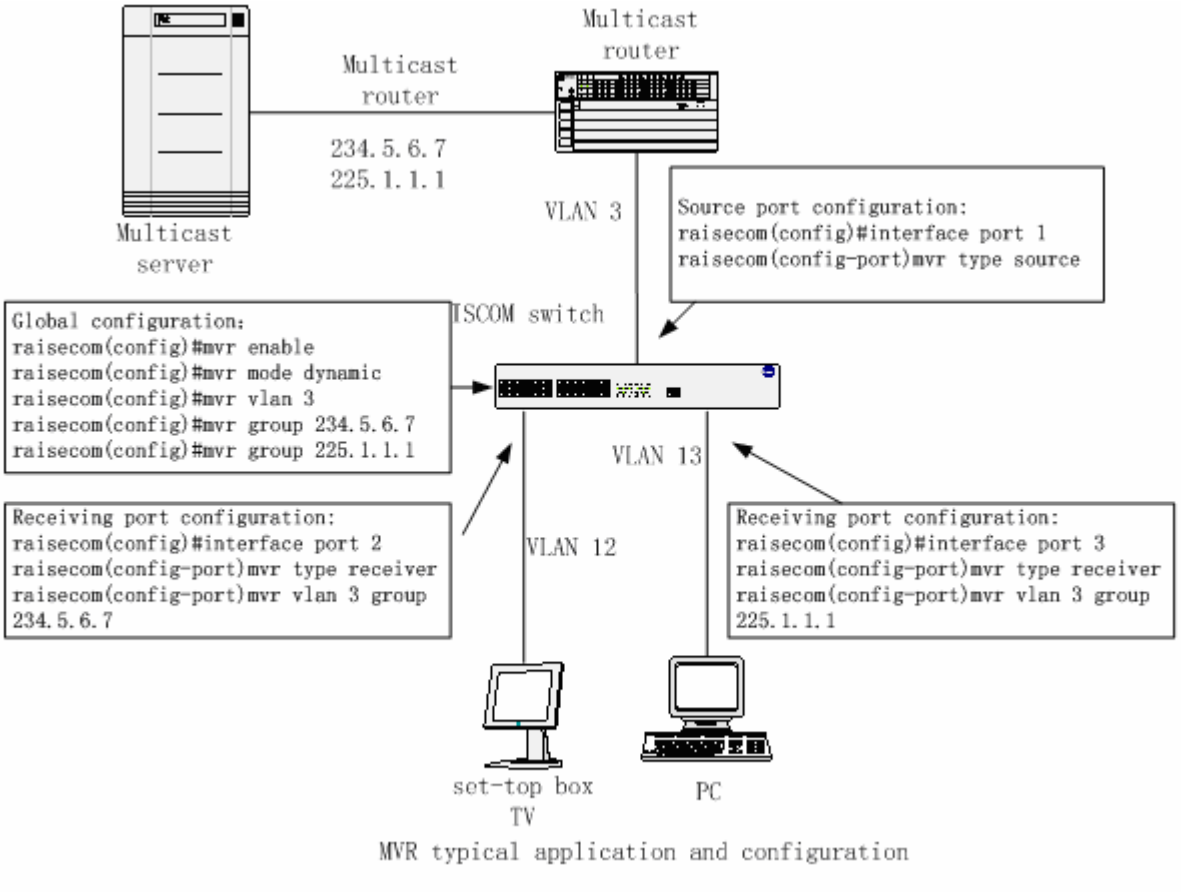
PC or TV set-top box can receive multicast traffics, one or multiple PC or televisions can connect to a receiving port called subscriber. When selecting scheduled programs, set-top or PC sends IGMP report information to join a group. If IGMP report matches to the configured multicast addresses on the switch, the CPU on the switch will modify the multicast switch table in the hardware, and add this port to the multicast VLAN group. When the source port receives the multicast traffic, it will send the traffic to the receiving ports according to the multicast forwarding table in the hardware.

When switching channels or shutting down the TV, the set-top box or PC will send IGMP leaving information, then the switch will forward this information to the multicast router, the router will send IGMP query information, if there is no other member in this group, the switch will delete this port from the group.

If enabling immediate leaving function on the receiving port, port will leave the group faster. If the immediate leaving function is not enabled yet, when the receiving port receives IGMP leaving information, the switch will forward router's IGMP query information and wait IGMP member report. If no report is received within the maximum query time, the member will be deleted from the group. If enabling the immediate leaving function, port member will be deleted as soon as it receives IGMP leaving information. This feature is normally used in the situation that one port is connected to only one user.

Multicast traffic will not be transmitted in all VLANs, but only need to be transmitted in multicast VLAN.

Use can save much bandwidth in this way.



30.6 MVR and IGMP filter troubleshooting

- ✧ When configuring source port, it shouldn't belong to multicast VLAN;
- ✧ When configuring receiving port, it should belong to multicast VLAN;
- ✧ When configuring MVR group, the multicast addresses may have conflicts since multiple IP addresses correspond to one MAC multicast address;
- ✧ When configuring static multicast on port, the address shouldn't be involved in the MVR groups;
- ✧ Under MVR compatible mode, to configure static multicast on source port;

30.7 MVR and IGMP filter commands references

Command	Description
mvr { enable | disable }	Enable/disable MVR
mvr vlan *vlanid*	Configure multicast VLAN
no mvr vlan	Recover multicast VLAN to default

	status
mvr timeout *timeout*	Configure MVR timeout
no mvr vlan	Recover MVR timeout to default status
mvr mode { dynamic | compatible }	Configure MVR mode
[no] mvr group *ip -adress* [*count*]	Configure MVR multicast group
[no] mvr	enable/disable port MVR
mvr type { source | receiver}	Configure port MVR type
no mvr type	Delete port MVR type
[no] mvr immediate	Configure mvr immediate
mvr vlan *vlanid* **group** *ip-address*	Configure the port as static multicast group member
no mvr vlan *vlanid* **group [***ip-address***]**	Delete static multicast group member
[no] ip igmp filter	Enable/disable IGMP filter function
[no] ip igmp profile [*profile-number***]**	Create IGMP profile information
permit | deny	Configure IGMP profile action
[no] range *start-ip* [*end-ip*]	Configure IGMP profile range
ip igmp filter *profile-number*	Apply IGMP profile on port
no ip igmp filter	Cancel applying IGMP profile on port
ip igmp max-groups *group-number*	Configure maximum group on port
no ip igmp max-groups	Recover maximum group on port to default configurations
ip igmp max-groups action { deny | replace }	Actions when the joining groups exceed the configured value
no ip igmp max-groups action	Recover to the default configuration as”deny”
show mvr	Show MVR configuration information
show mvr member [*ip-address* **]**	Show MVR multicast group member information
show mvr port [*portid***]**	Show MVR port configuration information
show mvr port *portid* **members**	Show static multicast group member information
show ip igmp filter	Show IGMP filter configuration information
show ip igmp profile [*profile-number***]**	Show IGMP profile configuration information
show ip igmp filter port [*portid* **]**	Show IGMP filter port configuration information

Chapter 31 KEEPALIVE configuration

31.1 Intruduce KEEPALIVE

Keepalive module Used to send KEEPALIVE trap to network management site, so the switch can be found by network management site.

31.2 KEEPALIVE configuration list

1. Send start, close and stop of KEEPALIVE trap periodically.
2. Set the period of KEEPALIVE trap.

31.2.1 Start and stop KEEPALIVE

KEEPALIVE is enabled by default. Send KEEPALIVE trap periodically.

step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server keepalive-trap {enable|disable|pause}**	Enable, disable and pause keepalive trap
3	**exit**	Back to privileged EXEC MODE
4	**show snmp config**	Show snmp basal configuration

31.2.2 Set the period of KEEPALIVE trap

Set the time interval of keepalive trap.

step	Command	Description
1	**config**	Enter global configuration mode
2	**snmp-server keepalive-trap interval** *<120-28800>*	Set the time interval of sending keepalive trap to SNMP network site
3	**exit**	Back to privileged EXEC MODE
4	**show snmp config**	Show snmp basal configuration

Time rang is from 120s to 28800s, default vaule is 300s.

Recover to default: Raisecom(config)**#no snmp-server keepalive-trap interval**

31.2.3 Monitor and maintenance

Show run and configuration of KEEPALIVE.

Command	Description

show snmp config	Show snmp basal configuration

Chapter 32 User network

This chapter introduces the configuration of user network. This function can diagnose the connectivity.

32.1 User network overview

RC581 is deployed at the demarcation point between the carrier and customer, which includes both a Network Interface Device for OAM functionality plus a User Network Interface (UNI) for providing advanced services definition. RC581 provides the functions such as monitoring, QoS, and VLAN that most layer-2 switches support.This enables carrier easy to remotely test and isolate customer premise.

32.2 User network command

32.2.1 Enter user network mode

step	Command	Description
1	**config**	Enter global configuration mode
2	**user-network diagnostics**	Enter user network mode
3	**exit**	Back to privileged EXEC MODE

There is only one user is allowed in user network mode. Exit save-diagconfig command can quit.

Congiguration load function is not support in this mode.

32.2.2 Confige user network IP address

step	Command	Description
1	**config**	Enter global configuration mode
2	**user-network diagnostics**	Enter user network mode
3	**ip address ipaddress [mask] <1-4094> [port {1-2}]**	Set user network IP address
4	**ip default-gateway A.B.C.D**	Set the default gateway
5	**show interface ip**	show ip interface configuration
6	**exit save-diagconfig**	Save user network configuration and Back to privileged EXEC MODE

The user netork can only support one virtual interface, which relate with multiple static vlan and management interface. If there is no static VLAN exist, the L3 interface can not be work.

By default, all interfaces are the management interface.

user netork is implyment by outlying network protocol, differentiate and manage network by VLAN.

When the L3 interface is set, ping command can be used to diagnose the connectivity, and telnet command can manage the remote host.

Chapter 33 Routing protocol configuration

This chapter introduces RIP and OSPF function and configuration of ISCOM3000 series switch.

33.1 routing overview

If there is no L3 device between VLANs, the devices which are in different VLAN can not communicate with each other. There are three kinds of route.

- ✧ default route;
- ✧ static route;
- ✧ dynamic route.

A default route is a special route. You can configure a default route using a static route.

A static route is a special route configured manually by an administrator.

You can set up an interconnecting network with the static route configuration. The problem for such

Configuration is when a fault occurs to the network, the static route cannot change automatically to steer away from the node causing the fault, if without the help of an administrator. In a relatively simple network, you only need to configure the static routes to make the router work normally. The proper configuration and usage of the static route can improve the network performance and ensure the bandwidth of the important

applications.

Dynamic rouing protocol can calculate the bast path, raisecom switch support 2 kinds of dynamic protocol.

- ➢ Distance-vector routing: Distance-vector routing can best be described as forwarding packets by getting directions along the way.

- ➢ Link state routing protocol: Link-state routing is a better technique for larger networks. L3 device use it to build a topological database that describes routes on the entire internetwork. This information is used to build routing tables with more accurate routing information. Link-state routing also responds faster to changes in the network. Link-state routing is now the preferred routing method for most organizations and Internet service providers.

ISCOM switches support RIP and OSPF dymamic routing protocol. RIP is a kind of Distance-Vector (D-V) algorithm-based protocol and exchanges routing information via UDP packets. Open Shortest Path First (OSPF) is an Interior Gateway Protocol based on the link state developed by IETF.

33.2 Layer 3 routing protocol

The command of ip routing can enable function of forwarding IP packet (IP packet is forbided by default).

	Command	Description
1	**config**	Enter global configuration mode
2	**ip routing**	Enable IP route forwarding function
3	**no ip routing**	Disable IP route forwarding function

Note: before setting the route function such as static routing, dynamic routing, default gateway etc, IP routing forward forwarding must be enabled.

ISCOM L3 switches support Wire Speed and fast route. So it can reduce CPU load. This fast route function adapts to access layer (only need default gateway and several static routing, dynamic routing protocol is unnecessary).

Start and stop fast routing:

step	Command	Description
1	**config**	Enter global configuration mode
2	**ip route fast**	Enable IP fast route function
3	**exit**	Back to privileged EXEC MODE
4	**show ip route hardware**	Show hardware routing table

If the fast routing function is enabled, the command of show ip route hardware can show direct link can be writed to the hardware routing protocol, CPU as the port and switch MAC as the next hop.

In fast routing mode, RIP and OSPF can be enabled. they only send local derect route, but can not learn route (OSPF can learn route but can not be writed to hardware). So it is suggested that RIP and OSPF are disabled.

33.3 static routing

33.3.1 Set default gateway

Support device: ISCOM3000/2800/2900/2000

The gateway is the computer that routes the traffic from a workstation to the outside network. All the packets that fail to find the suitable entry will be forwarded through this default route.

step	Command	Description
1	**config**	Enter global configuration mode
2	**ip default-gateway 192.168.1.1**	Set default gateway
3	**exit**	Back to privileged EXEC MODE

4	**show ip route**	Show ip routing table
5	**config**	Enter global configuration mode
6	**no ip default-gateway**	Cancel default gateway
7	**exit**	Back to privileged EXEC MODE
8	**show ip route**	Show ip routing table

Note: the IP addres of switch must be set first.

33.3.2 Set static routing

When use the command of no ip route, network mask must be specified (expect the default mask). It is must direct for next hop.

Set route aging time:

Command	Description	Command
1	**config**	Enter Global configuration mode
2	**ip route aging-time 100**	Set aging time to 100s

The command of no ip route age can restore the cost to default (180s)

Note: aging time is only useful for host route.

33.4 RIP routing protocol

33.4.1 Introduction to RIP

Routing Information Protocol (RIP) is a relatively simple interior gateway protocol (IGP), which is mainly applied to small scale networks. It is easy to implement RIP. You can configure and maintain RIP more easily than OSPF and IS-IS, so RIP still has a wide application in actual networking.

RIP Operation Mechanism

✧ **RIP basic concepts**

RIP is a kind of Distance-Vector (D-V) algorithm-based protocol and exchanges routing information via UDP packets. It employs Hop Count to measure the distance to the destination host, which is called Routing Cost. In RIP, the hop count from a router to its directly connected network is 0, and that to a network which can be reached through another router is 1, and so on. To restrict the time to converge, RIP prescribes that the cost value is an integer ranging from 0 to 15. The hop count equal to or exceeding 16 is defined as infinite, that is, the destination network or the host is unreachable.To improve the performance and avoid route loop, RIP supports Split Horizon and allows importing the routes discovered by other routing protocols.

✧ **RIP route database**

Each router running RIP manages a route database, which contains routing entries to all the

reachable destinations in the network. These routing entries contain the following information:

- Destination address: IP address of a host or a network.
- Next hop address: The interface address of the next router that an IP packet will pass through for reaching the destination.
- Output interface: The interface through which the IP packet should be forwarded.
- Cost: The cost for the router to reach the destination, which should be an integer in the range of 0 to 16.
- Timer: Duration from the last time that the routing entry is modified till now. The timer is reset to 0 whenever a routing entry is modified.

✧ **RIP timer**

In RFC1058, RIP is controlled by the following timers: Period update, Timeout and Garbage-Collection.

- Period Update is triggered periodically to send all RIP routes to all neighbors.
- If the RIP route is not updated (a router receives the update packets from the neighbor) when the Timeout timer expires, this route is regarded as unreachable. The cost is set to 16.
- If the Garbage-Collection timer expires, and the unreachable route receives no update packet from the same neighbor, the route will be completely deleted from the routing table.
- By default, the values of Period Update and Timeout timers are 30 seconds and 180 seconds respectively. The value of Garbage-collection timer is four times that of Period Update timer: 120 seconds.

RAISECOM support RIPv1 and RIPv2.

33.4.2 Monitor and maintenance

Command

1、show ip route
2、show ip protocol
3、show ip rip statistics

Use show ip route command to view the routing table summary. This command displays routing table information in summary form. Each line represents one route. The contents include destination ddress/mask length, protocol, preference, metric, next hop and output interface. Only current used route, namely, best route, is displayed using show ip route command. One RIP route includes the followings: how the router gets the route (R indicates RIP); Destination address/Mask length; Routing preference and Cost（120/2；Nexthop (via 172.18.1.1).

Example

Raisecom**# show ip route**
Codes: C - connected, G-GateWay S - static, R - RIP, O - OSPF

R 172.18.0.0/255.255.0.0 [120/2] via 172.18.1.1
C 10.0.0.0/255.0.0.0 is directly connected, 10.0.0.1
C 172.17.0.0/255.255.0.0 is directly connected, 172.17.1.1

The information displayed by the show ip protocols command is useful in debugging routing operations. Information in the Routing Information Sources field of the show ip protocols output can help you identify a router suspected of delivering bad routing information.

Example

1、Raisecom**#show ip protocol**
Routing Protocol is 'RIP'
RIP global Enable
Default version control:send version 1, receive any version
RIP supply interval is 30 (default 30)second
RIP router expire interval is 180 (default 180)second
RIP router flush interval is 300 (default 300)second
IF index Send Recv Metric Auth-mode Auth-key State
----------2 1 1 2 1 none UP
3 1 1 2 1 none DOWN

Routing for Networks:
172.18.0.0 0.0.255.255
2.0.0.0 0.0.0.255
Distance(default is 120):120
2、Raisecom**#show ip rip statistics** (view RIP packet)
Num of routes changed :1
Num of responses sent to RIP queries :0
interface 2:
The address of this interface is :172.18.1.1
Num of packets discarded :1
Num of routes discarded :0
Num of triggered updates :1

step	Command	Description
1	Raisecom# **show ip route**	Show ip routing table
2	Raisecom# **show ip protocol**	Show RIP prototol and configuration of the RIP interface
3	Raisecom# **show ip rip statistics**	Show RIP prototol and statistics of the RIP interface

33.4.3 Typical RIP configuration example

Several RIP configuration examples:

Implyment RIP protocol inter-connection

Split Horizon application

Implyment RIP protocol inter-connection

1）topology

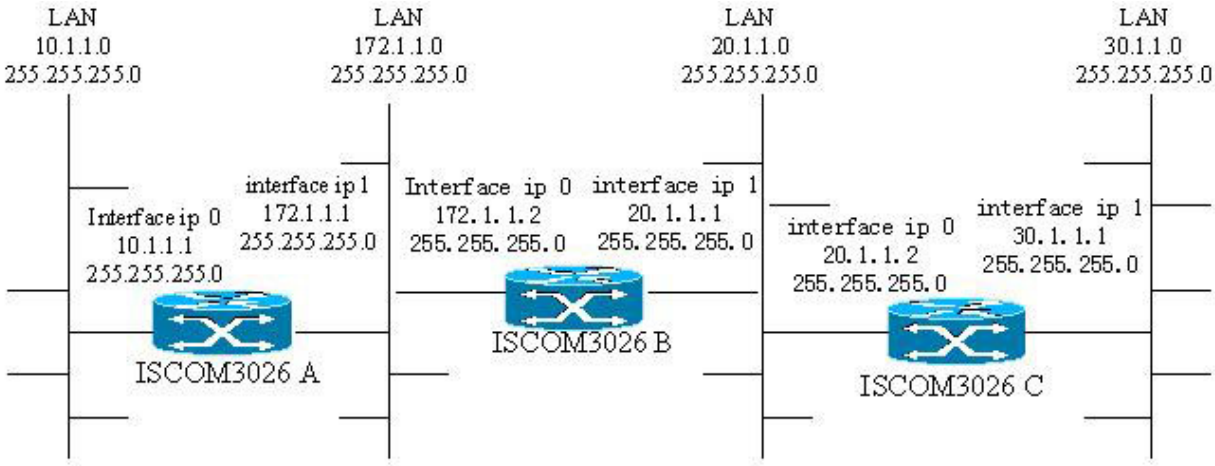


Figure 1 RIP protocol inter-connection

2）configuration

Set ISCOM A

！set port interface 0

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

Raisecom (config-ip)# **ip address** *10.1.1.1 255.255.255.0 1*

！set port interface 1

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

Raisecom (config-ip)# **ip address** *172.1.1.1 255.255.255.0 1*

！set RIP protocol

Raisecom (config)# **router rip**

Raisecom (config-router-rip)# **network** *10.1.1.0 0.0.0.255*

Raisecom (config-router-rip)# **network** *172.1.1.0 0.0.0.255*

Set ISCOM B

！set port interface 0

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

Raisecom (config-ip)# **ip address** *172.1.1.2 255.255.255.0 1*

！set port interface 1

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

Raisecom (config-ip)# **ip address** *20.1.1.1 255.255.255.0 2*

！set RIP 协议

Raisecom (config)# **router rip**

Raisecom (config-router-rip)# **network** *20.1.1.0 0.0.0.255*

Raisecom (config-router-rip)# **network** *172.1.1.0 0.0.0.255*

Set ISCOM C

！set port interface 0

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

Raisecom (config-ip)# **ip address** *20.1.1.2 255.255.255.0 1*

！set port interface 1

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

Raisecom (config-ip)# **ip address** *30.1.1.1 255.255.255.0 2*

！set RIP protocol

Raisecom (config)# **router rip**

Raisecom (config-router-rip)# **network** *20.1.1.0 0.0.0.255*

Raisecom (config-router-rip)# **network** *30.1.1.0 0.0.0.255*

3）view the resault

View ISCOM A

```
 Raisecom#show ip route
Codes: C - Connected, S - Static, R - RIP, O - OSPF
------------------------------------------------------------
C     10.1.1.0[255.255.255.0],is directly connected , Interface 0
R     20.1.1.0[255.255.255.0],Via 172.1.1.2
R     30.1.1.0[255.255.255.0],Via 172.1.1.2
C     172.1.1.0[255.255.255.0],is directly connected , Interface 1
Total route count: 4
```

View ISCOM B

```
 Raisecom#show ip rou
Codes: C - Connected, S - Static, R - RIP, O - OSPF
------------------------------------------------------------
R     10.1.1.0[255.255.255.0],Via 172.1.1.1
C     20.1.1.0[255.255.255.0],is directly connected , Interface 1
R     30.1.1.0[255.255.255.0],Via 20.1.1.2
C     172.1.1.0[255.255.255.0],is directly connected , Interface 0
Total route count: 4
```

View ISCOM C

```
Raisecom#show ip route
Codes: C - Connected, S - Static, R - RIP, O - OSPF
------------------------------------------------------------
R     10.1.1.0[255.255.255.0],Via 20.1.1.1
C     20.1.1.0[255.255.255.0],is directly connected , Interface 0
C     30.1.1.0[255.255.255.0],is directly connected , Interface 1
R     172.1.1.0[255.255.255.0],Via 20.1.1.1
Total route count: 4
```

Split Horizon application

Split horizon means that the route received via an interface will not be sent via this interface again. To some extent, the split horizon is necessary for reducing routing loop. But in some special cases, split horizon must be disabled so as to ensure the correct advertisement of the routes at the cost of efficiency. For example, split horizon is disabled on a NBMA network if it runs RIP.

Split horizon is enabled by default.

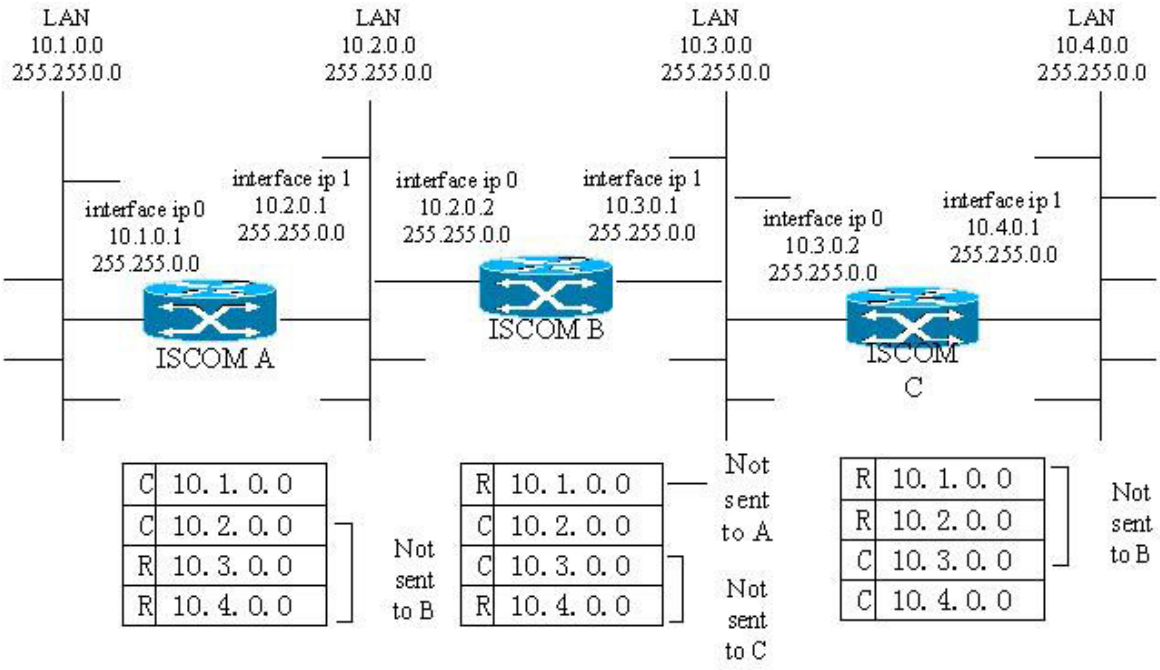


Figure 2 Split Horizon

ISCOM A , ISCOM B and ISCOM C need set interface and RIP.

When the RIP is set, the routing tables are as above. For example as ISCOM B, there are 2 RIP routes in the routing table (10.1.0.0 and 10.4.0.0). 10.1.0.0 route is learned by ISCOM A, so ISCOM B will set the cost as 16 (infinite) and announce to ISCOM A, then stop the announcement. As the same principle, 10.4.0.0 route is learned by ISCOM C, so ISCOM B will set the cost as 16 (infinite) and announce to ISCOM C, then stop the announcement. So the loopback is avoidable.

33.4.4 Troule shooting RIP faults

Symptom: cannot receive the update packets when the physical connection to the peer routing device is normal.

Solution:

1. Use ping command to diagnose whether the link is ok;
2. Use show ip protocols command to show whether RIP operate on the corresponding interface or this interface is not enabled through the network command
3. Check the authentication.
4. Check RIP version.

33.4.5 RIP command reference

Command	Description
router rip	Enable a RIP routing process, which places you in router configuration mode.
network	Associate a network with a RIP routing process.

passive	Only receiving (can not send)
timer update	Set sending dead time of all interfaces
timer invalid	Set receiving dead time of all interfaces
timer flush	Set the unvalide period of all interfaces
distance	Set the distance vector of RIP
ip rip auth-key	Set the password
ip rip auth-mode	Configure the interface to use MD5 digest authentication (or let it default to plain text authentication).
ip rip metric-default	Set the default metric of interface
ip rip receive-version	Accept RIP Version of the interface
ip rip send-version	Send RIP Version of the interface
ip rip split-horizon	Enable split horizon
show ip rip statistics	Show RIP protocol and interface statastics
show ip protocol	Show routing protocol

33.5 OSPF routing protocol

33.5.1 OSPF Overview

Introduction to OSPF

Open Shortest Path First (OSPF) is an Interior Gateway Protocol based on the link state developed by IETF. At present, OSPF version 2 (RFC2328) is used, which is available with the following features:

- ✧ Applicable scope: It can support networks in various sizes and can support several hundreds of routers at maximum.
- ✧ Fast convergence: It can transmit the update packets instantly after the network topology changes so that the change is synchronized in the AS.
- ✧ Loop-free: Since the OSPF calculates routes with the shortest path tree algorithm according to the collected link states, it is guaranteed that no loop routes will be generated from the algorithm itself.
- ✧ Area partition: It allows the network of AS to be divided into different areas for the convenience of management so that the routing information transmitted between the areas is abstracted further, hence to reduce the network bandwidth consumption.
- ✧ Equal-cost multi-route: Support multiple equal-cost routes to a destination.
- ✧ Routing hierarchy: OSPF has a four-level routing hierarchy. It prioritizes the routes to be intra-area, inter-area, external type-1, and external type-2 routes.
- ✧ Authentication: It supports the interface-based packet authentication so as to guarantee the security of the route calculation.
- ✧ Multicast transmission: Support multicast address to receive and send packets.

Process of OSPF Route Calculation

The routing calculation process of the OSPF protocol is as follows:

- ✧ Each OSPF-capable router maintains a Link State Database (LSDB), which describes the topology of the whole AS. According to the network topology around itself, each router generates a Link State Advertisement (LSA). The routers on the network transmit the LSAs among them by transmitting the protocol packets to each others. Thus, each router receives the LSAs of other routers and all these
  LSAs compose its LSDB.
- ✧ LSA describes the network topology around a router, so the LSDB describes the network topology of the whole network. Routers can easily transform the LSDB to a weighted directed graph, which actually reflects the topology architecture of the whole network. Obviously, all the routers get a graph exactly the same.
- ✧ A router uses the SPF algorithm to calculate the shortest path tree with itself as the root, which shows the routes to the nodes in the autonomous system. The external routing information is the leave node. A router, which advertises the routes, also tags them and records the additional information of the autonomous system. Obviously, the routing tables obtained by different routers are different.

Furthermore, to enable individual routers to broadcast their local state information to the entire AS, any two routers in the environment should establish adjacency between them. In this case, however, the changes that any router takes will result in multiple transmissions, which are not only unnecessary but also waste the precious bandwidth resources. To solve this problem, “Designated Router” (DR) is defined in the OSPF.

Thus, all the routers only send information to the DR for broadcasting the network link states in the network. Thereby, the number of router adjacent relations on the multi-access network is reduced. OSPF supports interface-based packet authentication to guarantee the security of route calculation. Also, it transmits and receives packets by IP multicast (224.0.0.5 and 224.0.0.6).

OSPF Packets

OSPF uses five types of packets:

- ✧ Hello Packet

It is the commonest packet, which is periodically sent by a router to its neighbor. It contains the values of some timers, DR, BDR and the known neighbor.

- ✧ Database Description (DD) Packet

When two routers synchronize their databases, they use the DD packets to describetheir own LSDBs, including the digest of each LSA. The digest refers to the HEAD of LSA, which uniquely identifies the LSA. This reduces the traffic size transmitted between the routers, since the HEAD of a LSA only occupies a small portion of the overall LSA traffic. With the HEAD, the peer router can judge whether it already has had the LSA.

- ✧ Link State Request (LSR) Packet

After exchanging the DD packets, the two routers know which LSAs of the peer routers are lacked in the local LSDBs. In this case, they will send LSR packets requesting for the needed LSAs to the peers. The packets contain the digests of the needed LSAs.

- ✧ Link State Update (LSU) Packet

The packet is used to transmit the needed LSAs to the peer router. It contains a collection of multiple LSAs (complete contents).

- ✧ Link State Acknowledgment (LSAck) Packet

The packet is used for acknowledging the received LSU packets. It contains the HEAD(s) of LSA(s) requiring acknowledgement.

LSA Type

I. Five basic LSA types

As mentioned previously, OSPF calculates and maintains routing information from LSAs. RFC2328 defines five LSA types as follows:

- ✧ Router-LSAs: Type-1. Each router generates Router-LSAs, which describe the link state and cost of the local router. Router-LSAs are generated for each area separately and advertised within the associated area only.
- ✧ Network-LSAs: Type-2. DRs on the broadcast network and NBMA network generate Network-LSAs, which describe the link state of the local network. Network-LSAs are broadcast within the area where a DR is located.
- ✧ Summary-LSAs: Include Type-3 and Type-4. Area border routers (ABRs) generate Summary-LSAs. Summary-LSAs are broadcast within the area related to the LSA. Each Summary-LSA describes a route (inter-area route) to a certain destination in other areas of this AS. Type-3 Summary-LSAs describe the routes to networks (the destination is network). Type-4 Summary-LSAs describe the routes to autonomous system border routers (ASBRs).
- ✧ AS-external-LSAs: or ASE LSA, the Type-5. ASBRs generate AS-external-LSAs, which describe the routes to other ASs. AS-external-LSA packets are transmitted to the whole AS (except Stub areas). AS-external-LSAs can also describe the default route of an AS.

II. Type-7 LSA

RFC1587 (OSPF NSSA Option) adds a new LSA type: Type-7 LSAs.

According to RFC1587, Type-7 LSAs differ from Type-5 LSAs as follows:

- ✧ Type-7 LSAs are generated and released within a Not-So-Stubby Area (NSSA). Type-5 LSAs cannot be generated or released within a NSSA.
- ✧ Type-7 LSAs can only be released within an NSSA. When Type-7 LSAs reach an ABR, the ABR can convert part routing information of Type-7 LSAs into Type-5 LSAs and releases the information. Type-7 LSAs cannot be directly released to other areas or backbone areas.

33.5.2 ISCOM switch OSPF configarion

ISCOM switches comply with OSPFv2 stander and support the followings:

- ✧ Stub area: support stub area;
- ✧ Authentication: cleartext and MD5;
- ✧ Interface parameter: output cost, retransmitted, delay, router priority, time interval, dead interval, authentication type, authentication key;
- ✧ VC: virtual conneetion
- ✧ Not-so-stubby-area (NSSA)——RFC 1587；

For OSPF protocol, router is classed inter-area route, Area border router and autonomous system border router.

1, Enabling OSPF

By default, OSPF is disabled.

step	Command	Description
1	**config**	Enter global configuration mode
2	**router ospf**	Enable OSPF

Note: when the ip address is not set, OSPF can not be set.

Disable OSPF protocol: **no router ospf**

2, Specifying an Interface to Run OSPF

After using the **ospf** command to enable OSPF in system view, you must specify the network to run OSPF. An ABR router can be in different areas, while a network segment can only belong to an area. That is, you must specify a specific area for each port running OSPF.

Perform the following configuration in OSPF area view.

step	Command	Description
1	**config**	Enter global configuration mode
2	**router ospf**	Enables OSPF routing, which places you in router configuration mode.
3	**network network-number netmask area area-id**	Defines an interface on which OSPF runs and define the area ID for that interface.

3, Confige OSPF interface parameter

Interface parameter includes hello-interval, dead-interval, authentication and password. The parameter must be consistent for the two ends.

step	Command	Description
1	**config**	Enter global configuration mode
2	**interface ip ifnum**	Enter interface mode
3	**ip ospf cost cost**	Set the interface cost
4	**ip ospf dead-interval seconds**	Sets the number of seconds that a device must wait before it declares a neighbor OSPF router down because it has not received a hello packet.
5	**ip ospf hello-interval seconds**	Specifies the length of time between the hello packets that the Cisco IOS software sends on an OSPF interface.
6	**ip ospf priority priority**	Sets priority to help determine the OSPF designated router for a network
7	**ip ospf retransmit-interval seconds**	Specifies the number of seconds between link-state advertisement (LSA) retransmissions for adjacencies belonging to an OSPF interface.
8	**ip ospf transmit-delay seconds**	Sets the estimated number of seconds required to send a link-state update packet on an OSPF interface.
9	**ip ospf authentication-type { simple-password | message-digest | none}**	Specifies the authentication type for an interface.
10	**ip ospf authentication-password string**	Assigns a password to be used by neighboring OSPF routers on a network segment that is using the OSPF simple password authentication.
11	**ip ospf message-digest-key keyid md5 key**	Enables OSPF MD5 authentication. The values for the *key-id* and *key* arguments must match values specified for other neighbors on a network segment.

Note: dead-interval is 4 times longer than hello-interval. When set the hello-interval, dead-interval increasing as well. But when set dead-interval, hello-interval will not change.

4, confige OSPF area parameter

The network size grows increasingly larger. If all the routers on a huge network are running OSPF, the large number of routers will result in an enormous LSDB, which will consume an enormous storage space, complicate the SPF algorithm, and add the CPU load as well. Furthermore, as a network grows larger, the topology becomes more likely to take changes. Hence, the network will always be in “turbulence”, and a great deal of OSPF packets will be generated and transmitted in the network. This will lower the network bandwidth utility. In addition, each change will cause all the routes on the network to recalculate the route.

OSPF solves the above problem by partition an AS into different areas. Areas are logical groups of routers. The borders of areas are formed by routers. Thus, some routers may belong to different areas. A router connects the backbone area and a non-backbone area is called Area Border Router (ABR). An ABR can connect to the backbone area physically or logically.

The area includes stub area, NSSA area, default route cost of ABR to stub or nssa area and summary route for area.

Stub Area of OSPF

Stub areas are some special areas, in which the ABRs do not propagate the learned external routes of the AS. The stub area is an optional configuration attribute, but not every area conforms to the configuration condition. Generally, stub areas, located at the AS boundaries, are those non-backbone areas with only one ABR. Even if this area has multiple ABRs, no virtual links are established between these ABRs. To ensure that the routes to the destinations outside the AS are still reachable, the ABR in this area will generate a default route (0.0.0.0) and advertise it to the non-ABR routers in the area. Pay attention to the following items when configuring a stub area:

- ✧ The backbone area cannot be configured to be the stub area and the virtual link cannot pass through the stub area.
- ✧ If you want to configure an area to be the stub area, then all the routers in this area should be configured with this attribute.
- ✧ No ASBR can exist in a stub area. In other words, the external routes of the AS cannot be propagated in the stub area.

NSSA Area of OSPF

RFC1587 introduced a new type of area called NSSA area, and a new type of LSA called NSSA LSA (or Type-7 LSA). NSSA areas are virtually variations of Stub areas. They are similar in many ways. Neither of them generates or imports AS-External-LSA (namely Type-5 LSA), and both of them can generate and import Type-7 LSA. Type-7 LSA is generated by ASBR of NSSA area, which can only be advertised in NSSA area. When Type-7 LSA reaches ABR of NSSA, ABR will select whether to

transform Type-7 LSA into AS-External-LSA so as to advertise to other areas.

For example, in the network below, the AS running OSPF comprises three areas: Area 1, Area 2 and Area 0. Among them, Area 0 is the backbone area. Also, there are other two ASs respectively running RIP. Area 1 is defined as an NSSA area. After RIP routes of the Area 1 are propagated to the NSSA ASBR, the NSSA ASBR will generate type-7 LSAs which will be propagated in Area 1. When the type-7 LSAs reach the NSSA ABR, the NSSA ABR will transform it into type-5 LSA, which will be propagated to Area 0 and Area 2. On the other hand, RIP routes of the AS running RIP will be transformed into type-5 LSAs that will be propagated in the OSPF AS. However, the type-5 LSAs will not reach Area 1 because Area 1 is an NSSA. NSSAs and stub areas have the same approach in this aspect.

Similar to a stub area, the NSSA cannot be configured with virtual links.

step	Command	Description
1	**config**	Enter global configuration mode
2	**router ospf**	Enables OSPF routing, which places you in router configuration mode.
3	**area area-id stub [no-summary]**	Defines an area to be a stub area.
4	**area area-id nssa [no-summary]**	Defines an area to be NSSA.
5	**area area-id default-cost cost**	Set the cost of default route from ABR to stub or nssa area
6	**area area-id range ip-address mask [{advertise|not-advertise}]**	Specifies an address range for which a single route will be advertised.

Note: only the inter area routers can establish.

5, Set up and confige Virtual link

According to RFC2328, after the area partition of OSPF, not all the areas are equal. In which, an area is different from all the other areas. Its Area-id is 0.0.0.0 and it is usually called the backbone Area. The OSPF routes between non-backbone areas are updated with the help of the backbone area. OSPF stipulates that all the non-backbone areas should maintain the connectivity with the backbone area. That is, at least one

interface on the ABR should fall into the area 0.0.0.0. If an area does not have a direct physical link with the backbone area 0.0.0.0, a virtual link must be created.

If the physical connectivity cannot be ensured due to the network topology restriction, a virtual link can satisfy this requirement. The virtual link refers to a logic channel set up through the area of a non-backbone internal route between two ABRs. Both ends of the logic channel should be ABRs and the connection can take effect only when both ends are configured. The virtual link is identified by the ID of the remote router. The area, which provides the ends of the virtual link with a non-backbone area internal route, is called the transit area. The ID of the transit area should be specified during

configuration.

The virtual link is activated after the route passing through the transit area is calculated, which is equivalent to a **p2p** connection between two ends. Therefore, similar to the physical interfaces, you can also configure various interface parameters on this link, such as hello timer.

The "logic channel" means that the routers running OSPF between two ABRs only take the role of packet forwarding (the destination addresses of the protocol packets are not these routers, so these packets are transparent to them and the routers forward them as common IP packets). The routing information is directly transmitted between the two ABRs. The routing information herein refers to the Type-3 LSAs generated by the ABRs, for which the synchronization mode of the routers in the area will not be changed.

step	Command	Description
1	**config**	Enter global configuration mode
2	**router ospf**	Enables OSPF routing, which places you in router configuration mode.
3	**area area-id virtual-link router-id [hello-interval hello-interval] [retransmit-interval retransmit-interval] [transmit-delay transmit-delay] [dead-interval dead-interval] [authentication-type {simple-password | message-digest | none}] [authentication-key authentication-key] [message-digest-key message-digest-key md5 md5]**	Establishes a virtual link.

Note: Virtual Link can not transmit stub area. It is established between the two ABR.

33.5.3 Show OSPF protocol

Command	Description
show ip ospf	Show OSPF overview information
show ip ospf database	Displays lists of information related to the OSPF database.
show ip ospf interface	Displays OSPF-related interface information
show ip ospf neighbor [router-id]	Displays OSPF neighbor information on a per-interface basis.
show ip ospf virtual-link	Displays OSPF-related virtual links information.

Show ospf overview

To display general information about Open Shortest Path First (OSPF) routing processes, use the show ip ospf command in EXEC mode.

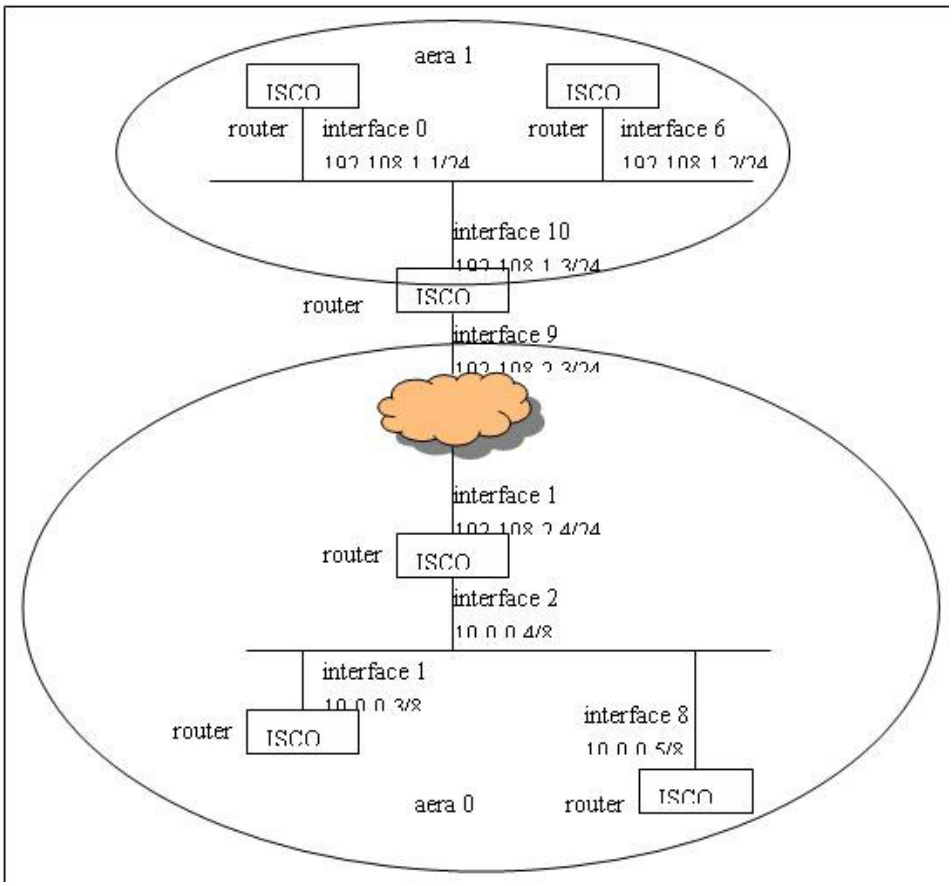
33.5.4 Typical OSPF Configuration Example

Different OSPF configuration example

Virtual link

Different OSPF configuration example

- Network diagram



- Configuration explaination
  - ✓ Confirm the interface of switch area
  - ✓ Enable OSPF
  - ✓ Add interface to area

  Note: **area** *areaid* **stub no-summary** can only be used on ABR of stub. **area** *areaid* **nssa no-summary** can only be used on ABR of NSSA.

- Configuration procedure

Router A
！confige interface 0
Raisecom(config)# **interface ip** *0*
Raisecom (config-ip)# **ip address** *192.108.1.1 255.255.255.0 1*
！confige OSPF
Raisecom (config)**#router ospf**
Raisecom (config-router-ospf)**#network** *192.108.1.0 0.0.0.255* **area** *1*

Router B
！confige interface 6
Raisecom (config)**#interface ip** *6*
Raisecom(config-if)**#ip address** *192.108.1.2 255.255.255.0 2*

！confige OSPF
Raisecom (config)**#router ospf**
Raisecom (config-router-ospf)**#network** *192.108.1.0 0.0.0.255* **area** *1*

Router C－ABR
！confige interface 10
Raisecom (config)**#interface ip** *10*
Raisecom (config-if)**#ip address** *192.108.1.3 255.255.255.0 1*
！confige OSPF
Raisecom (config)**#router ospf**
Raisecom (config-router-ospf)**#network** *192.108.1.0 0.0.0.255* **area** *1*
！confige interface 9
Raisecom (config)**#interface ip** *9*
Raisecom (config-if)**#ip address** *192.108.2.3 255.255.255.0 1*
！confige OSPF
Raisecom (config)**#router ospf**
Raisecom (config-router-ospf)**#network** *192.108.2.0 0.0.0.255* **area** *0*

Router D
！confige interface 1
Raisecom (config)**#interface ip** *1*
Raisecom (config-if)**#ip address** *192.108.2.4 255.255.255.0 1*
！confige OSPF 协议
Raisecom (config)**#router ospf**
Raisecom (config-router-ospf)**#network** *192.108.2.0 0.0.0.255* **area** *0*
！confige interface 2
Raisecom (config)**#interface ip** *2*
Raisecom (config-if)**#ip address** *10.0.0.4 255.0.0.0 2*
！confige OSPF 协议
Raisecom (config)**#router ospf**
Raisecom (config-router-ospf)**#network** *10.0.0.0 0.255.255.255* **area** *0*

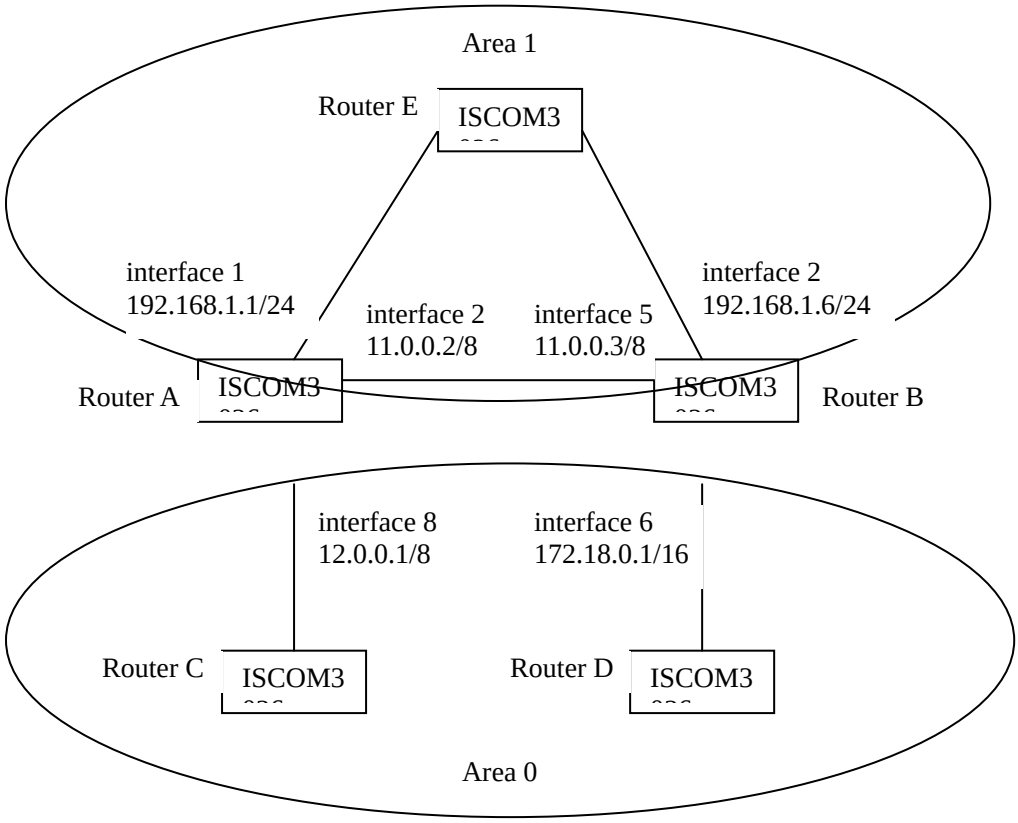
Router E－
！confige interface 1
Raisecom (config)**#interface ip** *1*
Raisecom (config-if)**#ip address** *10.0.0.3 255.0.0.0 1*
！confige OSPF
Raisecom (config)**#router ospf**
Raisecom (config-router-ospf)**#network** *10.0.0.0 0.255.255.255* **area** *0*

Router F
！confige interface 8

Raisecom (config)**#interface ip** *8*
Raisecom (config-if)**#ip address** *10.0.0.5 255.0.0.0 2*
！confige OSPF
Raisecom (config)**#router ospf**
Raisecom (config-router-ospf)**#network** *10.0.0.0 0.255.255.255* **area** *0*

Virtual link configuration example

- Network diagram



- Configuration explaination

There are 4 routers in the topology. If the link between A and B is down, the backbone area will be partitioned, C and D can not communite with each other. If the two routers are ABR, the communication between areas is also been interrupted.

So the best solution is that adding a redundancy link. But maybe the link between C and D can not be established for some reasons. So establish a virtual link will be a middle way.

- Configuration procedure

Router A
！confige interface 1
Raisecom(config)**#interface ip** *1*
Raisecom(config-if)**#ip address** *192.168.1.1 255.255.255.0 1*
！confige interface 8
Raisecom(config)**#interface ip** *8*
Raisecom(config-if)**#ip address** *12.0.0.1 255.0.0.0 4*

！confige interface 2
Raisecom(config)**#interface ip** *2*
Raisecom(config-if)**#ip address** *11.0.0.2 255.0.0.0 3*
！confige OSPF
Raisecom(config)**#router ospf**
Raisecom(config-router-ospf)**#network** *12.0.0.0 0.255.255.255* **area** *0*
Raisecom(config-router-ospf)**#network** *11.0.0.0* 0.*255.255.255* **area** *0*
Raisecom(config-router-ospf)**# network** *192.168.1.0 0.0.0.255* **area** *1*
Raisecom(config-router-ospf)**# area** *1* **virtual-link** *192.168.1.6*

Router B
！confige interface 5
Raisecom(config)**#interface ip** *5*
Raisecom(config-if)**#ip address** *11.0.0.3 255.0.0.0 1*
！confige interface 6
Raisecom(config)**#interface ip** *6*
Raisecom(config-if)**#ip address** *172.18.0.1 255.255.0.0 2*
！confige interface 2
Raisecom(config)**#interface ip** *2*
Raisecom(config-if)**#ip address** *192.168.1.6 255.255.255.0 3*
！confige OSPF
Raisecom(config)**#router ospf**
Raisecom(config-router-ospf)**#network** *11.0.0.0 0.255.255.255* **area** *0*
Raisecom(config-router-ospf)**#network** *172.18.0.0 0.0.255.255* **area** *0*
Raisecom(config-router-ospf)**# network** *192.168.1.0 0.0.0.255* **area** *1*
Raisecom(config-router-ospf)**#area** *1* **virtual-link** *192.168.1.1*

33.5.5 Troubleshooting OSPF Faults

Symptom 1: OSPF has been configured in accordance with the earlier-mentioned steps, but OSPF on the router cannot run normally.

Solution: Check according to the following procedure.

Local troubleshooting: Check whether the protocol between two directly connected routers is in normal operation. The normal sign is the neighbor state machine between the two routers reaches the FULL state. (Note: On a broadcast or NBMA network, if the interfaces for two routers are in DROther state, the neighbor state machines for the two routers are in 2-way state, instead of FULL state. The neighbor state machine between

DR/BDR and all the other routers is in FULL state.

- ✧ Execute the show ip ospf neighbor command to view neighbor s.
- ✧ Execute the show ip ospf interface command to view OSPF information on the interface.
- ✧ Check whether the physical connections and the lower layer protocol operate normally. You can execute the ping command to test. If the local router cannot ping the neighbor router, it indicates that faults have occurred to the physical link and the lower layer protocol.
- ✧ If the physical link and the lower layer protocol are normal, check the OSPF parameters configured on the interface. The parameters should be the same parameters configured on the router adjacent to the interface. The same area ID should be used, and the networks and the masks should also be consistent. (The **p2p** or virtually linked segment can have different

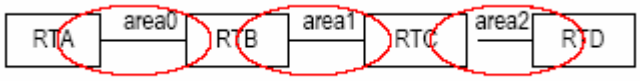
segments and masks.)

- ✧ Ensure that the dead timer on the same interface is at least four times the value of the Hello timer.
- ✧ If the network type is broadcast or NBMA, there must be at least one interface with a priority greater than zero.
- ✧ If an area is set as the stub area, to which the routers are connected. The area on these routers must be also set as the stub area.
- ✧ The same interface type should be adopted for the neighboring routers. If more than two areas are configured, at least one area should be configured as the backbone area (that is to say, the area ID is 0).
- ✧ Ensure that the backbone area is connected to all other areas.
- ✧ The virtual links do not pass through the stub area.

Global troubleshooting: If OSPF cannot discover the remote routes yet in the case that the above steps are correctly performed, proceed to check the following configurations.

- ✧ If more than two areas are configured on a router, at least one area should be configured as the backbone area.

As shown in Figure below: RTA and RTD are configured to belong to only one area, whereas RTB (Area0 and Area1) and RTC (Area1 and Area 2) are configured to belong to two areas. In which, RTB also belongs to area0, which is compliant with the requirement. However, none of the areas to which RTC belongs is Area0. Therefore, a virtual link should be set up between RTC and RTB. Ensure that Area2 and Area0
(backbone area) is connected.



- ✧ The backbone area (Area 0) cannot be configured as the stub area and the virtual link cannot pass through the stub area. That is, if a virtual link has been set up between RTB and RTC, neither Area1 nor Area0 can be configured as a stub area. In the figure above, only Area 2 can be configured as the stub area.
- ✧ Routers in the stub area cannot receive external routes.
- ✧ The backbone area must guarantee the connectivity of all nodes.

Chapter 34 OAM configuration

34.1 OAM Overview

Operations, administration and maintenance (OAM) is a Layer 2 protocol, used to monitor and solve network problems. OAM can report the network state at the data link layer so that a network administrator can manage the network effectively. Currently, OAM is used to solve OAM problems on Ethernet equipment in the last kilometer. It can monitor link performances, monitor faults and generate alarms, test loops, and send remote MIB variable request.

OAM functions:

- **Diagnosing Remote Faults** Ethernet faults are difficult to diagnose, especially in case that network performances decrease gradually when physical communication is not interrupted. OAMPDU defines a flag to allow an OAM entity to send information to the peer. The flag defines emergency link events supported by OAM. Currently, the link fault emergency link event is defined, which occurs when the local end can send data, but cannot receive data. In this case, OAMPDUs are sent once in every second.
- **Link Monitor** Through link monitor, you can detect and find faults in various environments at the data link layer. Link monitor uses event notification PDUs. When a link fault occurs, the local link notifies the OAM entity of the fault after detecting the fault. The following table defines standard link events.
- **Remote MIB Variable Request** A local OAM entity can send a remote MIB request OAMPDU to the remote OAM entity, requesting the remote OAM entity to notify the local end of the current MIB variable. This function can be used to periodically monitor the link state of the remote port.
- **Remote Loopback** A local OAM entity can send a remote loopback OAMPDU to the remote OAM entity, requesting the remote OAM entity to perform loopback. This function can provide necessary help for troubleshooting.

  In the loopback mode, all packets except OAMPDU and pause packets are returned along the way they are sent. Periodical loopback detection can guarantee that current links are smooth. Loopback detection in phases can help you locate specific areas where faults occur.

34.2 OAM configuration

- Enabe and disable OAM port

- ✧ OAM mode configuration
- ✧ Remote Loopback configuration
- ✧ Link Monitor configuration
- ✧ Link Monitor notify configuration
- ✧ Faults indication configuration
- ✧ OAM Variable configuration
- ✧ Clear OAM port statistics
- ✧ Clear OAM port event

34.2.1 Enabe and disable OAM port

step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**oam {disable | enable}**	Enabe or disable OAM
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam**	Show the OAM configuration status

example for OAM: disable port 2

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)#oam disable

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show oam

34.2.2 OAM mode configuration

Since the IEEE link-layer OAM is generally used over a link between a service provider and a customer, it defines two modes for OAM entities: active or passive. The elements of the provider network (e.g. DSLAMs or provider Ethernet switches) operate in active mode, and can exert control over the passive-mode devices (e.g. DSL modems or customer premises

switches). All the OAM port share the mode.

step	Command	Description
1	**config**	Enter global configuration mode
2	**oam {active | passive}**	Enter OAM configuration mode
3	**exit**	Back to privileged EXEC MODE
4	**show oam**	Show the OAM information

Configuration Example

Raisecom#config

Raisecom(config)#oam active

Raisecom(config-port)#exit

Raisecom#show oam

Note:

Only the OAM entity in the active mode can initiate an OAM connection, while the OAM entity in the passive mode can only wait for the connection request sent from the opposite OAM entity.

You cannot establish an OAM connection between two OAM entities in the passive mode.

34.2.3 Remote Loopback configuration

In the loopback mode, all packets except OAMPDU and pause packets are returned along the way they are sent. Periodical loopback detection can guarantee that current links are smooth. Loopback detection in phases can help you locate specific areas where faults occur.

It is enabled by default.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**oam loopback {ignore | process}**	Enable or disable OAM loopback response
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam loopback**	Show the OAM loopback information

Configuration Example

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)#oam loopback ignore

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show oam loopback

Enable remote loopback at center office

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**oam remote-loopback**	Establish remote loopback
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam loopback**	Show the OAM loopback information

Configuration Example

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)#oam remote-loopback

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show oam loopback

Remove remote loopback

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**no oam remote-loopback**	Remove remote loopback
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam loopback**	Show the OAM loopback information

Configuration Example

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:

You can perform remote loopback only after establishing the OAM connection; otherwise the system will give an error prompt.

Remote loopback needs the support of remote hardware. If the remote hardware does not support remote loopback, the system gives a prompt message.

Remote loopback is used to test a single link, so aggregated ports does not support remote loopback. If you enable remote loopback on an aggregated port, the system gives an error prompt. The port in remote loopback is not allowed to join aggregation.

34.2.4 Link Monitor

Through link monitor, you can detect and find faults in various environments at the data link layer. Link monitor uses event notification PDUs. When a link fault occurs, the local link notifies the OAM entity of the fault after detecting the fault. The following table defines standard link events.

Standard link events:

Standard link events	Definition
Error signal event	The number of error signals within a fixed period of time exceeds the defined threshold.
Errored frame event	The number of errored-frames within a fixed period of time exceeds the defined threshold.
Errored frame period event	The number of Errored frames received within the period of N frames exceeds the defined threshold.
Errored frame seconds event	The number of error seconds within M seconds exceeds the defined threshold

802.3 ah does not guarantee that all OAMPDUs can be sent successfully. An event notification OAMPDU should be sent for multiple times to reduce the possibility of losing and a counting sequence number is used to identify an OAMPDU to be sent.

- **Configuring the Interval and Threshold for Detecting Error Frame Events**

By default: Interval 1, Threshold 1

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**oam errored-frame window** <1-60> **threshold** <0-65535>	Configure error frame event window and threshold
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam notify**	Show the OAM envent information

Configuration Example:
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)# oam errored-frame window 2 threshold 8
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam notify

Renew the configuration to default:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**no oam errored-frame**	renew error frame event window and threshold to default
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam notify**	Show the OAM envent information

Configuration Example:
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)# no oam errored-frame
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam notify

- Configuring the Interval and Threshold for Detecting Error Frame Period Events

Dy default: errored-frame-period window 1000ms, Threshold 1 error frame.

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**oam errored-frame-period window** <100-60000> **threshold** <0-65535>	Configure error frame period window and threshold
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam notify**	Show the OAM information

Configuration Example:
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)# oam errored-frame-period window 100 threshold 128
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam notify

Renew the configuration to default:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**no oam errored-frame-period**	renew error frame period window and threshold to default
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam notify**	Show the OAM information

Configuration Example:
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)# no oam errored-frame-period
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam notify

- Configuring the Interval and Threshold for Detecting Error Frame Second Events

By default: Interval 60s, Threshold 1s

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port | line | client} <1-26>	Enter Ethernet physical interface configuration mode
3	oam errored-frame-seconds window <10-900> threshold <0-900>	Configure Error Frame Second Events window and threshold
4	exit	Back to global configuration mode
5	exit	Back to privileged EXEC MODE
6	show oam notify	Show the OAM information

Configuration Example:
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)# oam errored-frame-second window 100 threshold 8
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam notify

Renew the configuration to default:

Step	Command	Description
1	config	Enter global configuration mode
2	interface {port | line | client} <1-26>	Enter Ethernet physical interface configuration mode
3	no oam errored-frame-second	renew Error Frame Second Events to default
4	exit	Back to global configuration mode
5	exit	Back to privileged EXEC MODE
6	show oam notify	Show the OAM information

Configuration Example:
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)# no oam errored-frame-second
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam notify

34.2.5 OAM Link Monitor notify configuration

- OAM notify configuration

By default, when the device detecte the monitor event, it will inform its opposite device with OAM event.

Step	Command	Description
1	**Config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**oam notify {errored-frame-second | errored-symbol-period | erroed-frame | errored-frame-second} {disable | enable}**	Enable or disable OAM monitor event
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam notify**	Show the OAM notify information

Configuration Example:
Raisecom#config
Raisecom(config)#interface port 2
Raisecom(config-port)# oam notify errored-frame-second disable
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show oam notify

- Local link monitor trap configuration

By default, when the device detecte the monitor event, it will not inform management center with SNMP TRAP.

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

2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**oam event trap {disable | enable}**	Enable or disable OAM monitor event to inform management center
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam trap**	Show the OAM trap information

Configuration Example:
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

- Remote link monitor trap configuration

By default, when the device recive remote link monitor event notify, it will not inform management center with SNMP TRAP.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**oam peer event trap {disable | enable}**	Enable or disable OAM monitor event to inform management center in the remote
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam trap**	Show the OAM trap information

Configuration Example:
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

34.2.6 Faults indication configuration

This function is used to notify remote device that there is something wrong with local device, for example link-fault, dying-gasp, temperature and so on. This will result in the faults, such as the link un usable and device reset.
critical-event: link-fault, dying-gasp, temperature
by default, device fault indication is enabled. If there is a fault, the device will notify the remote device with OAM.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**oam notify { | critical-event}**	Enable or disable OAM fault

	{disable | enable}	indication
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam notify**	Show the OAM event information

Configuration Example:
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

34.2.7 OAM variable configuration

OAM variable is a link monitor measure, which allow loacal device to gain variable value of the remote, then know the link states. IEEE802.3 Clause30 specify variable of OAM. Variable is classified by Object, and each Object contains Package and Attribute. Package is composed of Attribute, so Attribute is the basal nuit. All the device support the two kinds of variable gain: OAM information and interface statistics. EPON OLT also supports MPC and OMPEmulation.

When OAM device works as master, the fallowing operation canbe used to gain OAM information and interface statistics.

Step	Command	Description
1	**show oam peer {link-statistic | oam-info} {port-list | client | line} <1-26>**	gain OAM information and interface statistics

Configuration Example:

Raisecom(debug)#show oam peer oam-info port-list 2

34.2.8 Clear OAM interface statistics

OAM protocol can calculate quantity of message at OAM interface. There are many kinds of message: information, link event, loopback, variable request, variable resonse, organization special, unknown type and repeating event information.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**clear oam statistics**	Clear OAM interface statistics
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam statistics**	Show link statistics

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)# clear oam statistics

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show oam statistics

34.2.9 Clear OAM interface event

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface {port | line | client}** <1-26>	Enter Ethernet physical interface configuration mode
3	**clear oam event**	Clear OAM link event note
4	**exit**	Back to global configuration mode
5	**exit**	Back to privileged EXEC MODE
6	**show oam event**	Show local OAM link event note
7	**Show oam peer event**	Show remote OAM link event note

Configuration Example:

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

34.3 monitor and maintenance

34.3.1 View OAM link atate

In privileged EXEC MODE, show oam can show local OAM link configuration and state. The information includes mode configuration, management state, run state, max longness of the massage, configuration version and function. This commade can make user know link configuration and run state 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: Disabled

Max OAMPDU size: 1518

Config revision: 0

Supported functi ons: Loopback, Event, Variable

34.3.2 View remote information

In privileged EXEC MODE, show oam peer can show the remote information of on OAM link, includes MAC address, vendor OUI, vendor information, mode information, max longness of the massage configuration version and function. If the OAM link does't be established, there is no 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

34.3.3 View remote loopback configure

In privileged EXEC MODE, the command of show oam loopback can be used to view remote loopbck information, including state and contral information.

Raisecom#sh oam loopback

Port: 1

Loopback status: Local

Loopback react: Process

Port: 2

Loopback status: No

Loopback react: Ignore

34.3.4 View local event

In privileged EXEC MODE, show oam event can view local device event, including OAM port, time, window, the cost and total event etc.

```
Raisecom#sh oam event
Port: 1
TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredSymbol
Window: 0
Threshold: 0
Value: 0
RunningTotal: 0
EventTotal: 5

TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredFramePeriod
Window: 0
Threshold: 0
Value: 3
RunningTotal: 412,350,956,240
EventTotal: 34096404

TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredFrame
Window: 0
Threshold: 0
Value: 8,628,970,312
RunningTotal: 412,350,956,240
EventTotal: 34096404

TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredFrameSeconds
Window: 0
Threshold: 17,213,965,568
Value: 130,120,368,057,556
RunningTotal: 412,350,956,240
```

EventTotal: 34096404

Port: 2
TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredSymbol
Window: 0
Threshold: 0
Value: 0
RunningTotal: 0
EventTotal: 5

TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredFramePeriod
Window: 0
Threshold: 0
Value: 3
RunningTotal: 412,350,956,240
EventTotal: 34096404

TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredFrame
Window: 0
Threshold: 0
Value: 8,628,970,312
RunningTotal: 412,350,956,240
EventTotal: 34096404

TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredFrameSeconds
Window: 0
Threshold: 17,213,965,568
Value: 130,120,368,057,556
RunningTotal: 412,350,956,240
EventTotal: 34096404

34.3.5 View remote event

In privileged EXEC MODE, show oam event can view remote device event, including OAM port, bring time, window, the cost and total event etc.

Raisecom#sh oam peer event
Port: 1
TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredSymbol
Window: 0
Threshold: 0
Value: 0
RunningTotal: 0
EventTotal: 5

TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredFramePeriod
Window: 0
Threshold: 0

Value: 3
RunningTotal: 412，240
EventTotal: 340964

TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredFrame
Window: 0
Threshold: 0
Value: 8,628,970,312
RunningTotal: 956,240
EventTotal: 346404

TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredFrameSeconds
Window: 0
Threshold: 17,965,568
Value: 130,120，556
RunningTotal: 412,350
EventTotal: 340964

Port: 2
TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredSymbol
Window: 0
Threshold: 0
Value: 0
RunningTotal: 0
EventTotal: 5

TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredFramePeriod
Window: 0
Threshold: 0
Value: 3
RunningTotal: 412,350,956,240
EventTotal: 34096404

TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredFrame
Window: 0
Threshold: 0
Value: 8,628,970,312
RunningTotal: 412,350,956,240
EventTotal: 34096404

TimeStamp: 0 days, 0 hours, 0 minutes
Type:erroredFrameSeconds
Window: 0
Threshold: 17,213,965,568
Value: 130,120,368,057,556
RunningTotal: 412,350,956,240
EventTotal: 34096404

34.3.6 View event information configure

In privileged EXEC MODE, show oam notify can view local OAM link event information and configure, including fault and link monitor. The show information includes event window, threshold and the close instance. For the fault event, there is only close instance.

```
Raisecom#show oam notify
Port: 1
Errored frame period: Enable
Errored frame period window: 100ms
Errored frame period threshold: 128
Errored frame: Enable
Errored frame window: 60s
Errored frame threshold: 0
Errored frame seconds summary: Enable
Errored frame seconds summary window: 100s
Errored frame seconds summary threshold: 16
Dying gasp: Enable
Critical event: Enable

Port: 2
Errored frame period: Enable
Errored frame period window: 1000ms
Errored frame period threshold: 1
Errored frame: Enable
Errored frame window: 1s
Errored frame threshold: 1
Errored frame seconds summary: Enable
Errored frame seconds summary window: 60s
Errored frame seconds summary threshold: 1
Dying gasp: Enable
Critical event: Enable
```

34.3.7 View OAM SNMP TRAP

In privileged EXEC MODE, show oam trap can view the SNMP TRAP information and configuration of OAM, including local event, remote event, found and lose.for the local and remote TRAP, this command can show enable and disable information for TRAP. For the found and lose TRAP, it will show the total TRAP and time.

```
Raisecom#show oam trap
Port: 1
Event trap: Disable
Peer event trap: Disable
Discovery trap total: 5
Discovery trap timestamp: 0 days, 5 hours, 42 minutes
Lost trap total: 1
Lost trap timestamp: 0 days, 5 hours, 42 minutes

Port: 2
Event trap: Disable
Peer event trap: Disable
```

Discovery trap total: 0
Discovery trap timestamp: 0 days, 0 hours, 0 minutes
Lost trap total: 0
Lost trap timestamp: 0 days, 0 hours, 0 minutes

34.3.8 Show OAM port statistic information

In privileged EXEC MODE, show oam statistics can view all the OAM port statistic, including total quantity of supported and Unsupported massage.

```
Raisecom#show oam statistics
Port: 1
                                    Tx              Rx
-------------------------------------
Information                      : 2389          2368
Event notification               : 0             0
Loopback control                 : 0             1
Variable request                 : 0             0
Variable response                : 0             0
Organization specific            : 3             3
Unsupported codes                : 0             0
Duplicate event notification : 0             0

Port: 2
                                    Tx              Rx
-------------------------------------
Information                      : 0             0
Event notification               : 0             0
Loopback control                 : 0             0
Variable request                 : 0             0
Variable response                : 0             0
Organization specific            : 0             0
Unsupported codes                : 0             0
Duplicate event notification : 0             0
```

Chapter 35 Extended OAM configuration

【support devide】
ISCOM2828F/RC551 series
This chapter introduce how to config extended OAM function:

- extended OAM function overview
- extended OAM function configuration
- monitor and maintanance

35.1 extended OAM function overview

Extended OAM, using IEEE802.3ah OAM to manage and monitor the remote device. It is composed by 3 parts:

1. Get the attribute of remote device;

2. Upload and down file of remote device;

3. Manage extended OAM link state and statistic.

Extended OAM includes the followings:

- ✓ Get remote attribute: the extended OAM attribute can be used to get the remote attribute form the center site.
- ✓ Set remote device: config the remote device, including host name, enable and disable port, duplex, bandwidth, fault transfer etc.
- ✓ Set remote device nettwork management parameter: can config remote device network management parameter, such as ip address, gateway, community parameter and management VLAN etc, then implement full management with SNMP protocol.
- ✓ Remote TRAP: when the port of remote device show LINK UP/DOWN, the remote device will send extended OAM notification fram to inform the center site, then the center device will send TRAP.
- ✓ Extended remote loopback: the remote optical port can be set loopback function, the function of whether to count repeatedly can be set.
- ✓ Reset remote device: send command to reset remote device.
- ✓ Other remote device function management: with the increasing of remote device, center device can manage more remote device with extended OAM function such as: SFP、Q-in-Q、Virtual Circuit diagnosis etc.
- ✓ Download remote file: the remote can get remote file from FTP/TFTP server. The file also can be send from the server to center device, then the remote device can get from the center device.
- ✓ Upload remote file: put the file to FTP/TFTP server, or from the remote device to center one, then put to server from the center device.
- ✓ Link statistic and management of extended OAM function.

Note: extended OAM link can only be established between center and remote site. The devices of two end must be set to master and passive, or the link can’t be up.

35.2 extended OAM configuration

Extended OAM configuration guid

Set port of remote device

Set SNMP community and IP address of remote device.

Set Q-in-Q configuration

Reset remote device

Stop and start extended loopback function

Enforce diagnosis remote link

Center device get file from server

Center device put file to server

Remote device get file from server

Remote device put file to server

Remote device get file from center device

Remote device put file to center deivce

Clear extended OAM link statistic information

Enable and disable extended OAM

Open and close trap

Enable and disable power configuration

35.2.1 Extended OAM configuration guide

Configure remote device at center office. Enter remote configuration mode

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configure mode

Configure remote device port. Then enter the remote port mode.

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configure mode
interface client *client-id*	Enter remote physical configure mode

35.2.2 Set remote device system configuration

Set remote device system configuration, including host name, mtu, save and delete configuration file (the confige file can be saved and deleted, not the operation to center device).

Set remote host name:

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
hostname *HOSTNAME*	Set host name

Set the mtu, the value is different according to the remote device. Such as: for the RC512-GE, the mtu can be 1916 or 1536. So if the value is is less than 1916, efficient value will be 1536, or it will be 1916.

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
system mtu *<1500-8000>*	Set the mtu

In remote configuration mode, the command of show remote-device information can view host name and really mtu of the remote device.

Save the configuration:

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
write	Save file

Delete the configuration:

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode

remote-device	Enter remote configuration mode
erase	Delete remote file

When delete the remote configuration file, it is need to be confirmed.

Save and delete file will need a long time. So the OAM link may be down when perform this operation.

35.2.3 Set port configuration of the remote device

The configuration includes enable/disable port, duplux, speed, flow control and the discrabe.

Disable port:

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
interface client *client-id*	Enter physical mode
shutdown	Disable port

no shutdown will enable port

Set speed and duplux:

Command	Description
Config **interface {port | line | client}** *portid*	Enter global configuration mode Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
interface client *client-id*	Enter physical port mode
speed {auto | 10| 100 |1000 } **duplex** { full | half }	Set speed and duplux

For a 1000M optical port, can set auto negotiation:

Command	Description
Config **interface {port | line | client}** *portid*	Enter global configuration mode Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
line-speed auto	Set optical auto negotiation

disable optical auto negotiation: no line-speed auto

Enable/disable flowcontrol:

Command	Description
Config **interface {port | line | client}**	Enter global configuration mode Enter Ethernet physical interface

portid	configuration mode
remote-device	Enter remote configuration mode
interface client *client-id*	Enter physical port mode
flowcontrol { **on** | **off** }	Enable/disable remote port flow control

Set the bandwidth of inbound:

Command	Description
Config **interface {port | line | client}** *portid*	Enter global configuration mode Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
rate-limit line *line-id* **ingress** *rate* **rate-limit client** *client-id* **ingress** *rate*	the bandwidth of inbound

Recover: no rate-limit line *line-id* ingress, no rate-limit client *client-id* ingress

Set the bandwidth of outbound:

Command	Description
Config **interface {port | line | client}** *portid*	Enter global configuration mode Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
rate-limit line *line-id* **egress** *rate* **rate-limit client** *client-id* **ingress** *rate*	Set the bandwidth of outbound:

Recover: no rate-limit line *line-id* egress, no rate-limit client *client-id* egress

Set discrabe information:

Command	Description
Config **interface {port | line | client}** *portid*	Enter global configuration mode Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
description line *line-id WORD* **description client** *client-id WORD*	Set discrabe information

In remote configuration mode,delete discrabe: no description line line-id,description client client-id WORD

35.2.4 Set SNMP Community and IP address

Set community name and popedom:

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
snmp-server community *community-name* **{ ro | rw}**	Set community name and authority community-name community name • ro read only • rw write only

Detele community name no snmp-server community community-name

Set remote device IP address:

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
ip addreass *ip-address [ip-mask] vlan-list*	Set IP address • *ip-address* IP address • *ip-mask* mask • *vlan-list* manage VLAN list

When set IP address, VLAN is needed.

Delete VLAN: no ip addreass *ip-address*

View community name and IP address: show remote-device information

35.2.5 Q-in-Q configuration

Selectivity Q-in-Q configuration includes: switching, TPID, native VLAN and access port.

Set the switch-mode to transparent (other configurations are not valid):

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
switch-mode transparent	Set the mode to transparent

When the switch-mode is Dot1q VLAN (single TAG),the native VLAN and access port will be valid.

The packet without tag will be taded. Or else, it will be transparent.

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
switch-mode dot1q-vlan native-vlan *<1-4094>* **[line]**	Set the mode to Dot1q VLAN • *<1-4094>* VLAN ID; line omit line will be access port

Set the switch-mode to Double tagged VLAN: TPID, native VLAN and access port is vlaid at this mode.

In Double tagged mode, the packet will be tagged no matter there is tag exist.

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
switch-mode double-tagged-vlan [tpid *HHHH***] native-vlan** *<1-4094>* **[line]**	Set the mode to Double tagged • **native-vlan native** VLAN; • *<1-4094>* VLAN ID; • **line** as access port • **tpid** **ourter** TPID • *HHHH* outer TPID, hex, from 0000 to FFFF If there is no tpid, indicate the outer TAG TPID is 0x9100

View remote device selectivity Q-in-Q: show remote-device information

35.2.6 Reset remote device

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
reboot	Reset remote device

This operation is needed to be conformed.

OAM link will be down when the device reset and restart.

35.2.7 Start and stop extended loopback

Perform loopback function will influence the data.

When start the loopback, CRC will be calculate again.

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
inside-loopback [crc-recalculate]	Start remote local loopback • **crc-recalculate** recalculate CRC。

Stop loopback: no inside-loopback

View the state and parameter: show inside-loopback

35.2.8 Diagnose remote link

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
test cable-diagnostics	Implyment remote device link diagnosis

view the result of device link diagnosis.

35.2.9 Clear extended OAM link

the extended OAM includes: get and response variable, set and responsevariable, file request and response, information etc.

Command	Description
Config	Enter global configuration mode
clear extended-oam statistics [port-list *port-list***]** **clear extended-oam statistics [line-list** *line-list***]** **clear extended-oam statistics [client-list** *client-list***]**	Clear extended OAM link statistics

35.2.10 Enable and disable OAM information

Enable and disable the device to send OAM notification frame. This function can send LINK UP/DOWN information to center device. but if it is disabled,OAM notification will not be sent.

Command	Description
Config	Enter global configuration mode
extendeded-oam notification {enable| disable}	Enable/disable send OAM notification frame

35.2.11 Open and close the trap

If the trap function is disabled, the trap will not be sent to SNMP management when there are OAM notification frame. but if trap function is enabled, the trap will be send.

Command	Description
Config	Enter global configuration mode
snmp trap remote {enable| disable}	Open/close trap

view trap configuration:show snmp trap remote

35.2.12 Get file from server

The system bootroom file, startup file, startup configration file and FPGA file of remote device can be downloaded from server to remote device (center device as the relay). This function can be started by center device or remote device, and multiple remote devices can be upgraded at the same time.

Center device starts, download from FTP/TFTP server:

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
download { bootstrap | system-boot | startup-config | fpga } ftp *A.B.C.D USRNAME PASSWORD FILENAME*	Download from FTP server to remote device • A.B.C.D IP address of server • USRNAME ftp server username • PASSWORD ftpserver password • FILENAME file name on server
download { bootstrap | system-boot | startup-config | fpga } tftp *A.B.C.D FILENAME*	Download file from TFTP server to remote device • *A.B.C.D* IP address of server • *FILENAME* file name on server

Remote device starts, download from FTP/TFTP server:

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
download { bootstrap | system-boot | startup-config | fpga } ftp *A.B.C.D USRNAME PASSWORD FILENAME*	Download from FTP server to remote device • A.B.C.D IP address of server • USRNAME ftp server username • PASSWORD ftpserver password • FILENAME file name on server
download { bootstrap | system-boot | startup-config | fpga } tftp *A.B.C.D FILENAME*	Download file from TFTP server to remote device • *A.B.C.D* IP address of server • *FILENAME* file name on server

View command: dir.

Delete command: erase

35.2.13 Upload file from remote device to server

The system startup file and configration file can be uploaded from remote device to server (center device as the relay). This function can be started by center device or remote device, but multiple remote devices can not be sent at the same time.

Center device starts, download from FTP/TFTP server:

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
upload {startup-config | system-boot } ftp *A.B.C.D USRNAME PASSWORD FILENAME*	Upload file from remote device to TFTP server • A.B.C.D IP address of server • USRNAME ftp server username • PASSWORD ftpserver password • FILENAME file name on server

upload {startup-config | system-boot } tftp *A.B.C.D FILENAME*	Upload file from remote device to TFTP server • A.B.C.D IP address of server • FILENAME file name on server

Remote device starts, download from FTP/TFTP server (center device as the relay):

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
upload {startup-config | system-boot } ftp *A.B.C.D USRNAME PASSWORD FILENAME*	Upload file from remote device to FTP server • A.B.C.D IP address of server • USRNAME ftp server username • PASSWORD ftpserver password • FILENAME file name on server
upload {startup-config | system-boot } tftp *A.B.C.D FILENAME*	Upload file from remote device to TFTP server • A.B.C.D IP address of server • FILENAME file name on server

35.2.14 Download file to center device

The system bootroom file, startup file, startup configration file and FPGA file of remote device can be downloaded from server to remote device (center device as the relay), utilizing FTP and TFTP protocol, save the file in the FLASH.

When the file is saved, it will attach suffix. So it is needn't specify suffix (the name can not be same as the exist file).

Download file from from server to center device:

Command	Description
download {remote-bootstrap | remote-system-boot | remote-startup-config | remote-fpga } ftp *A.B.C.D USRNAME PASSWORD FILENAME LOCAL-FILENAME*	• A.B.C.D IP address of server • USRNAME ftp server username • PASSWORD ftpserver password • FILENAME file name on server *LOCAL-FILENAME* file name which is saved by center device.

download { remote-bootstrap | remote-system-boot | remote-startup-config | remote-fpga } tftp *A.B.C.D FILENAME LOCAL-FILENAME*	• A.B.C.D IP address of server • FILENAME file name on server *LOCAL-FILENAME* file name which is saved by center device.

View command: dir.

Delete command: erase

35.2.15 Upload file from center device to server

Utilizing FTP/TFTP:

Command	Description
upload {remote-bootstrap | remote-system-boot | remote-startup-config | remote-fpga } ftp *A.B.C.D USRNAME PASSWORD FILENAME LOCAL-FILENAME*	• A.B.C.D IP address of server • USRNAME ftp server username • PASSWORD ftpserver password • FILENAME file name on server *LOCAL-FILENAME* file name which is saved by center device.
upload { remote-bootstrap | remote-system-boot | remote-startup-config | remote-fpga } tftp *A.B.C.D FILENAME LOCAL-FILENAME*	• A.B.C.D IP address of server • FILENAME file name on server LOCAL-FILENAME file name which is saved by center device.

35.2.16 Download file from center device to remote device

The file in flash of center device, can be downloaded from OAM protocol. This function can be started by center device or remote device. If the center device starts, multiple devices can be upgraded at the same time.

Center device starts, download from remote device:

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
download { bootstrap | system-boot | fpga } *FILENAME*	Download bootroom file, startup file and FPGA file from center site to remote device
download startup-config [*FILENAME***]**	Download configuration file from center site to remote device

Remote device starts, download from center device.

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
download { bootstrap | system-boot | fpga } *FILENAME*	Download bootroom file, startup file and FPGA from center device to remote device • *FILENAME* file name on center device
download startup-config [*FILENAME***]**	Download file from center device to remote device • *FILENAME FILENAME* file name on center device

View command: dir.

Delete command: erase

35.2.17 Upload file from remote device to center device

System startup file and startup configuration file of remote device can be uploaded to center device utilizing extended OAM. This function can be started by center device or remote device, but multiple remote devices can not be sent at the same time.

Center device starts, download from remote device:

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
upload system-boot *FILENAME*	Upload file from remote device to center • *FILENAME* file name on center device
upload startup-config	Upload file from remote device to center

Remote device starts, upload file to FTP/TFTP server.

Command	Description
Config **interface {port | line | client}** *portid*	Enter global configuration mode Enter Ethernet physical interface configuration mode

upload system-boot *FILENAME*	Upload file from remote device to center • *FILENAME* file name on center device
upload startup-config	Upload file from remote device to center

View command: dir.

Delete command: erase

35.2.18 Enable/disable power on configuration request

The remote device such as RC551, can be set whether to be configged when power on.

Command	Description
Config	Enter global configuration mode
extended-oam config-request {enable| disable}	Enable/disable power on configuration request

View power on configuration request: show extended-oam status

35.2.19 Save the remote configuration to center device

When the RC552 as the remote device, the configuration file doesn't be save at local. The command of write local will save the file to center cevice. When the center device is restarted, it will load RC552 configuration. If there is configuration request from remote device, it will send the new configuration.

Command	Description
Config	Enter global configuration mode
interface {port | line | client} *portid*	Enter Ethernet physical interface configuration mode
remote-device	Enter remote configuration mode
write local	Save the remote configuration to center FLASH

Is there is no configuration file of RC552, also no configuration have been sent, this command will not be vilaid.

It is a long time to save the file to FLASH, so OAM link maybe down at this time.

35.3 Monitor and maintaince

Command	Description
show interface port	Show port information
show interface port detail	Show port information in detail
show interface port statistics	show interface port statistics
show oam capability	show oam function support capability
show remote-device information	Show remote device information
show sfp	remote-device SFP information

show cable-diagnostics	Show the result of link diagnostics
show inside-loopback	Show the state and parameter of remote loopback
show extended-oam statistics	Show extended OAM statistics
show extended-oam status	Show extended OAM link state statistics
show snmp trap remote	Show whether the trap is enabled

北京瑞斯康达科技发展有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road, Haidian District, Beijing Postcode: 100085 Tel: +86-10-82883305 Fax: +86-10-82883056 Email: export@raisecom.com http://www.raisecom.com