RAISECOM

Raisecom ISCOM Series Switch Configuration Guide

Software version—ROS 3.0

Raisecom Technology Co. Ltd.

(10/2005)

Contents

1. Overview 8

1.1. Audience 8
1.2. Abbreviation 8
1.3. Reference 8

2. Summary 9

2.1. layter-2 static management and hardware assistant function 9
2.2. Stardard layer 2 protocol 9
2.3. Management function 9
2.4. DHCP 9
2.5. Bandwidth management 9
2.6. Layer 3 function 9

3. How to use command-line 10

3.1. Environment 10
3.2. Command line mode 10
3.3. Get help 11
3.4. Use history commands 11
3.5. Editing properties 12

4. System command configuration 13

4.1. Basic system command and configuration 13
4.2. Configuration files and boot files management 13
4.2.1. configuration files 13
4.2.2. Startup files 13
4.3. User management 13

5. Mirror function configuration 14

5.1. Enable or disable mirror function 14
5.2. Configure the monitor port 14
5.3. configure the source port. 15
5.4. Example 16

6. Port rate limiting configuration 17

6.1. Configure the port bandwidth 17
6.2. Example 17

7. MAC address table manangement 19

7.1. Configure the aging time of MAC address 19
7.2. Confiugre static MAC address 20
7.3. Enable/disable the MAC address learning function 20
7.4. Delete MAC address table. 21
7.5. Show MAC address table. 21
7.6. Search particular MAC address. 22

8. Physical interface configuration 23
8.1. Configure the speed and duplex mode of the port. 23
8.2. Configure the 802.3x flow control function of the port 24
8.3. Open/shutdown the port 24
9. Strom control 26
9.1. Enable the control function 26
9.2. Threshold of strom control 26
10. Shared VLAN 28
10.1. Enable SVL 28
10.2. Configure SVL of port 28
10.3. Configure SVL default VLAN 29
11. Packet transparent transmission 30
11.1. Overview 30
11.2. Configure packet transparent transmission 30
11.3. Forward DLF packets 30
12. The layer-3 interface configuration 32
13. Link Aggregation Control Protocol 33
13.1. About link aggregation control protocol (LACP) 33
13.2. Command description 33
13.2.1. Enable or disable trunk LACP function 33
13.2.2. Add or delete trunk group 33
13.2.3. Set load sharing mode 33
13.3. Maintenance 34
14. RSTP configuration 35
14.1. About RSTP 35
14.2. RSTP configuration list 35
14.3. Step by step introduction 35
14.3.1. RSTP globally enable and disable 35
14.3.2. RSTP switch priority setting 36
14.3.3. RSTP Hello Time setting 36
14.3.4. RSTP Max Age setting 36
14.3.5. RSTP Forward Delay setting 37
14.3.6. Switch RSTP running mode 37
14.3.7. the maximum packets sent within hello time 38
14.3.8. RSTP port enable and disable 38
14.3.9. RSTP port priority setting 38
14.3.10. The path cost configuration 39
14.3.11. RSTP edge port setting 39
14.3.12. Setting of RSTP port link 40
14.3.13. Force the urrent Etherent port in RSTP mode 40

14.3.14. Clear RSTP port statistical information 41
14.4. Mornitoring 41
15. DHCP configuration 43
15.1. DHCP Relay configuration 43
15.2. DHCP Relay protocol introduction 43
15.3. DHCP Relay configuration task list 43
15.4. DHCP Relay configuration 43
15.4.1. Start and stop DHCP Relay 43
15.4.2. Server address configuration 44
15.4.3. Monitor and maintenance 44
15.5. DHCP Relay trouble shooting 46
15.5.1. DHCP Relay command reference 46
15.6. DHCP Server configuration 46
15.6.1. DHCP Server protocol introduction 46
15.6.2. DHCP Server configuration task list 46
15.6.3. the start and stop of DHCP Server 47
15.6.4. address pool configuration. 47
15.6.5. lease time configuration for lease table 48
15.6.6. Neighbouring DHCP Relay address configuration 49
15.7. Monitor and maintenance 50
15.7.1. typical configuration example 51
15.7.2. DHCP Server touble shooting 55
15.7.3. DHCP Server command reference 55
16. IGMP SNOOPING configuration 56
16.1. IGMP Snooping function configuration 56
16.2. About IGMP Snooping protocol 56
16.3. IGMP snooping configuration list 56
16.3.1. IGMP Snooping enable and disable 56
16.3.2. IGMP Snooping aging time configuration 57
16.3.3. router port configuration 58
16.3.4. immediate-leave function setting: 58
16.3.5. manual configuration of multicast MAC address table 59
16.4. monitor and maintenance 60
16.5. IGMP Snooping trouble shooting 61
16.6. IGMP Snooping command reference 61
17. RMON configuration 62
17.1. RMON Introduction 62
17.2. RMON configuration 62
17.3. show RMON configuration information and the result 65
18. ARP 66
18.1. ARP address table introduction 66
18.2. ARP setting 66

18.2.1. add static ARP address 66
18.2.2. delete ARP address mapping term: 67
18.2.3. Set the timeout of ARP dynamic address mapping terms. 67
18.2.4. clear ARP address mapping table 67
18.3. Show ARP address mapping table 67
19. SNMP configuration 68
19.1. SNMP protocol introduction 68
19.2. SNMP configuration 68
19.2.1. Configure SNMP user 68
19.2.2. Access priority configuration 69
19.2.3. TRAP configuration 72
19.3. Other configuration 73
19.4. Show SNMP configuration information 74
20. Cluster management 75
20.1. Cluster introduction 75
20.2. Cluster management configuration list 76
20.2.1. Globally enable RNDP 76
20.2.2. RNDP port enable 77
20.2.3. RTDP enable 77
20.2.4. RTDP collection range 78
20.2.5. Enable and disable of cluster management 78
20.2.6. Automaticly active function enable 78
20.2.7. add and active cluster member 79
20.2.8. delete cluster member 80
20.2.9. Cluster member suspend 81
20.2.10. add and suspend all the candidate member 81
20.2.11. Cluster member remote management 82
20.3. Monitoring and maintenance 83
20.3.1. RNDP neighbour information display 83
20.3.2. RTDP device information display: 83
20.3.3. Display cluster management informaiton 84
21. System log configuration 85
21.1. System log introduction 85
21.2. System log configuration 85
21.2.1. The enable and disable for system log 85
21.2.2. The time mark setting of log information 86
21.2.3. log rate configuration 86
21.2.4. Log information output configuration 86
21.2.5. show log configuration 87
22. System clock 88
22.1. System clock 88
22.1.1. SNTP synchronized time 88

22.1.2. Manually configure system time 88
22.1.3. Set summer time 89
23. Loopback detection 91
23.1. Detection method 91
23.2. loopback detection function configuration 91
24. Schedule-list configuration 93
24.1. The setting for schedule-list 93
24.2. Schedule-list configuration based on command line 93
25. Trouble shooting command 94
25.1. trouble shooting 94
25.1.1. Memory usage information 94
25.1.2. Port driving pool usage information 94
25.1.3. Process and stack status 95
25.1.4. UP/DOWN statistical information 96
25.1.5. Information gathering for trouble shooting 97
26. VLAN Configuration 98
26.1. VLAN introduction 98
26.2 VLAN member port mode 99
26.2. VLAN configuration list 99
26.2.1. Create and delete VLAN 99
26.2.2. VLAN name settings: 100
26.2.3. VLAN active status settings 100
26.2.4. VLAN mode of port and relevant attributes setting 101
26.2.5. Monitor and maintenance 106
27. Port Statistics 107
27.1. Introduction to port statistics 107
27.2. Port statistics configuration 107
27.3. Monitor and maintenance 107
28. ACL and network security setting 109
28.1. ACL introduction 109
28.2. configure ACL 109
28.3. use ACL at second layer physical interface or on the VLAN 117
28.4. Use ACL on third layer interface 119
29. QoS Configuration 121
29.1. QoS Introduction 121
29.1.1. Classification 123
29.1.2. Policying and marking 124
29.1.3. Mapping table 125
29.1.4. Queueing and scheduling 125
29.2. Configure QOS list 126

29.2.1. QOS Default setting 126
29.2.2. QOS enable and disable 127
29.2.3. Configure QoS trust status and CoS default value 127
29.2.4. Configure QoS mapping table: 128
29.2.5. Configure the class map of QoS 135
29.2.6. configure QoS policy map 137
29.2.7. configure QoS flow classification 137
29.2.8. Apply the policy on the port 141
29.2.9. Set the scheduling mode for egress queue 141
29.3. QOS monitor and maintenance 142
29.3.1. Show QOS enable information 143
29.3.2. show QOS policer information 143
29.3.3. show QOS map information 143
29.3.4. show QOS queue information 144
29.3.5. show QOS port information 145
29.3.6. show QOS class-map information 146
29.3.7. Show QOS policy-map information 146
29.3.8. Show QOS policy-map application information 147
29.4. QOS trouble shooting: 147
29.5. QOS command reference 147
30. MVR configuration 150
30.1. About MVR 150
30.2. IGMP filter introduction 151
30.3. Configure MVR function 151
30.3.1. MVR default configuration 151
30.3.2. MVR global configuration 151
30.3.3. Configure MVR port information 153
30.3.4. MVR monitor and maintenance 154
30.4. Configure IGMP filter table 155
30.4.1. IGMP filter default configuration 156
30.4.2. profile configuration 156
30.4.3. Apply IGMP profile 157
30.4.4. The maximum port number configuration 158
30.4.5. The monitor and maintenance of IGMP filtering 159
30.5. Typecial configuration for MVR application 160
30.6. Trouble shooting of MVR and IGMP filtering 161
30.7. MVR and IGMP filter command reference 161

1. Overview

1.1. Audience

The *Raisecom series Switch Software Configuration Guide* is for the network manager responsible for configuring the ISCOM series switches. This guide provides information about configuring and troubleshooting a switch or switch clusters. It includes descriptions of the management interface options and the features supported by the switch software.

1.2. Abbreviation

GARP: Generic Attribute Registration Protocol
GVRP: GARP VLAN Registration Protocol
GMRP GARP Multicast Registration Protocol
LACP: Link Aggregation Control Protocol
STP: Spanning Tree Protocol
VLAN: Virtual LAN
DHCP: Dynamic Host Configuration Protocol
BOOTP: BOOTSTRAP PROTOCOL
IGMP Internet Group Management Protocol
QoS: Quality of Service
CoS: Class of Service
ToS: Type of Service
DSCP: Differentiated Services Code Point
WRR: Weighted Round Robin
CIDR Classless Inter Domain Routing
EGP: Exterior Gateway Protocol
ICMP: Internet Control Message Protocol
IGP: Interior Gateway Protocol
InARP: Inverse ARP
MBZ: Must be Zero
MIB: Management Information Base
OSPF: Open Shortest Path First
PDU: Protocol Data Unit
RIP: Routing Information Protocol
MVR: Multicast VLAN registration

1.3. Reference

1 < RAISECOM ISCOM Series Switch Command Reference >

2. Summary

2.1. layter-2 static management and hardware assistant function

1 Port mirror(any port to any port);
2 Storm-control, provide the control for broadcast, multicast and DLF frame control
3 The static management for the ARL table of the switch (capacity is 8K).

2.2. Stardard layer 2 protocol

1 802.1w fast spanning tree protocol;
2 802.1D/W,802.1Q;
3 IGMP Snooping(multicast address:256);

2.3. Management function

1 Support cluster management function;
2 Support SNMP(RFC1157),SNMP V2 and SNMPV3;
3 Support CONSOLE management;
4 Support remote management by TELNET;
5 Support automaticly control function, that is it can download configuration file automaticly from network configuration server, finish the configuration.
6 Support rmon 1,2,3,9 group;

2.4. DHCP

Configure DHCP SERVER and DHCP RELAY function (three layer support) after authentication.

2.5. Bandwidth management

Bandwidth management based on the port.

2.6. Layer 3 function

1 Support static route;
2 8k route table as the maximum;
3 Support the wire speed transfer for the third layer data traffic.

3. How to use command-line

3.1. Environment

Software requirement: ROS 3.0.

3.2. Command line mode

Mode	Mode description	Access	Prompt
User EXEC	To connect the remote device, change terminal settings on a temporary basis, perform basic tests, and display system information.	Login	Raisecom>
Privileged EXEC	In this mode, user can configure the basic information of a switch.	From User EXEC mode, type **enable** and password	Raisecom#
Global configuration mode	Use this command to configure parameters that apply to the whole switch.	From Privileged EXEC mode type **config.**	Raisecom(config)#
Physical interface configuration mode.	Configure parameters of physical Ethernet interface.	From global configuration mode mode type **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 mode type **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	Config parameters of particular data flows in this mode.	From global configuration mode mode, type **class-map** class-map-name **[match-all | match-any]** command.	Raisecom(config-cmap)#
Policy Map configuration mode	Config the data flow of class-map defined encapsulation and classification.	From global configuration mode mode, type **policy-map** policy-map-name command.	Raisecom(config-pmap)#
Traffic classification config mode	Config the data flow under this mode.	From policy map exec mode, type **class-map** class-name command.	Raisecom(config-pmap-c)#
Cluster configuration mode	Config the cluster under this mode.	From global configuration mode mode, type **cluster** command.	Raisecom(config-cluster)#
ACL config mode	Config ACL filtering table	From global configuration mode mode, type access-list-map <0-399> {permit | deny} command.	Raisecom(config-aclmap)#

3.3. Get 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 a incompleted 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 ?**

3.4. Use history commands

Switch will record 20 history commands by default. User can use Raisecom>**terminal history** <*0-20*> command to comfigure the recorded historical

command count.

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

3.5. Editing properties

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 on the right side the cursor
Ctrl+w:	delete all the characters on the left side of the cursor
Ctrl+u:	delete the row all
Ctrl+z:	exit from other modes to privileged mode

4. System command configuration

This chapter introduces the basic system configuration and user management.

4.1. 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.

4.2. Configuration files and boot files management

4.2.1. configuration files.

- Default name for current system stored file is: startup_config.conf;
- Use **write** command to save configuration information to the flash file systems, 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 config information.
- Use **show runnging_config** command to show current system configuration information.

4.2.2. Startup files

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

4.3. User management

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

Add a new user, the steps are as follows:

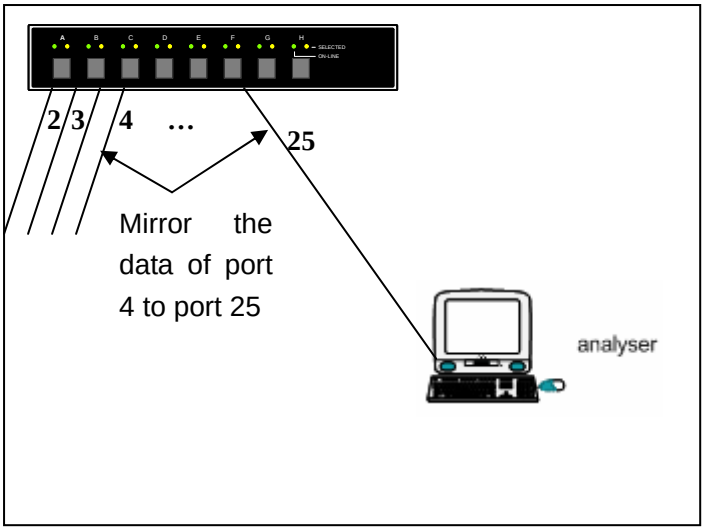
Step	Command	Description
1	**user** *USERNAME* **password** { **no-encryption | md5 }** *PASSWORD*	·*USERNAME* Username; ·**Password** password key word; ·{ **no-encryption | md5} use no-encryptionor md5 encryption password.** ·*PASSWORD* password information;
2	**user** *USERNAME* **privilege** *<1-15>*	·*USERNAME* username; ·**Privilege** privilege key word; ·*<1-15>* user privilege.
3	**Write**	Save configuration information
4	**show user**	Show user information.

5. Mirror function configuration

This chapter includes the following parts:

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

The mirror function is that mirror the traffic of one port to a specified port according to configured rules. Administrator can use this function to analyze network traffic. It allows many mirror ports at the same time but only one monitor port. Mirror function is not available in default situation.



5.1. Enable or disable mirror function

All the configuration are enabled after the mirror function is enabled.

Command	Description
config	Access global configuration mode
mirror { **enable** | **disable** }	Enable/disable mirror function.
exit	Exist from global configuration mode to privileged EXEC
show mirror	Show mirror configuration onformation.

5.2. Configure the monitor port

The traffic of source port will be copied to the 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 the same port.

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

show mirror	Show mirror configuration

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

5.3. configure the source port.

When the mirror function is enabled, the egress/ingress packets of source port will be copied to the monitor port. Users should configure the mirror rules when configure the source port: both, ingress and/or egress. The port cannot be set to source port if it has been set to monitor port.

(1) Mirror both the ingress and egress packets.

Command	Description
config	Enter global configuration mode.
mirror source-port-list both *port-list*	Set the source port and the mirror rule is that copy both the ingress and egress packets . *port-list* is the physical port list, range is 1-26, comma "," and "-" to set multiple port.
exit	Exist from global configuration mode to privileged EXEC
show mirror	Show mirror setting.

(2)mirror the ingress message,,mirror rule is ingress.

Command	Description
config	Enter global configuration mode
mirror source-port-list ingress *port-list*	Set the source port and the mirror rule is that copy the ingress packets. Port-list is the physical port list, range is 1-26, use "," and "_" for multiple input.
exit	Exist from global configuration mode to privileged EXEC
show mirror	Show mirror configuration.

(3)mirror the egress message, mirror rule is egress

Command	Description
config	Enter global configuration mode
mirror source-port-list egress *port-list*	Set the source port and the mirror rule is that copy the egress packets. Port-list is physical port list, range is 1-26, can use "," and "-" for multiple input.
exit	Exist from global configuration mode to privileged EXEC
Show mirror	Show mirror configuration.

(4)configure the mirror for different direction, the mirror rule is ingress or egress.

Command	Description
config	Enter global configuration mode.
mirror source-port-list ingress *port-list* **egress** *prot-list*	Set the source port and the mirror rule is that copy some ports' ingress packets and some ports' egress packets. Port-list is the physical port list, range is 1-26, use ","and"-" for multiple input.
exit	Exist from global configuration mode to privileged EXEC
show mirror	Show mirror configuration.

Delete the mirror configuration through command **no mirror source-port-list**

Use global configuration command **no mirror all** to delete all the mirror setting, use command **show mirror** to show all the mirror settings.

5.4. Example

Set port 26 as monitor port, ingress packets of port 5-8 and egress packets of port 7-12 will be monitorred.

```
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
```

6. Port rate limiting configuration

This chapter describes the port rate limiting on Raisecom ISCOM series switche.

6.1. Configure the port bandwidth

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

Command	Description
config	Enter global configuration mode
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 input. *rate stands for the bandwidth value, unit is kbps,range is 1-1048576. The real value is not the same with the configured value.* burst: unit is KBps, the available value is 1-512. *The real value can be different with the configured value.* ingress is the input direction.
exit	Exist from global configuration mode and enter privileged user exec.
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 for egress fraffic.

Command	Description
config	Enter global configuration mode.
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,can use","and"-"for multiple port input. *Rate* is the set bandwidth value, unit is kbps,the scale is 1-1048576*, The real value can be different with the set value.* burst: unit is KBps, the available value is 1-512. *The real value can be different with the set value.* egress is the input direction.
exit	Exist from global configuration mode and enter privileged user mode.
show rate-limit port-list [*port-lis*]	Show the bandwidth limitation for the port. *port-list*: the same with above

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

6.2. 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

7. MAC address table manangement

This chapter includes following parts.

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

7.1. Configure the aging time of MAC address

The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. 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 unicast or multicast address that does not age and that is not lost when the switch resets. The address table lists the address, the associated VLAN ID, port number associated with the address and the flags.

Command	Description
config	Enter global configuration mode.
mac-address-table aging-time { *0* | *time* }	Set the aging time for MAC address. 0 stands for MAC address aging is disabled Time is the target MAC address aging time, unit is second, range is 3-765, and default value is 300.
exit	Exist from global configuration mode and enter privileged user exec.
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!

7.2. Confiugre static MAC address

Static address is a manually entered unicast or multicast address that does not age and that is not lost when the switch resets. There is no static MAC address by default.

Command	Description
config	Enter global configuration mode.
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 hexdecimal string,* dotted notation for every four characters. Vlan_id range is 1-4094. *port_number* is the physical port number, range is 1-26.
exit	Exist from global configuration mode and enter privileged user exec.
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.

Delete static MAC address and use **no mac-address-table static** HHHH.HHHH.HHHH **vlan** vlan_id **port** port-number.

For example: set the 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 Addrress

---

10 1 1234.1234.1234

7.3. Enable/disable the MAC address learning function

The MAC address learning function can be enabled/disabled based on per port:

Command	Description
config	Enter global configuration mode.
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 function. **disable** disable MAC address learning function function. *port_number* physical port number, range is 1-26.
exit	Withdraw global configuration mode and enter privilege configuration mode.
show interface port [*port-number*]	Show port status. *port_number physical port*,range is 1-26.

For example:Deny 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

7.4. Delete MAC address table.

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

Command	Description
clear mac-address-table {**all** | **dynamic** | **static**}	**all: delete all the layer 2 MAC address.** **dynamic: only delete dynamic MAC address** **static: only delete static MAC address.**

For example:Delete dynamic MAC address.
Raisecom#clear mac-address-table dynamic

7.5. Show MAC address table.

show,check the layer 2 MAC address information for the switch.

Command	Description
show mac-address-table l2-address [{**count** [{**port** *port-number* | **vlan** *vlan_id*}] | **port** *port-number* | **vlan** *vlan_id*}]	Show the MAC address information for the switch. **Count calculate the number of MAC address** *port_number physical port, range is 1-26*. *vlan_id* rane is 1-4094.

For example:show the MAC address on 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 all the studied MAC address on port 1.
Raisecom#show mac-address-table l2-address count port 1

MAC address count of port 1: 97

7.6. Search particular MAC address.

Search the MAC address information of the switch.

Command	Description
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 the MAC address status in the switch.

```
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          Sysbol
------------------------------------------------------------
1234.1234.1234       10              1           Static
```

8. Physical interface configuration

This chapter includes following parts:

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

8.1. Configure the speed and duplex mode of the port.

GE port will always be in 1000Mbps and full duplex mode. When enable auto negociation function, the duplex mode (speed) will be set according to auto negotication result. In default situation, auto negociation is enabled.

Command	Description
config	Enter global configuration mode.
interface port *port-number* **interface range** *port-list*	Enter Ethernet physical interface configuration mode or physical port range configuration mode. *port_numberis the phycial port, range is 1-26.* *port-list range is 1-26, use "," and "-" for multiple input.*
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 to autonegociation. 10: represents that the speed is set to 10Mbps. 100:represents that the speed is set to 100Mbps. 1000: set kilomega port. full: set the duplex mode to full duplex. half: set the duplex mode to half duplex.
exit	Exist from Ethernet physical port and enter global configuration mode.
exit	Withdraw global configuration mode and enter privileged user exec.
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 negociation 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

8.2. Configure the 802.3x flow control function of the port

The flow control function for both ingress and egress traffic can be differently. In default situation, flow control function is disabled for both direction.

Command	Description
config	Enter global configuration mode
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.
flowcontrol {receive|send}{ **on** | **off** }	Enable/disable the flow control function of ingress and egress traffic. **Send** represents the traffic control function at egress direction. **Receive** represents the traffic control function at ingress direction. **on** enabe the traffic control function for the port. **off** disable the traffic control function for the port.
exit	Exist from the physical interface configuration mode and enter global configuration mode.
exit	Exist from global configuration mode and enter privileged user exec.
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 traffic 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: Receive Direction

S: Send Direction

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

---

10 enable down auto on/off enable

8.3. Open/shutdown the port

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

Command	Description
config	Enter global configuration mode.
interface port *port-number* **interface range** *port-list*	Enter Ethernet physical port configuration mode or 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.
{ **shutdown | no shutdown** }	Close or start physical port.

	shutdown close physical port. **no shutdown** start physical port.
exit	Exist from physical port configuration mode and enter global configuration mode.
exit	Exist from global configuration mode and enter privileged user exec.
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

9. 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 sencond).

9.1. Enable the control function

This function is used to enable/disable storm control function on ports.

Command	Description
config	Enter global configuration mode
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.
exit	Exist from global configuration mode and enter privileged user exec.
show storm-control	Show storm control status.

Example: shutdown 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

9.2. Threshold of strom control

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

Command	Description
config	Enter global configuration mode.
storm-control pps *value*	Set the threshold of storm control. Threshold of storm-control packet. Range is 0-262143.
exit	Exist from global configuration mode and enter

	privileged user exec.
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

10. 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.

10.1. Enable SVL

Command	Description
config	Enter global configuration mode
svl { **enable** | **disable** }	Enable/disable SVL function.
exit	Exist from global configuration mode and enter privileged user exec.
show svl	Show SVL status.

Example: start SVL mode.

Raisecom # **config**

ISCOM2826 (config)# **svl** enable

ISCOM2826 (config)# **exit**

Raisecom # **show svl**

SVL: Enable

10.2. Configure SVL of port

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

Command	Description
config	Enter global configuration mode.
interface port <1-26>	Enter port configuration mode
switchport svl vlanlist {1-4094}	Set SVL of the port.
end	Exist from port configuration mode and enter privileged user exec.
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
```

10.3. 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:

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

Example: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

11. Packet transparent transmission

11.1. Overview

There are some kinds of layer-2 packets need to be transparently transmitted, including: BPDU, Dot1x, LACP, GARP, GMRP and GVRP.

11.2. Configure packet transparent transmission

Configure the pass through port and the type of protocol packet that needed to transmit transparently. The port that receive the packet do not pass through any more.

Command	Description
config	Enter global configuration mode
relay {bpdu | dot1x | lacp | garp | gmrp | gvrp | all**} port-list** *port-list*	Set the transmission port of specified protocol packet Packet types:bpdu,dot1x,lacp,garp,gmrp,gvrp *port-list* physical port list, use "," and "-" for multiple setting, range is 1-26.
exit	Withdraw global configuration mode and enter privileged use mode.
show relay port-list	Show the configuration of transmission port.

Cancel the 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          --
```

11.3. Forward DLF packets

Generally speaking, the DLF unicast packet will be dropped locally. But for some users' requirements, DLF packets need to be broadcasted sometimes. DLF packets forwarding is disabled by default. The configuration steps are as follows:

Command	Description

config	Enter global configuration mode.
dlf-forwarding {enable | disable**}**	Whether to broadcast DLF message or not. Enable: enable broadcast. Disable: disable broadcast.
exit	Withdraw global configuration mode and enter privileged user mode.
show dlf-forwarding	Show DLF transmission configuration.

Example: forward DLF packets.

iscom2826#config

iscom2826(config)# dlf-forwarding enable

SUCCESS !

iscom2826(config)#exit

iscom2826# show dlf-forwarding

DLF-forwarding: Enable

12. The layer-3 interface configuration

Layer-3 interface configuration provides a virtual interface for management, users can configure IP address for different VLANs. Use **ip address** command to configure the interface IP address and specify associate VLAN ID and then create a layer-3 interface, use **no ip address** command to delete it. Refer chaper 13 for VLAN configuration

ISCOM2826 support 15 virtual layer-3 interface, each interface corresponding to a static VLAN ID. One static VLAN can only associate with one layer-3 interface.

Following is the procedure for creating three layer interface and IP configuration:

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

13. Link Aggregation Control Protocol

13.1. About link aggregation control protocol (LACP)

Link aggregation control protocol allows facilitate the automatic creation of Ethernet channel by exchanging packets between Ethernet interfaces. LACP is defined in IEEE802.3AD and can dynamically group similarly configured interfaces into a single logical link.

This chapter describes the following parts:

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

13.2. Command description

13.2.1. Enable or disable trunk LACP function

Disable or enable the trunk (LACP) function:

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

Example:

Raisecom#config

Raisecom(config)#trunk disable

Raisecom(config)#exit

13.2.2. 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, including port 1,5,6,7.

Raisecom#config

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

Raisecom(config)#exit

13.2.3. 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 destrination MAC address.
- **sxordmac** select forwarding port based on logical “or” calculation of source and destination MAC address.
- **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” calculation of source and destination IP address.

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 allthe trunk.

Example: Based on source MAC address to set the load-sharing mode for all the trunks to choose the transmission port.

Raisecom#config

Raisecom(config)#trunk loading-sharing mode smac

13.3. Maintenance

User can use show command to check associated configuration of the trunk.

Command	Description
show trunk	Whether to start the trunk,trunk load sharing mode, ports of all the trunk group mumber and current effective ports of the mumber.

Use **show trunk** command to display trunk information, trunk load sharing mode, ports of all the trunk group member and current effective ports of the member.

Current effective ports are the port which are forwarding 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
```

14. RSTP configuration

This chapter introduces how to config RSTP on the switch, including following contents:

- ✧ 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.
- ✧ RSTP system priority configuration.
- ✧ RSTP Hello Time setting
- ✧ RSTP Max Age 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
- ✧ From current Ethenet port move to RSTP mode
- ✧ Clear RSTP port statistical information

14.3. Step by step introduction

14.3.1. RSTP globally enable and disable

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 | disalbe}**	Enable or disable RSTP
3	**exit**	Back to privileged user mode.
4	**show spanning-tree**	Show spanning tree configuration information.

Following is an example for RSTP disable:

Raisecom#config

Raisecom(config)#spanning-tree disable

Raisecom(config)#exit

Raisecom#show spanning-tree

14.3.2. RSTP switch 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 much 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**	Back to privileged user mode
4	**show spanning-tree**	Show RSTP configuration situation

Set RSTP system priority to 4096:

Raisecom#config

Raisecom(config)#spanning-tree priority 4096

Raisecom(config)#exit

Raisecom#show spanning-tree

14.3.3. RSTP Hello Time setting

Switch sends Bridge Protocol Data Unit (BPDU) periodically, and the default interval time value is 2 seconds. Users can change the value based on network situation. When system configuration information losses frequently, user can reduce the value to make the STP more stronger.

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 的 Hello Time
3	**exit**	Back to privileged user mode
4	**show spanning-tree**	Show RSTO configuration information

Set RSTP hello time to 3 seconds:

Raisecom#config

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

Raisecom(config)#exit

Raisecom#show spanning-tree

14.3.4. RSTP Max Age 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 spannin-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 Max Age
3	**exit**	Back to privileged use 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

14.3.5. 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**	Back to privileged user mode.
4	**show spanning-tree**	Show RSTP configuration situation.

Example:

Set RSTP Forward Delay to 5 seconds:

Raisecom#config

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

Raisecom(config)#exit

Raisecom#show spanning-tree

14.3.6. 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**	Back 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

14.3.7. 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 packet by RSTP protocol within hello time to 6:

Raisecom#config

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

Raisecom(config)#exit

Raisecom#show spanning-tree

14.3.8. RSTP port enable and disable

To control RSTP flexibly, user can disable the RSTP protocol based on per port. It will let those ports do not take part in the STP computing. Use following commands to enable/disable the RSTP protocol 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}**	Set the priority of RSTP port.
4	**Exit**	Back to global configuration mode.
5	**Exit**	Back to privileged user mode
6	**show spanning-tree**	Show RSTP configuration situation

Example:

Shutdown RSTP protocol of port 2:

Raisecom#config

Raisecom(config)#interface port 2

Raisecom(config-port)#spanning-tree disable

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show spanning-tree

14.3.9. 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**	Back to global configuration mode.
5	**Exit**	Back to privileged user mode.
6	**show spanning-tree**	Show RSTP configuration information

Example:

Set the RSTO port priority of physical port 2 to 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

14.3.10. 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**	Back to global configuration mode.
5	**Exit**	Back to privileged user 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

14.3.11. 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 connects 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**	Exist to global configuration mode.
5	**Exit**	Exist to privileged user mode.
6	**show spanning-tree**	Show RSTP configuration information.

Example:

Set the Ethernet physical port 2 to 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

14.3.12. 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 etherent physical interface mode.
3	**spanning-tree link-type** {**point-to-point** | **shared**}	Set the point-to-point link type
4	**Exit**	Back to global configuration mode
5	**Exit**	Back to privileged user 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

14.3.13. Force the urrent Etherent 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 compatibility 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 mode.
3	**spanning-tree mcheck**	Force the port move back to RSTP mode.
4	**Exit**	Back to global configuration mode.
5	**Exit**	Back to privileged user mode.
6	**show spanning-tree**	Show RSTP configuration mode.

Example:

Force physical port 2 move back 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

14.3.14. Clear RSTP port statistical information

RSTP counts the BPDU message quantity for each RSTP port: ingress STP detection message, ingress notification message, ingress RSTP message, egress STP detection message, egress notification message, and egress RSTP message.

Clear RSTP port statistical information:

Step	Command	description
1	**Config**	Enter global configuration mode.
2	**interface port** <1-26>	Enter etherent interface mode.
3	**spanning-tree clear statistics**	Clear port statistical information.
4	**Exit**	Back to global configuration mode.
5	**Exit**	Back 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

14.4. Mornitoring

Under privileged exec mode, use **show spanning-tree** command to check the current global status and configuration of RSTP. This command is used to display uniform configuration information of spanning-tree of current 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
```

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

```
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
```

15. DHCP configuration

DHCP Relay is NOT AVAILABLE FOR ISCOM2826.

15.1. DHCP Relay configuration

- ✧ DHCP Relay protocol introduction
- ✧ Configure the task list
- ✧ Introduction step by step
- ✧ Monitor and maintenance
- ✧ DHCP Relay trouble shooting

15.2. DHCP Relay protocol introduction

DHCP Relay agent realizes the alternating capability between client and server, that is to say, it transmit different packets to different sub-network, do not need to set DHCP server on every sub-network. Different sub-network can use a DHCP server to realize the dynamic districtuition of IP address, it is convenient to manage large-scale network.

15.3. DHCP Relay configuration task list

The configuration of DHCP includes following setting:

- ✧ The start and stop of DHCP Relay
- ✧ Server address configuration

15.4. DHCP Relay configuration

15.4.1. Start and stop DHCP Relay

Default situation, DHCP Relay is not effective on the switch. When the globally start or close DHCP Relay, the default situation is: all the VLAN start or close DHCP Relay function. Apply following command under global configuration mode to let DHCP Relay go into effect.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**dhcp-relay enable**	Start DHCP Relay
3	**exit**	Back to privileged configuration mode.
4	**show dhcp-relay**	Show DHCP Relay configuration mode

In order to stop DHCP Relay, type **dhcp-relay disable** command.

This command is used to start DHCP Relay function under global configuration mode, in order to stop the DHCP Relay function of particular VLAN, type following command under global configuration mode:

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

Similarly, in order to reenalbe DHCP Relay function on the VLAN, type **dhcp-relay listen under** global configuration mode.

When DHCP Relay function is disabled under global configuration status, user can start DHCP Relay on particular VLAN, but only when the DHCP Relay is enabled under global configuration mode, the DHCP Relay function can go into effect.

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

ISCOM2826# **show dhcp-relay listen**

the VLAN that enabled the DHCP Relay include:

VLAN ID = 1,2

The total enabled VLAN num is 2

Use following command:

ISCOM2826# **show dhcp-relay listen vlan** 3

VLAN 3 disabled DHCP Relay

15.4.2.Server address configuration

In order to realize the message transmission capacity of RELAY, user should know the address of DHCP address, it need manual configuration of administrator.

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**	Back to privileged user mode
4	**show dhcp-relay server-ip**	Display the address configuration information of DHCP server

In order to delete configured server address, use **no dhcp-relay server-ip** *ip-address* command under global configuration mode. If the IP address that user want to delete doesn't exist, return "failure".

Note: the maximum quantity of Server IP address is 8. User should guanrantee the IP address is corrent.

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 some show command to check the running situation and configuration situation of DHCP Relay on the switch. It is convenient to for monitor and maintenance. Use following command for the monitor and maintenance of DHCP Relay:

Command	Description
show dhcp-relay	Show DHCP Relay configuration information.
show dhcp-relay listen [**vlan** *vlanid*]	Show the configuration information for all the VLAN or designated VLAN DHCP Relay.
show dhcp-relay server-ip	Display the address information of DHCP server.

Use **show dhcp-relay** command to check configuration information, for example the VLAN configuration information or global configuration information, and statistical 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 particular VLAN configuration information, use **show dhcp-relay listen** [**vlan** *vlanid*], if the VLAN is not specified, show all the VLAN information, that is all the existed 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

1. If the server IP address is not specified, the device will not transmit message normally.
2. There are some reasoms for the trouble: the IP address has get to the limitation (the Maximum limitation is 8); or input wrong IP address.
3. If fail to delete the address, the possible reason is IP address incorrect, or the IP address doesn't exist.

15.5.1. DHCP Relay command reference

Command	Description
dhcp-relay service	Start DHCP Relay function
dhcp-relay listen vlan-list {1-4094}	Start DHCP Relay function on designated VLAN.
dhcp-relay server-ip *ip-address*	Configure DHCP server address.
show dhcp-relay	Show DHCP Relay configuration information
show dhcp-relay listen [**vlan** *vlanid*]	Show designated or all the VLAN information of DHCP Relay.
show dhcp-relay server-ip	Show address information of DHCP server.

15.6. DHCP Server configuration

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

15.6.1. DHCP Server protocol introduction

Dynamic Host Configuration Protocol,DHCP let user get configuration information in TCP/IP network, it is based on BOOTP protocol, and appends some functions like automaticly distribute useable network addresses. These two protocols can operate with each other. DHCP provides configuration parameter to network host computer 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 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 are reduced.

15.6.2. DHCP Server configuration task list

The configuration of DHCP server includes following functional configuration:

- ✧ The start and stop of DHCP Server.
- ✧ The configuration of address pool.
- ✧ The configuration of lease table overtime.
- ✧ The address configuration of neighbouring agent.

15.6.3.the start and stop of DHCP Server

Default situation, DHCP server is disabled on the switch. when the DHCP server is enabled/disabled in global configuration mode, DHCP server function is enabled on all the VLAN. Apply following commands can enable DHCP server protocol.

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

In order to stop DHCP Server,execute **dhcp-server disable** command under global configuration mode.

This command is used to start DHCP server function under global configuration mode, execute following commands to stop the DHCP server function on particular VLAN:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**dhcp-relay deactive vlan-list {***1-4094***}**	Stop the DHCP server function on this VLAN.
3	**exit**	Back to privileged configuration mode.
4	**show dhcp-server**	Show VLAN configuration situation.

Similarly, in order to restart DHCP server function on the VLAN, execute **dhcp-relay active** command under global configuration mode.

If the DHCP relay is in disabled status under the global configuration mode, user can start DHCP server on particular VLAN. But the DHCP server only goes into effect when the global DHCP server is started.

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

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.address pool configuration.

In order to realize DHCP address configuration function, user must configure address pool for DHCP server. It needs the manual configuration by administrator.

Configuration steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**dhcp-sever ip-pool WORD……**	Set the IP address pool for the DHCP server.
3	**exit**	Back to privileged configuration

		mode.
4	**show dhcp-server ip-pool**	Show the configuration information of DHCP server address pool.

In order to delete the address pool that has been configured, use **no dhcp-server ip-pool** command under global configuration mode. If the IP address doesn't exist, return failure

Note: the maximum quantity of IP address pool is 20, the maximum quantity of IP address is 1000. Name is the only mark for address 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 do not choose them, do not specify gate and DNS for the client end.

15.6.5.lease time configuration for lease table

User should specify the lease time of IP address when distribute the IP address for the clients. The default lease time is 30 minutes (Generally speaking, it will not be used); the maximum lease time is: 10080 minutes (seven days), if the client request lease time is longer than this value, use the maximum lease time; the minimum lease time is 30 minutes, if the client request time less than this value, use the minimum lease time; otherwise use client request time; if the client end doesn't specify the lease time, use minimum lease time. Administrator can manually configure the value.

Configuration steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode.
2	**dhcp-sever default-lease** *timeout*	Set the IP address pool of DHCP server to the default lease time.
3	**dhcp-sever max-lease** *timeout*	Set the maximum lease time of

		DHCP
4	**dhcp-sever min-lease** *timeout*	Set the minimum lease time of DHCP server.
5	**exit**	Back to privilege mode.
6	**show dhcp-server**	Show the configuration information of DHCP server address pool.

In order to recover the system time to the default value, use **no dhcp-server default,no dhcp-sever max-lease,no dhcp-sever min-lease** command under global configuration mode.

Note: the lease time will be applied to all the IP address of the address pool. At the same time, the maximum lease time should 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.Neighbouring DHCP Relay address configuration

When DHCP Relay connects the client end to the server, DHCP server should know the IP address of neighbouring DHCP Relay. It needs the manual configuration by administrator.

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 neighbouring agent IP address of DHCP server.
3	**exit**	Back to privileged configuration mode.
4	**show dhcp-server relay-ip**	Display the configuration information of DHCP server.

In order to delete the IP address of neighbouring agent, use **no dhcp-server relay-ip** *ip-addres* command under global configuration mode.

Note: the neighbouring agent IP address we set here is the interface address, which connected to the client. Refer to typical example. The maximum quantity neighbouring agent IP address is 8.

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. Monitor and maintenance

It is convenient to use some show commands to check the running and configuration information of DHCP Server. Use following **show command** for monitor and maintenance for DHCP server protocol:

Command	Description
show dhcp-server	Show configuration and statistical information of DHCP Server.
show dhcp-server ip-pool	Show DHCP SERVER address pool informaiton
show dhcp-server relay-ip	Show neighbouring DHCP agent address information.

Use **show dhcp-server** command to check configuration information, for example global or VLAN configuration information, statistical information etc.

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

15.7.1.typical configuration example

Following are the typical DHCP Relay and Server configuration examples:

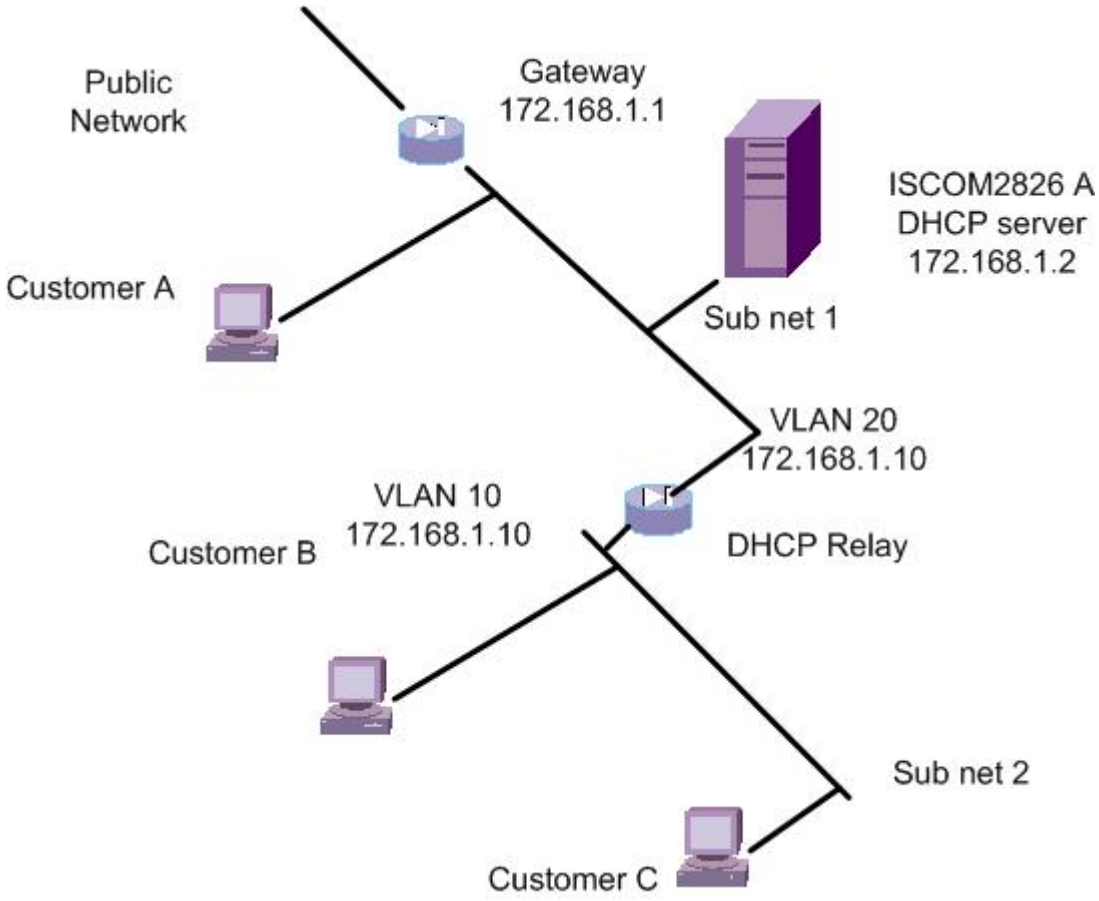
- Directly connected client end obtains IP address.
- Client obtains IP address by the agent.

1) Configuration introduction

This is a typical example for the realization of DHCP protocol. See detail connection as following picture.

The ISCOM2826 has two VLAN, VLAN 10 and VLAN 20, corresponding to two subnets: one is 192.168.1.10 and 172.168.1.10. DHCP server is the ISCOM2826 system integrated DHCP server (here ISCOM2826 is the server only, we just want to show the configuration procedure), the IP address is 172.168.1.2, suppose the DNS of the subnet is 172.168.1.3. Subnet 1 and subnet 2 are connected by network gateway 172.168.1.1 to the public network. In order to realize that the client end connects to the public network resource normally, configure DHCP server and DHCP Relay correctly is enough.

2) Topology



3) Configuration steps

- Configure DHCP SERVER:
- Configure VLAN and interface:

ISCOM2826A(config)# vlan 20
ISCOM2826A(config-vlan)# state active
ISCOM2826A(config-vlan)# exit
ISCOM2826A(config)# interface port 1
ISCOM2826A(config-port)# switchport access vlan 20
ISCOM2826A(config-port)# exit
ISCOM2826A(config)# interface ip 2
ISCOM2826A (config-ip)# ip address 172.168.1.2 255.255.0.0 20

- Configure address pool

Configure IP address pool for subnet 1 and subnet 2 respectively.
ISCOM2826A (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
ISCOM2826A(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
ISCOM2826A (config)# exit
ISCOM2826A #show dhcp-server ip-pool

- Start DHCP server

ISCOM2826A (config)#dhcp-server enable
DHCP are started on all the VLAN, if in order to start DHCP only on VLAN20, user

shold stop DHCP on other VLANs.

ISCOM2826 A(config)#vlan 1

ISCOM2826A (config-vlan)#dhcp-server deactive

ISCOM2826A (config-vlan)#exit

ISCOM2826A (config)#exit

ISCOM2826A # show dhcp-server

- Set the IP address of neighbouring agent

ISCOM2826 A(config)#dhcp-server relay-ip 192.168.1.10 255.255.255.0

ISCOM2826A (config)#exit

ISCOM2826A # show dhcp-server relay-ip

- Set the router for network section 192.168.1.0(subnet 2).

ISCOM2826A (config)#ip route 192.168.1.0 255.255.255.0 172.168.1.10

Configure DHCP Relay

- Create VLAN and interface

ISCOM2826B (config)# vlan 10

ISCOM2826 B(config-vlan)# state active

ISCOM2826B (config-vlan)#exit

ISCOM2826B (config)# interface port 1

ISCOM2826B(config-port)# switchport access vlan 10

ISCOM2826B(config-port)#exit

ISCOM2826B (config)# interface ip 2

ISCOM2826 B(config-ip)# ip address 192.168.1.10 255.255.255.0 10

ISCOM2826B (config)# vlan 20

ISCOM2826B (config-vlan)# state active

ISCOM2826B (config-vlan)#exit

ISCOM2826B (config)# interface port 2

ISCOM2826B(config-port)# switchport access vlan 20

ISCOM2826B(config-port)#exit

ISCOM2826B (config)# interface ip 3

ISCOM2826B (config-ip)# ip address 172.168.1.10 255.255.0.0 20

- Configure server IP address

ISCOM2826 B(config)#dhcp-relay server-ip 172.168.1.2

ISCOM2826B (config)#exit

ISCOM2826B #show dhcp-relay server-ip

- Start DHCP Relay

ISCOM2826B (config)#dhcp-relay enable

all VLAN start DHCP function at this time, if want to start DHCP relay function only on VLAN 10 and VLAN 20, user should stop DHCP on all other VLANs.

ISCOM2826 B(config)# vlan 1

ISCOM2826B (config-vlan)# no dhcp-relay listen

ISCOM2826B (config-vlan)#exit

ISCOM2826 B(config)#exit

ISCOM2826B #show dhcp-relay listen

Client end obtains IP address.
By DHCP, client end automaticly obtain 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 on ISCOM2826.

- Check DHCP Relay information

Use **show dhcp-relay** on the ISCOM2826B.

- 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.

15.7.2.DHCP Server touble shooting

1. If do not specify the IP address of neighbouring agent, the device can not realize DHCP agent function normally;
2. When set the neighbouring agent address, the possible reason for the trouble is: input wrong IP address or the IP address has got to the maximum limitation 8;
3. When set the address pool, the possible reason is: input wrong IP address or the IP address has got to the maximum limitation 20;
4. If fail to delete address pool, the possible reason is that the address pool doesn't exist or the input parameter is incorrect.
5. If after above configuration, DHCP still can not work normally, please check whether the default gateway or route of neighbouring agent has been set.

15.7.3.DHCP Server command reference

Command	Description
dhcp-server enable	Start DHCP Server function
dhcp-server disable	Stop DHCP Server function
dhcp-server active vlan-list {1-4094}	Start DHCP Server function on designated VLAN.
dhcp-server deactive vlan-list {1-4094}	Stop DHCP Server function on designated VLAN.
dhcp-server relay-ip *ip-address*	Configure the IP address of DHCP neighbouring agent IP address.
dhcp-server ip-pool *name startip endip maskip* **vlan** *vlanlist* **gateway** *gtwip* **dns** *dnsip* **secondary-dns** *dnsip*	Configure address pool.
dhcp-server default-lease *timeout*	Set the default lease time of DHCP table.
dhcp-server max-lease *timeout*	The maximum lease time of DHCP table.
dhcp-server min-lease *timeout*	The minimum lease time of DHCP table.
show dhcp-server	Show configuration and statistics information of DHCP server.
show dhcp-server relay-ip	Show the neighbouring agent IP address of DHCP server.

16. IGMP SNOOPING configuration

16.1. IGMP Snooping function configuration

- Introduction to IGMP Snooping protocol
- Configuration task list.
- Monitor and maintenance
- Typical configuration example
- IGMP Snooping 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. As the name implies, IGMP snooping requires the 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.

ISCOM switches supports 255 IP multicast 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 Router port configuration

4 Immediate-leave function configuration

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 snoopig 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**	Exist 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 enable 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**	Stop the IGMP snooping function for this VLAN.
4	**exit**	Exist to global configuration mode
5	**exit**	Exist to privileged user mode
6	**show ip igmp snooping vlan** *vlan-id*	Show VLAN configuration information

In order to restart 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 serveral 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**	Exist to privileged user mode
4	**show ip igmp snooping**	Show VLAN configuration information

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

In order to check whether the configuration is corrent 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

When layer 2 multicast router does not have IGMP jion or query message within some a period, the host or router may have left already without sending any leaving message, so it needs to be deleted. The default aging time is 300 seconds. Manual configuration as following:

Step	Command	Description

1	**config**	Enter global configuration mode.
2	**ip igmp snooping timeout** *timeout*	Set IGMP overtime.
3	**exit**	Exist to privilege mode
4	**show ip igmp snooping**	Exist to configuration situation

The range of aging time is 30 seconds to 3600 seconds, in order to recover default value, use following command:

ISCOM2826(config)**#no ip igmp snooping timeout**

Configuration 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. router port configuration

The router port can dynamicly study address (by IGMP request message), manual configuration is also ok. That is to say, multicast report and leave message of downstream hosts can be transmitted to router port. The configuration steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode
3	**ip igmp snooping mrouter vlan <1-4094> port <1-26>**	Configure router port
5	**exit**	Exist to privileged mode
6	**show ip igmp snooping mrouter**	Show configuration situation

There can be several router ports in a VLAN, and the port is applicable to all the multicast address. Use following command to delete configured ports of the router:

ISCOM2826 (config)**#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 setting:

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 mode
3	**ip igmp snooping immediate-leave**	Set immediate-leave function on the VLAN.
4	**exit**	Exist to global configuration mode.
5	**exit**	Exist to privilege configuration mode.
6	**show ip igmp snooping**	Show configuration situation

Under VLAN mode, in order to recover device default setting, use following command: ISCOM2826 (config)**#no ip igmp snooping immediate-leave**.

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 make the multiple VLAN setting conveniently, 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**	Back to privileged configuration mode.
4	**show ip igmp snooping**	Show configuration situation.

In order to recover device default setting, use following commands:

iscom2016(config)**#no ip igmp snooping vlan** *vlanlist* **immediate-leave**

Configuration 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. manual configuration of multicast MAC address table

Generally speaking, ports are added to multicast group by IGMP packet which is sent by host computer. In order to make it conveniently, users can add a port to a multicast group manually.

Undre privileged user mode, use 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 group
3	**exit**	Back to privilege user mode
4	**show mac-address-table multicast**	Show layer 2 multicast router information.

The MAC address is the multicast MAC address, and the format is HHHH.HHHH.HHHH. For example,IP address 224.8.8.8 corresponding to MAC address 0100. 5e08.0808;The range of the port is from 1 to 26. In order to delete the port from multicast router 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**

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)

16.4. monitor and maintenance

Use show command to check switch IGMP snooping running and configuration status. Use following **show** command for the monitor and maintenance of IGMP snooping:

Command	Description
show ip igmp snooping [**vlan** *vlan-id*]	Show all the VLAN or designated VLAN configuration information of IGMP snooping on the switch.
show ip igmp snooping multicast [**vlan** *vlan-id*]	Show multicast router port information that are dynamicly studied or configured manually on all the VLAN or designated VLAN.
show mac-address-table multicast [**vlan** *vlan-id*] [**count**]	Show the layer 2 multicast entity of all the VLAN or designated VLAN, do not display detail entity information.

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

If only want to check particular configuration information, use **show ip igmp snooping vlan** *vlanid*. If do not specify VLAN, then all the VLAN information are displayed, that is all the existent and active VLAN.

Show igmp-snooping multicast router information, command execution echo as following:

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

Layer 2 multicast router information as following commands:

```
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

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

16.6. IGMP Snooping command reference

Command	Description
ip igmp snooping	Start IGMP Snooping
ip igmp snooping timeout	Configure the time limitation of IGMP snooping
ip igmp snooping	Enable the IGMP snooping function on the VLAN.
ip igmp-snooping vlan	Enable IGMP snooping on multiple VLAN.
ip igmp snooping immediate-leave	Set immediate-leave function on the VLAN.
ip igmp snooping vlan immediate-leave	Set immediate-leave function on the VLAN.
ip igmp snooping mrouter port	Set router ports
show ip igmp snooping	Show IGMP snooping configuration information.
show ip igmp snooping multicast	Show dynamicly studied or manually configured multicast router information.
show mac-address-table multicast	Show the layer 2 multicast entity of the switch or designated VLAN

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.

Command	Description
config	Enter global configuration mode
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”.
exit	Withdraw global configuration mode and enter privileged user mode.
show rmon statistics	Show statistics group information.

Stop statistics group, 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.

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

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

Example:

Set the 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

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

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 monitorred.* ● *time* unit is second, monitor the period of MIB object.; ● **delta** specify the two times sampling difference of MIB variables. ● **absolute** directly sampling MIB variable ● **rising-threshold** *value* upper bound ● *event-number the event number of which get to the upper bound.* ● **falling-threshold** *value* lower bound. ● *event-number the event number of which get to the lower bound.* ● **owner** *string* specify the owner of Alarm.
3	**exit**	Withdraw global configuration mode.
4	**show alarm** *number*	Display the execution echo

Delete the alarm,use command **no alarm** *number*.

Example:

Set an alarm, monitor MIB variable 1.3.6.1.2.1.2.2.1.20.1, every 20 seconds each time, check the rise or down of this variable. If the value raises 15, alarm will be touched, 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 configuration parament for 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*]	● *number index number* ● **log** whether write the log information and

	[**owner** *string*]	send syslog ● **trap** whether to send trap ● **description** *string*:*describe string* ● **owner** *string* the owner of the event
3	**exit**	Withdraw global configuration mode.
4	**show event** *number*	Show configuration result.

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

Example:

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

Raisecom#config

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

Raisecom(config)#exit

Raisecom#show rmon event 1

Recover to default status:

Set all the function of RMON group to default status, that is the starting status of the switch.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**clear rmon**	Recover to default status
3	**exit**	Back to global configuration mode

17.3. show RMON configuration information and the result

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

18. ARP

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

ARP mapping table includes 2 types tems:

- ✧ Dynamic term: switch use ARP protocol to study MAC address dynamicly and it will be aged if not used.
- ✧ Static term: manually added by the user and will not be aged.

ARP address resolution protocol, mainly used to resolve the map from IP address to Ethernet MAC address.

If host A sends IP packets to host B, host A uses the IP address of host B to search corresponding physical address in its own mapping table. If host B physical address is found out, send IP packet; if host B physical address isn't found out, host A sends ARP request to host B, and add the mapping of IP address and MAC address to host B.

In most situations, when host A sends data to host B, it is pretty possible that host B will sent data to host A again, so host B will also sends ARP request to host A. In order to reduce the communication in the network, host A write its own MAC address when sends ARP request. When host B receives the ARP request, host B will record the MAC address of host A to its mapping table. Then it is more convenient for host B to send data packet to host A.
In some special situation, user can use static MAC address configuration command to operate ARP address mapping table.

18.2. ARP setting

18.2.1.add static ARP address

Static ARP address term has following characters:
Static ARP address must be manually added, and also must be manually deleted and cannot be aged.

Following are the configuration commands for adding static mapping terms of ARP address mapping table.

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

arp *ip-address mac-address* command is used to add a ARP static mapping term. Ip-address demonstrates ip address; mac-address demonstrates IP address associated

Ethernet MAC address. The format of MAC address is HHHH.HHHH.HHHH. For exmple: 0050.8d4b.fd1e.

18.2.2.delete ARP address mapping term:

Command	Function
No arp *ip-address*	Delete a term in the ARP address-mapping table.

Use **no arp** *ip-address* command to delete a map from ARP address mapping table, includes statis term and dynamic term.

18.2.3. Set the timeout of ARP dynamic address mapping terms.

Command	Function
arp aging-time *sec*	Set the living time of ARP dynamic table.

This command is used to set the timeout of ARP dynamic term, if exceed this timeout value, the ARP dynamic term will be deleted automatically. The range of timeout is 0,30-2147483, If set the timeout to zero, ARP dynamic table isn't aging.

18.2.4.clear ARP address mapping table

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

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

18.3. Show ARP address mapping table

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

Use this command to show all the terms in ARP address mapping table including the ip address of each IP address, MAC address and type of term.

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) such as CiscoWorks. 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.

ISCOM switches SNMP Agent support SNMPv1,SNMPv2 and SNMPv3.

19.2. SNMP configuration

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

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

19.2.1. Configure SNMP user

SNMPv3 uses 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, user table records user names, user associated engine ID, and other information like whether need to be authenticated or *authpassword* etc. 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. The configuration of SNMP user is created by *authpassword* generated from command line, and it adds a user in switch local 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**}	Use password format to add a SNMP user.

	authpassword]	
3	**exit**	Back to privileged user mode.
4	**show snmp user**	Show configuration information

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

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

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

Example 2:
Add a user *guestuser2,* local engine ID, do not authenticate.
Raisecom(config)#**snmp-server user** *guestuser2*

Example 3:
Delete user *guestuser2*,local engine ID:
Raisecom(config)#**no snmp-server user** *guestuser2*

19.2.2. Access priority configuration

SNMP protocol has several access control model.

1,The access control based on community

In order to protect itself and MIB from the unauthorization access, SNMP has the concept of community. All the Get and Set operations of agent within a community should use the correct community nume, otherwise its requests will not be answered. That is to say, SNMPv1 and SNMPv2 take community name as the authorization solution, the SNMP packet that doesn't match authorized community name will be dropped.

Actually, the community name use different string to mark different SNMP community. Communities has read-only or read-write priority. The community that has read-only priority can only search the device information, but the community that has read-write priority can not only search the device information, but also configure the device.

The switch use following commands to set the SNMP group name:

Table 19.2 configure SNMP group name and access priority

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

Community-name is the community name, **view-name** is view name, **ro** indicates that the managers can use this name to inquire the MIB variables in designated view; **rw** indicates that the managers can use this name to inquire MIB variable in designated view of the switch and change the MIB variable in designated view.

Example 1:

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

Use this command to define the community name to 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). Usm has the concept of access group: One or more users corresponds to an access group, each access group set correspongding read, write and notification view, the user in the access group has the priority in the view. the access group that has the user who sends requests like Get and Set should has corresponding priority, or else, the request will not be answered.

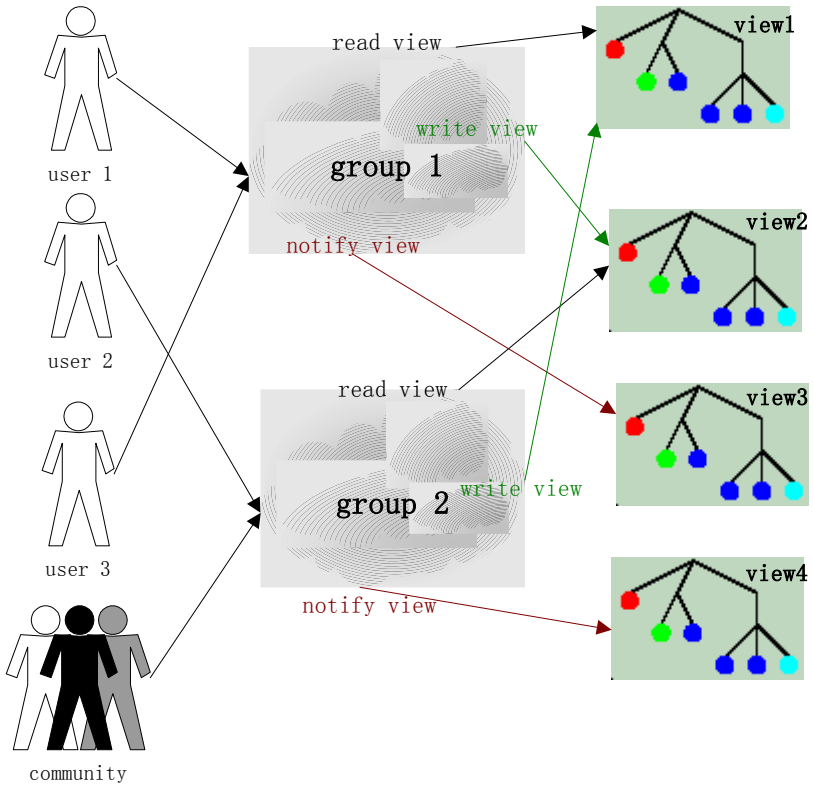


Figure 1 SNMPV3 access control model

From above figure, we know that if NMS wants to access the switch normally, it should not only configure the user, but also make sure which user belongs to which group, the access group has view priority and each view. The whole configuration (including the configuration for the user) procedure is in following table.

Table 19.3 Configuration of SNMPv3 access control

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

2	**snmp-server user** *username* [**remote** *engineid*] [**authentication**{**md5** | **sha**} *authpassword*]	Add a user
3	**snmp-server view** *view-name oid-tree* [*mask*] {**included | excluded**}	Define the view and its range of MIB.
4	**snmp-server group** *groupname* **user** *username* { **v1sm | v2csm | usm**}	Make sure the user belongs to which access group.
5	**snmp-server access** *groupname* **[read** *readview***] [write** *writeview***] [notify** *notifyview***] [context** *contextname* **[**{**exact | prefix**}**]]** { **v1sm | v2csm | usm**} { **noauthnopriv | authnopriv** }	Define the access priority of access group
6	**exit**	Back to privileged configuration mode
7	**show snmp group** **show snmp access** **show snmp view** **show snmp user**	Show configuration information

- **View configuration information**

view-name specify the configured name of view ,*oid-tree* specify OID 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.

mack is the mask of OID subtree, each of its bit corresponding to a term of the subtree. If some of the mask is 1, view should match the corresponding term of subtree; if some of the mask is 0, view doesn't need to match any term. The maximum length of mask is 16 characters; that is to say, it supports the subtree with depth 128. For example: a view OID subtree is 1.3.6.1.2.1, mask is 1.1.1.1.0.1, then real subtree which view included is 1.3.6.1.x.1 (x can be any number), that is the first term of all the nodes under 1.3.6.1. The default view of the switch is Internet, the scale of the view includes all the MIB variables under the tree 1.3.6. All default bits of mask are 1.

- **Configuration introduction of access control group.**

Groupname is the name of access group; *readview* is the read view, 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 be matched with the name of context; v1sm|v2csm|usm are the security model, stands for SNMPv1 security model,SNMPv2 is the security model based on the group, and SNMPv3 is the security model based on the user respectively; **noauthnopriv|authnopriv** is the security level, stands for no authentication no encryption, and authentication without encryption respectively. When delete an access group, the name of accesss group, name of context, security mode and security level should be specified

If the security model is v1sm or v2csm, security level is noauthnopriv automaticly, so the model doesn't has the option {**noauthnopriv | authnopriv**},and at the same time, without

the option **[context** *contextname* **[{exact | prefix**}**]].**

Example 1:
Create an access group “guestgroup”, security model is usm, security level is authentication without encryption, readable view is mib2, both readable view and informational view are empty view as default:
Raisecom(config)#**snmp-server access** *guestgroup* **read** *mib2* **usm authnopriv**

Example 2:

Delete access group guestgroup:

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

- **Configuration introduction for the map from user to access group**

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

Example 1:

Map the *guestuser1* who has a security level usm to access group *guestgroup.*
Raisecom(config)#**snmp-server group** *guestgroup* **user** *guestuser1* **usm**

Example 2:

Delete the map from *guestuser 1* with security level usm to access group *guestgroup.*
Raisecom(config)#**no snmp-server group** *guestgroup* **user** *guestuser1* **usm**

19.2.3. TRAP configuration

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

The switch needs following commands to configure parameters for SNMP target host computer.

Table 19.4 Configure SNMP target host computer

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

Example 1:
Add a host computer address of host_1, ip address is *172.20.21.1*,user name is raisecom, SNMP version is v3, authentication but no encryption, with trap.
Raisecom(config)#**snmp-server host** *172.20.21.1* version 3 authnopriv raisecom

Example 2:

Delete host computer address host_1
Raisecom(config)#**no snmp-server host** *172.20.21.1*

19.3. Other configuration

- **Configure the mark and contact method of network administrators**

The mark and contact method of network administrator is a variable of MIB system group; the effect is to set the mark for network administrator and contact method.

Table 19.5 the mark of network administrator and contact method

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

Example:

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

- **Permit or deny trap information send by the system**

Trap is mainly used to provide some important events to network management station (NMS). The switch will send to the NMS a authentication failure trap if the switch gets a request with incorrect community name and the switch is set to allow to send snmp trap.

Table 19.6 allow or deny Trap

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

Use **snmp-server enable traps** command to all trap.

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

- **Set the position of the switch**

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

Table 19.7 Set the position 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**	Back to privilege configuration 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

Table 19.8 SNMP information

Command	Function
show snmp community	Show all the group name, corresponding name of view and priority.
show snmp host	Show all the IP address of trap target host computer.
show snmp config	Show the ID for local SNMP engine, the mark of network administrator and contact method, the position of the switch and TRAP on-eff.
show snmp view	Show all view name and their scale.
show snmp access	Show all the names of access group and the attributes of access group.
show snmp group	Show all the mapping relationship from user to access group.
show snmp user	Show all the old users, and all the other authentication and encryption protocol.
show snmp statistics	Show SNMP packet statistics information

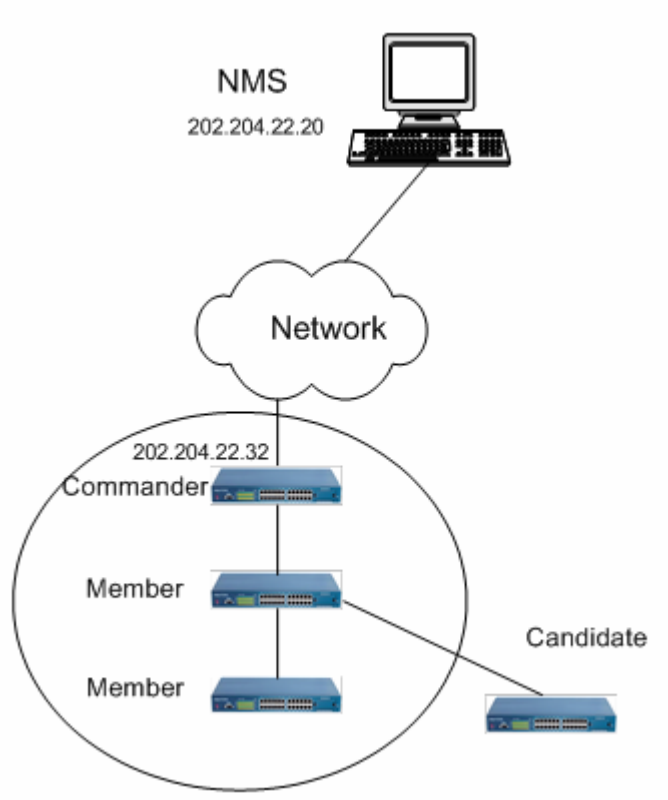
20. Cluster management

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

1. Cluster introduction
2. Cluster management configuration list
3. Monitor 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 switchs. 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, that is RNDP (Raisecom Neighbor Discover Protocol),RTDP (Raisecom Topology Discover Protocol) and RCMP (Raisecom Cluster Management Protocol). RNDP is in charge of neighbour discovery and information collection, RTDP is in charge of the collecting and processing topology information, RCMP is in charge of the relevant configuration like add, active, and delete for cluster members. RTDP and RCMP protocol communicate in VLAN 2. So if there is no such a device that supports Raisecom cluster management function 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 t the management interface to all the switches in the cluster. Commander uses command redirection to manage the members: users send the management command to the commander in public network, let the commander to handle the commands; if the commander finds that this command is for other members and it will send the commands to members. Commanders have the functions: discover neighbour, collect the network topology, cluster management, maintaining cluster status, and support different proxy.
- Member: cluster member, generally speaking, do not configure IP address. User uses the command redirection function to manage the device. Member device has the functions including discovering neighbour, receiving the management info of commander, executing the proxy command, failure/log report function. Once the member is actived, it can be managed by network commander.
- Candidate: it isn't added into any cluster but do has 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 will be the member; user has to active this switch by cluster management function, or by configuring automaticly active function on the switch to active the switch.

20.2. Cluster management configuration list

1. RNDP globally enable
2. RNDP port enable
3. RTDP enable
4. RTDP collection area configuration
5. Enable and disable cluster management function
6. Automaticly active and enable
7. Add and active cluster member
8. Delete cluster member
9. Suspend cluster member
10. Add and active all the candidate member
11. Cluster member remote management

20.2.1. Globally enable RNDP

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

Step	Command	Description
1	**config**	Enter global configuration mode
2	**rndp** {**enable | disable**}	Global enable or deny RNDP

3	**exit**	Back to privilege configuration mode
4	**show rndp**	Show RNDP configuration

Globally deny RNDP function
Raisecom#config
Raisecom(config)#rndp dis
Raisecom(config) #exit
Raisecom #show rndp

20.2.2. RNDP port enable

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

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port <1-26>**	Enter port configuration mode
3	**rndp** {**enable	disable**}	Port enable or deny RNDP
4	**exit**	Back to privilege configuration 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. RTDP enable

Under global configuration mode, user can enable or disable RTDP function, RTDP is disabled as the default. If RTD is enabled, RTDP will collect all the information of the 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**	Back to privilege configuration 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. 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**>**	Back to RTDP collection range
3	**exit**	Back to privilege configuration mode
4	**show rtdp**	Show FTDP 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 of 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**	Back to global configuration mode
4	**exit**	Back to privilege configuration 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. Automaticly active function enable

Users can use **cluster-autoactive** command to enable automatically activing

function. **no cluster-autoactive** command will disable automatically activing function. When the autoactive function is enabled, and the commander MAC address is configured, the switch will set itself as an active member.

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

This MAC address is only available when the autoactive function is active. When the actoactive function is started, and the switch will automatically be active.

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

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

Following command is used to enable automaticly 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 the candidates to the cluster or active some members; it also can delete some or all the member 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-acitve commander for this member is current switch, 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 candidate member to the cluster; Active: active the device that has been added to the cluster.

		Usrename: active the username that is used by the device. Password: active the password that is used by the device.
4	**exit**	Back to global configuration mode.
5	**exit**	Back to privilege configuration mode
5	**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

Under cluster management mode, user can delete the device that do not need the cluster management function from the cluster.

Step	Command	Description
1	**config**	Enter globalc 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 MAC address that will be deleted. All: delete all the devices;
4	**exit**	Back to global configuration mode.
5	**exit**	Back to privilege mode
5	**show cluster member**	Show cluster member relevant 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. Cluster member suspend

Under cluster management mode, user can suspend the device that has been actived. Although the device has been suspended, but it isn't 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**	Back to global configuration mode.
5	**exit**	Back to privilege configuration mode.
5	**show cluster member**	Show cluster member relevant 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 candidate member

In order to make the operation of add and active conveniencely, this command allows user to use the same username and password to add and active all the candidate members, or add or active the candidate members which have been configured as the automaticly active by the switch. User can also user following commands to add or active all the candidate members:

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 to active member. Password: the password that isused to active

		members. All: add and active all the members.
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege configuration mode
5	**show cluster member**	Show cluster members relevant information

Use **member auto-build** command to automaticly add and active all the candidates that have been configured to be automaticly actived to be automaticly actived by the switch.

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

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

Use 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 member device, that has been actived, 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. RNDP neighbour information display

Step	Command	Description
1	**show rndp neighbor**	Display directly connected neighbour device information.
2	**show rndp**	Show RNDP configuration

Use show rndp neighbor check directly connected device information:
Raisecom# show rndp neighbor

Use **show rndp** command to check RNDP configuration:
Raisecom# show rndp

20.3.2.RTDP device information display:

Step	Command	Description
1	**show rtdp device-list** [*HHHH.HHHH.HHHH* | *WORD*] [**detailed**]	Display RTDPdevice information
2	**show rtdp**	Display RTDPconfiguration

Use **show rtdp device-list** to check all the concise information for neighbour device:
Raisecom# show rtdp device-list

Use **show rtdp device-list detailed** to check detail information for all the finded devices:
Raisecom# show rtdp device-list detailed

Use **show rtdp device-list HHHH.HHHH.HHHH** to check the concise information of 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 designated MAC device:
Raisecom# show rtdp device-list HHHH.HHHH.HHHH detailed

Use **show rtdp device-list WORD** to check concise information for device with a designated host computer name.
Raisecom# show rtdp device-list WORD

Use **show rtdp device-list WORD detailed** to check detail information for the device with a designated host computer name:
Raisecom# show rtdp device-list WORD detailed

Use **show rtdp** to check RTDP configuration:

Raisecom# show rtdp

20.3.3. Display cluster management informaiton

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 candidate member 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

21. System log configuration

21.1. System log introduction

The system messages of the switch and some debugging information will be sent to system log. Based on the configuration of system log, the log information will be sent to: log file, console, TELNET, log host computer.

The general format of system log is:

timestamp module-level- Message content

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

21.2. System log configuration

The configuration for system log includes:

1 The enable and disable of system log
2 Time stamp configuration of system log.
3 The configuration of log speed.
4 Log information output configuration
5 Display log.

21.2.1. The enable and disable for system log

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

Example:

Raisecom#**config**

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

CONFIG-I:Configured from console ...

Raisecom(config)#**logging on**

set sucessfully!

Raisecom(config)#**exit**

Raisecom#**show logging**

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

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

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

Time-stamp logging messages: date-time

Log host information:

Target Address Level Facility Sent Drop

21.2.2. The time mark setting of log information

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

Example:

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

set sucessfully!

21.2.3. log rate configuration

Step	Command	Description
1	**config**	Enter global configuration mode
2	**logging rate <1-1000>**	Set the number of the log that will be sent per second.
3	**exit**	Back to privilege configurationmode

21.2.4. Log information output configuration

1,log information sent to console or TELNET

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

2,set logging host

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

The meaning for each term as following:

local0-local7 Device name for logging host
·**<0-7>** The log level
·**alerts** need immediate action (level=1)
·**critical** critical status (level=2)
·**debugging** debugging status (level=7)
·**emergencies** the system is not available (level=0)
·**errors** error condition (level=3)
·**informational** informational events (level=6)
·**notifications** the events in the critical conditions(level=5)
·**warnings** warning events (level=4)

Example:

Raisecom(config)#**logging console warnings**
set console logging information successfully
Raisecom(config)#**logging host 10.168.0.16 local0 warnings**
set log host logging information successfully
Raisecom(config)#**ex**
Raisecom#**show logging**
Syslog logging: enable, 0 messages dropped, messages rate-limited 0 per second
Console logging: enable, level=warning ,18 Messages logged
Monitor logging: disable, level=info ,0 Messages logged
Time-stamp logging messages: enable

Log host Information:

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

3,open log file

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

21.2.5.show log configuration

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

22. System clock

22.1. System clock

There are two ways to set the system clock of ISCOM switches: first, use SNTP protocol synchronize system time with the SNTP server computer, the SNTP protocol synchronized time is the Greenwich time, system will change the time to local time based on the time zone; second, manually configure the time, the manually configured time is the local time. System clock configuration includes:

1 Configure SNTP synchronized time
2 Manually configure system time.
3 Set summer time.

22.1.1. SNTP synchronized time

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

22.1.2. Manually configure system time

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

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

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

Note: when configure the time manually, if the system uses summer time, such

as the second Sunday of each April at 2 am to the second Sunday of each September at 2 am, in this time zone, clock should be move one hour ahead, that is time excursion for 60 minutes.

22.1.3. Set summer time

When the summer time is started, all the time that is synchronized by SNTP will be changed to summertime. the steps to configure summer as following:

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

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

Raisecom#**clock summer-time enable**

set sucessfully!

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

set sucessfully!

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

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

Timezone offset: +08:00:00

Summer time recuuring: Enable

Summer time start: week 02 Sunday Apr 02:00

Summer time end: week 02 Sunday Sep 02:00

Summer time Offset: 60 min

23. Loopback detection

23.1. Detection method

For an Ethernet network to function properly, only one active path can exist between two stations. Loops occur in network for a variety of reasons. So Spanning Tree Protocol (STP) was defined as a link management protocol that provides path redundancy while preventing undesirable loops from the network. STP is a technology that allows bridges/switches to communicate with each other to discover physical loops in the network. The protocol then specifies an algorithm that bridges can use to create a loop-free logical topology.

In practice, there is the possibility that users make loops un-aware, for example a family has more than one computer facility and they use a hub to let all the computers to access Internet. And this kind of loop will not be detected by STP but may result in broadcast storm. Raisecom provides loop-back detection function on our switches to avoid the loops making by our users. ISCOM2826 loop back detection function is based on each port. If there is loop in one port, that port will be shutdown automatically, and when the loop unchains the port will recover automatically. The detection period is configurable

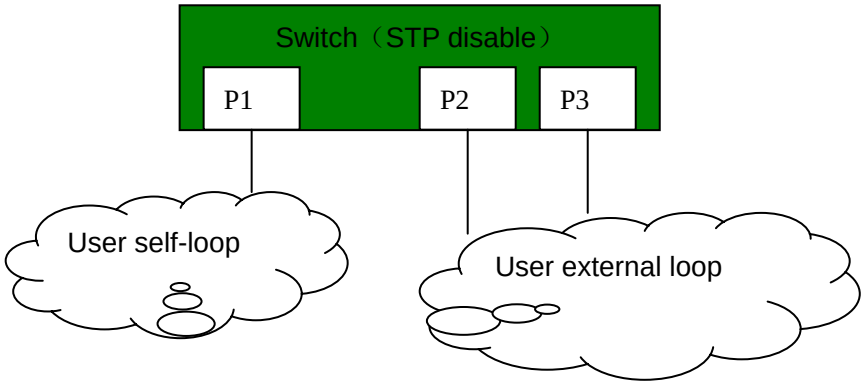


图 1

The procedure for finding the loop as following:

1. The switch (time interval can be set, usually is 4 seconds) sends Loopback-detection packets periodically;
2. Check the CPU MAC address of the received packets, if the CPU-MAC character section is the MAC of current switch, then there are some loops on the switch; otherwise, giving up;
3. If the packet sending port and the receiving port are the same, that is the self loop, otherwise, that is the external loop;
4. If there is loop happened, close the port which has bigger number.

23.2. loopback detection function configuration

Includes following two parts:

- Configure enable/disable loop detection function;

- Configure the hello time of loop detection

Configure enable/disable loop detection function:

Command	Description
config	Enter global configuration mode
loopback-detection { *enable* | *disable* **} port-list {** *port-list* | all **}**	Enable/disable the loop detection function of designated port. Default is enabled. *enable*,enable loop detection function; *disable*,close loop detection function *port-list: is the physical port number*,rangeis 1-26, use ","and "-" for multiple port input; *all*,all the ports;
exit	Withdraw global configuration mode and enter privileged configuration mode.
show loopback-detection	Show port detection status.

Configure loop detection time period:

Command	Description
config	Enter global configuration mode
loopback-detection hello-time <1-65535>	Configure loop detection time period. 1-65535,the time interval of sending loop detection packet, unit is second, default is 4 seconds;
exit	Withdraw global configuration mode and enter privileged user mode
show loopback-detection	Show loop detection statusof the port

Use global configuration command **no loopback-detection hello-time** to recover default setting.

Use **show loopback-detection** to show the loop detection status of the port.

Example: set the loop detection time period to 3 seconds. Enable all the loop detection function. Port 2 and port 6 form external loop. Port 9 form self loop. STP stopped already.

```
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: 3s
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       --
```

24. Schedule-list configuration

This function is used to periodicly excute particular command, timely maintain the configuration function of the switch. set a time character list by configuring a time list, this list includes a starting time, a periodic time and a ending time. There are two types of time characters, one is counted from the startup of the switch, that is a relevant time; another is a standard time(year,month and day, hour,minute and second), that is a absolute time.

This chapter includes following parts:

1,the setting for schedule-list;

2,schedule-list configuration based on command line;

24.1. The setting for schedule-list

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, this command is used to set the starting time, ending time, and time period of periodicly executed command. No format command is used to delete a schedule-list. *list-no* :schedule list range is <0-99>; **up-time** :Count from the system start, that is a relevant time; **date-time** :Based on the system time, that is a absolute time; *days time* :is a time section,input format is days: <0-65535>,time: HH:MM:SS, for example:3 3:2:1 *date time* : a time point,input format is MMM-DD-YYYY HH:MM:SS for example jan-1-2003 or 1-1-2003,the range of YYYY is from 1970 to 2199
Show schedule-list	Show schedule-list configure information

24.2. Schedule-list configuration based on command line

Command	Description
config	Enter global configuration mode
command-string **schedule-list** *list-no*	Support the command to the schedule-list
show schedule-list	Show schedule-list configuration information.

25. Trouble shooting command

25.1. trouble shooting

When something wrong happended in the system, use trouble shooting commands to solve the problem. Check contents including following commands:

1 Memory usage information
2 Port driving pool usage information
3 Process and stack status
4 Port UP/DOWN statistical information
5 Information gathering for trouble shooting

25.1.1. Memory usage information

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

Example:

```
Raisecom#show memory

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

SUMMARY:
  status     bytes       blocks     avg block    max block
  ------ --------- -------- ---------- ----------
current
     free    34120840           5      6824168    32017512
    alloc    23460160       62554          375           -
cumulative
    alloc    23591248       64754          364           -
```

25.1.2. Port driving pool usage information

Step	Command	Description
1	**show buffer [port** <1-26>**]**	Check the port driving port usage information

Example

```
Raisecom(config)# show buffers port 2
Port 2
------------------------------------------------------------
Total mBlks: 500        Free mBlks: 500        DATA: 0

HEADER:   0          SOCKET:   0          PCB:        0
```

RTABLE: 0 HTABLE: 0 ATABLE: 0

SONAME: 0 ZOMBIE: 0 SOOPTS: 0

FTABLE: 0 RIGHTS: 0 IFADDR: 0

CONTROL: 0 OOBDATA: 0 IPMOPTS: 0

IPMADDR: 0 IFMADDR: 0 MRTABLE: 0

25.1.3. Process and stack status

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

Example:

Raisecom#**show processes**

Task Information :

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

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

TSD- task delay;DTS-dead task

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

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

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

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

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

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

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

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

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

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

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

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

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

2db3bd0 tCOUNTER.0 15896 50 3d0004 (3 / 0.0%)

27d9500 tScrnBg_0 13888 50 RDY 30067 (28 / 0.0%)

27d1c78 tScrnBg_1 16192 50 POS 0 (0 / 0.0%)

27ca4e0 tScrnBg_2 16192 50 POS 0 (0 / 0.0%)

27c2d48 tScrnBg_3 16192 50 POS 0 (0 / 0.0%)

27bb5b0 tScrnBg_4 16192 50 POS 0 (0 / 0.0%)

27b3e18 tScrnBg_5 16192 50 POS 0 (0 / 0.0%)

2a6ba58 tRndpRecv 7944 51 POS 0 (0 / 0.0%)

2a632d0 tRtdpRecv 7912 51 POS 0 (1 / 0.0%)

2907680 tCcomTm 840 55 TSD 0 (2 / 0.0%)

348df68 tSntpS 4344 56 POS 0 (0 / 0.0%)

2a7c008 tDhcpS 19464 56 0 (0 / 0.0%)

```
2a6f480          tLoopD      3944     60      TSD          0   (     10 /   0.0%)
2906408            tCcom     3848     60      POS          0   (      2 /   0.0%)
2a1e7f0            tRmon    32632     75      TSD    81000c   (     15 /   0.0%)
2a11358     tPortStats      3632     75      TSD          0   (      6 /   0.0%)
2a0aeb8       tLinkTrap     8040     75      TSD          0   (      2 /   0.0%)
2a06868       tColdTrap     3944     75      TSD          0   (      1 /   0.0%)
2a23a38         tIgmpTm     2848    100      TSD          0   (      0 /   0.0%)
2a22c20      tIgmpSnoop     3816    100      POS          0   (      0 /   0.0%)
2a21a08           tSnmp    11816    100      POS          0   (      0 /   0.0%)
2a16590         tIpBind     3904    100      TSD    81000c   (      1 /   0.0%)
2a08b78        tEndStat     7832    100           3d0004   (      0 /   0.0%)
29e2558       tRmonAlrm     7976    100      POS          0   (      2 /   0.0%)
27aea90 tTelnetdOut0       3336    100      POS          0   (      0 /   0.0%)
27ad878   tTelnetdIn0      3384    100      POS          0   (      0 /   0.0%)
27ac610 tTelnetdOut1       3336    100      POS          0   (      0 /   0.0%)
27ab3f8   tTelnetdIn1      3384    100      POS          0   (      0 /   0.0%)
27aa190 tTelnetdOut2       3336    100      POS          0   (      0 /   0.0%)
27a8f78   tTelnetdIn2      3384    100      POS          0   (      0 /   0.0%)
27a7d10 tTelnetdOut3       3336    100      POS          0   (      0 /   0.0%)
27a6af8   tTelnetdIn3      3384    100      POS          0   (      0 /   0.0%)
27a5890 tTelnetdOut4       3336    100      POS          0   (      0 /   0.0%)
27a4678   tTelnetdIn4      3384    100      POS          0   (      0 /   0.0%)
27a3460       tTelnetd     3640    100      POS          0   (      0 /   0.0%)
3489320         tSyslog     7968    105      POS          0   (      0 /   0.0%)
2daaac8           tx_cb    15912    110      POS          0   (      0 /   0.0%)
348f558      tSntpCLsn      4760    150      TSD          0   (      1 /   0.0%)
2a52d20         tRelay      3880    151      POS          0   (      0 /   0.0%)
2da0958             rx0    15888    200           3d0004   (     29 /   0.0%)
2cc1c98      tArlAging      1896    200      TSD          0   (      0 /   0.0%)
2b38248         tSnmpTm     3856    200      POS          0   (      0 /   0.0%)
2c25d60       tRosInit      5912    250      POS    81000e   (      0 /   0.0%)
27af260           tIdle       568    251      RDY          0   (    281 /   0.0%)
```

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

25.1.4. UP/DOWN statistical information

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

Example:

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

The above example means that when the device is enabled: port 19 up/down twice,

there is no up/down happened within this minute; port 21 up/down twice, and up/down twice happened twice with this minute.

25.1.5. Information gathering for trouble shooting

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

This command displays trouble shooting needed information gathering, including:

1 Version information(show version)
2 Current configuration information(show running-config)
3 Current CPU occupation rate(show cpu-utilization)
4 Memory usage information(show memory)
5 Port driving pool usage information(show buffer)
6 Process information(show processes)
7 Flash file(dir)
8 Current system time(show clock)
9 Port status information(show interface port)
10 Port statistics informaton(show interface port statistics)
11 Port Up/Down statistics information(show diags link-flap)
12 SNMP statistics information(show snmp statistics)
13 Spanning tree information(show spanning-tree)
14 Static VLAN information(show vlan static)
15 ARP information(show arp)
16 Trunk information(show trunk)
17 TCP connection status.

26. VLAN Configuration

The switch introduces how to configure VLAN on the switch, including following contents:

1,VLAN introduction

2,VLAN configuration list:

3,Monitor and maintenance

26.1. VLAN introduction

A VLAN is a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. In the function point of view, VLAN and LAN have the same characteristics. But there is no physical limitation for VLAN member. For example, the users connected to the same switch can belong to different VLAN, users connected to different switchs can also belong to the same VLAN. The broadcast domain and multicast domain of the VLAN is relevant to VLAN member. Multicast, broadcast, and unicast will not be sent to the other VLAN. Only layer-3 switch or router can communicate different VLANs. Since the above characterics, it is convenient for the users to use VLAN to separate different users of the network. So the network bandwidth usability and security are improved a lot.

Following is a typical VLAN topology figure:

VLAN topology:

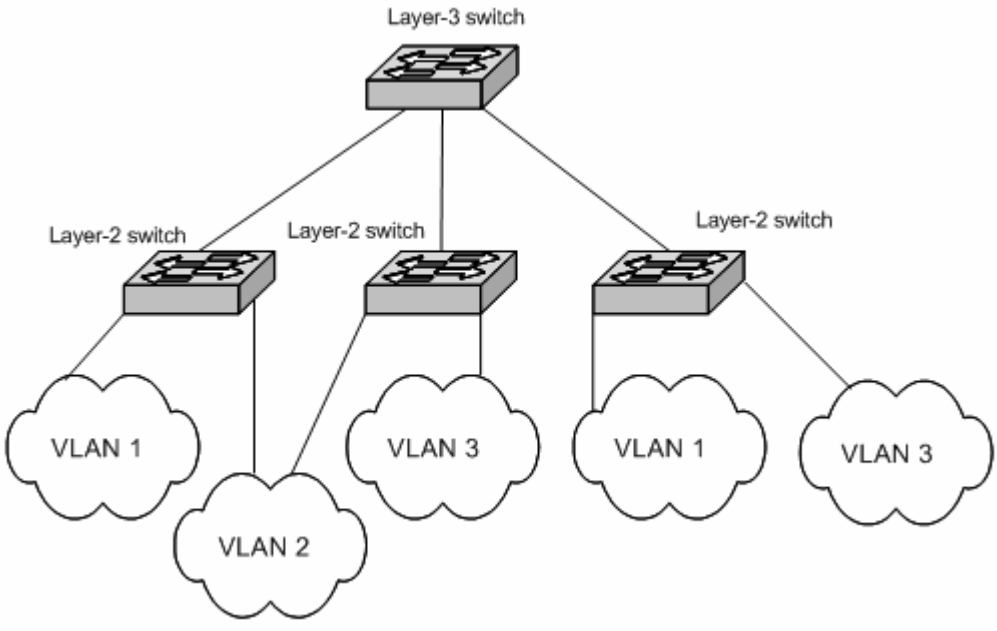


Figure 9-1 VLAN topology

In the real network application, vlan is always corresponding to an IP subnet, as above figure, VLAN 1 is corresponding to 10.0.0.0/24 network, VLAN 2 is corrpesponding to 20.0.0.0/24 network. Though they are isolated at layer two, but at layer three, they can interconnect with each other through layer-3 switch.

26.2 VLAN member port mode

Port member mode	VLAN member attributes
Access	Access port mode can only be assigned to one VLAN, the data packet that is sent from Access port doesn't have 802.1Q mark, the Access port in different VLAN cannot be interconnected.
Hybrid	Hybrid port mode can be assigned to several VLANs, and it can also limit whether the data packet has 802.1Q VLAN or not. At the same time, hybrid port configure Native attribute and use it to classify non-802.1Q data packet that is entering the port.
Trunk	Trunk port mode exists in all the VLAN, and all the data packets (except for Native VLAN) have 802.1Q mark. But users can use allowed vlans attribute to limit VLAN data packet that is transmitted by the Trunk port.

26.2. VLAN configuration list

VLAN configuration includes following contents:

1,Create and delete VLAN;

2,VLAN name configuration;

3,VLAN active attribute configuration;

4,VLAN mode of the port and relevant attributes;

5,Monitor and maintenance.

26.2.1.Create and delete VLAN

There are two VLANs in the system, they are default VLAN (VLAN 1) and cluster VLAN (VLAN 2), all the port are Access attributes belongs to default VLAN. Default VLAN cannot be deleted. When it is needed to create the new VLAN, based on following steps:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**vlan** *<3-4094>*	Create VLAN, and enter configuration mode.
3	**exit**	Back to global configuration mode
4	**exit**	Back to privilege user mode
4	**show vlan**	Show VLAN configuration information

The new created VLAN is in hang status, if the users hope that it is active in the system, following **state** command is also needed.

Take following steps to delete a VLAN:

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

Following example is to create VLAN 3, and use show command to check configuration:

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
```

26.2.2.VLAN name settings:

In order to make the setting of VLAN name convenient for the users,the name of default VLAN (VLAN 1) is “Default”, the name of cluster VLAN (VLAN 2) is “Cluster-Vlan”, the name of other VLAN is the string “VLAN”plus four digits VLAN ID, for example, for example, the default name of VLAN 1 is “VLAN0001”,VLAN 4094 default name is “VLAN4094). Configuration steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**vlan** *<3-4094>*	Enter corresponding VLAN configuration mode.
3	**Name** *WORD*	Name VLAN
4	**Exit**	Back to global configuration mode.
5	**Exit**	Back to privilege user mode
6	**show vlan**	Show VLAN configuration

The following example is to set VLAN 2 name to “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
```

26.2.3.VLAN active status settings

Only if the VLAN is active, all the settings of VLAN will be effective in the system. If the status of VLAN is suspended, user can configure the VLAN. For example delete/add port, set VLAN name etc. The system will save these settings; all the settings will be effective if the VLAN is actived. Set the VLAN active stutus as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**vlan** *<3-4094>*	Enter corresponding VLAN configuration mode
3	**state** {**active	suspend**}	Set the active status of VLAN.
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege user mode.
6	**show vlan**	Show VLAN configuration information.

Following example is to set the active status of VLAN 2 to active:

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

26.2.4. VLAN mode of port and relevant attributes setting

Configure the VLAN mode of the port under physical interface configuration mode, steps as following:

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

Recover the port VLAN mode to default Access mode, steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <*1-26*>	Enter corresponding physical interface configuration mode.
3	**no switchport mode {access | hybrid | trunk }**	Recover the VLAN mode of the port to default mode.
4	**exit**	Back to global configuration mode.
5	**exit**	Back to privilege user mode
6	**show vlan**	Show the port VLAN attribute

Following example is to set physical interface 2 to 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 of Access,Extend-access,Tunnel ports

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <1-26>	Enter corresponding physical interface configuration mode
3	**switchport access vlan** *<1-4094>*	Set the Access VLAN of the port
4	**exit**	Back to privilege configuration mode.
5	**exit**	Back to privilege user mode
6	**show interface port** [{*1-26*}] **switchport**	Show the VLAN attributes of the port.

Recover Access VLAN to default VLAN 1, steps as following:

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

Set the Access VLAN of the physical port 24 to 4094:

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 Hybrid port allowed VLAN,steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <1-26>	Enter corresponding physical interface configuration mode
3	**switchport hybrid allowed vlan**	Configure Hybrid port allowed

	{**all |** {*1-4094*} }	VLAN
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege use mode
6	**show interface port** [{*1-26*}] **switchport**	Show the VLAN attributes configuration of VLAN

Recover Hybrid port allowed VLAN list to 1-4094, steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <*1-26*>	Enter corresponding physical interface configuration mode
3	**no switchport hybrid allowed vlan**	Recover the Hybrid port allowed VLAN list.
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege user mode.
6	**show interface port** [{*1-26*}] **swithport**	Show port VLAN attrivute configuration

Set the physical interface 3 to Hybrid mode allowed VLAN 1-100:

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 Hybrid port allowed Untagged VLAN, steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <1-26>	Enter corresponding physical interface configuration mode
3	**switchport hybrid untagged vlan** {**all |** {*1-4094*} }	Set Hybrid port allowed Untagged VLAN.
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege user mode.
6	**show interface port** [{*1-26*}] **swithport**	Show port VLAN attribute configuration.

Recover Hybrid port allowed Untagged VLAN list to 1-4094, steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <*1-26*>	Enter corresponding physical interface configuration mode
3	**no switchport hybrid untagged vlan**	Recover Hybrid port allowed Untagged VLAN list
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege user mode
6	**show interface port** [{*1-26*}] **swithport**	Show port VLAN attribute configuration

Following example is to set phycial port 3 to Hybrid mode allowed Untagged VLAN 3-100:

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 Trunk port allowed VLAN, steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <1-26>	Enter corresponding physical interface configuration mode
3	**switchport trunk allowed vlan** {**all |** {*1-4094*} }	Set Trunk port allowed VLAN
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege user mode
6	**show interface port** [{*1-26*}] **switchport**	Show port VLAN attribute configuration

Recover Trunk port allowed VLAN list to 1-4094, steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <*1-26*>	Enter corresponding physical interface configuration mode
3	**no switchport trunk allowed vlan**	Recover Trunk port allowed VLAN list

4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege user mode
6	**show interface port** [{*1-26*}] **switchport**	Show port VLAN attribute configuration

Following example is to set the physical port 3 to Trunk mode allowed VLAN 1-100:

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 of Trunk, and Hybrid port, steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <1-26>	Enter corresponding physical interface configuration mode
3	**switchport native vlan** <*1-4094*>	Set Native VLAN of Trunk portand Hybrid port
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege user mode
6	**show interface port** [{*1-26*}] **swithport**	Show port VLAN attrivute configuration

Recover the Native VLAN of Trunk port and Hybrid port, steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <*1-26*>	Enter corresponding physical interface configuration mode
3	**no switchport native vlan**	Recover Native VLAN of Trunk port, and the Hybrid port.
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege user mode
6	**show interface port** [{*1-26*}] **swithport**	Show port VLAN attrivute configuration

Following example is to set the Native VLAN of physical interface 3 to VLAN 100:

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

26.2.5.Monitor and maintenance

Users can use two **show** command to check VLAN relevant configuration, realizing the monitor and maintenance for the VLAN:

Command	Description
show vlan [{*1-4094*}]	Show VLAN configuration information
show interface port [{*1-26*}] **swithport**	Show VLAN relevant configuration of physical interface.

Use **show vlan** to check VLAN that is created by CLI or SNMP, including current VLAN and suspended VLAN:

Raisecom#**show vlan**

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

Use **show interface port** [{*1-26*}] **swithport** to check the port VLAN attribute set by 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

27. Port Statistics

27.1. Introduction to port statistics

The introduction of this chapter only suits for ISCOM2026 switch.

ISCOM2026 supports the packet statistics based on the port. User can use this command to set the statistics packet type of designated port. Ingress packet types statistics includes: received good packets, received bad packets, received local packets, default statistical ingress packet. Egress statistics packets type include: sent good packet, sent bad packet, dropped packet, and default egress packet.

27.2. Port statistics configuration

Set the type of statistics packet on designated port.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port** <1-26>	Enter Ethernet physical interface mode.
3	**statistic packet ingress {good |bad |local} egress {good |bad |abort}**	Set the type of port statistics packet
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege user mode
6	**show interface port [<1-26>] statistics**	Show port statistics information

Set port 2 statistics port egress bad packet and ingress bad packet:

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. Monitor and maintenance

User use **show** command to check the packet statistics information for the port:

Command	Description
Show interface port [{*1-26*}] **statistics**	Show the packet statistic information for the physical port.

Example:

Set the egress good packet and ingress bad packet of port 2, and check the packet statistics information for 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)

28. ACL and network security setting

28.1. ACL introduction

Packet filtering can limit network traffic and restrict network use by certain users or devices. ACLs can filter traffic as it passes through a switch and permit or deny packets at specified interfaces.

In access-list configuration mode, An ACL is a sequential collection of permit and deny conditions that apply to packets. When an interface receives a packet, it will compare the fields in the packet against the conditions in access list one by one.

ACLs permit or deny packet forwarding based on how the packet matches the entries in the ACL. For example, you can use ACLs to deny the access of packets from VLAN 5.

If the access list type is deny, then all the access of data packet will be denied if conditions are matched; if the access type is set to permit, the access of data packe will be permitted if conditions are matched;.

28.2. configure ACL

Relevant configuration command as following:

1 Configure MAC ACL

The switch can define 400 layer-2 (MAC) ACL that numbered from 0 to 399. Layer-2 ACL will deny or permit packets based on the following fields: the source MAC address, destination MAC address, source VLAN ID, and Ethernet length/type etc.

Command	Description
config	Enter global configuration mode
mac-access-list *list-number* {**deny** | **permit**} [*protocol* | **any**] {*source-MAC-address* **| any**} {*destination-MAC-address* | **any**}	Set MAC access list. *list-number series number of ACL, range is 0-399*. **deny|permit** deny|permit access. [*protocol* | **any**] binding protocol type,**any** stands for there is no limitation for the protocol type. *source-MAC-address:* the set source MAC address, format is “HHHH.HHHH.HHHH” is hex and stands for any source MAC address. *destination-MAC-address: is the destination MAC address, format is* “HHHH.HHHH.HHHH” is hexdecimal characters, each four characters dotted separated; any stands for any source MAC address. **any** stands for any destination MAC address.
exit	Back to global configuration mode and enter privileged user mode.
show mac-access-list *list-number*	Show MAC ACL. *list-number*: is the series number of MAC ACL that will be displayed, range is 0-399.
no mac-access-list	Delete the set MAC ACL

list-number	*list-number:* the series number that will be deleted.

Example: the source MAC address is 1234.1234.1234, destination MAC address is 5678.5678.5678,protocol is IP and access type is deny. Source MAC address is 1111.2222.3333, destination MAC address is 4444.5555.6666, protocol is ARP, access type is 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 Configure IP ACL

The switch can define 400 IP ACL as the maximum (the range of digital mark is 0~399). It will design the classification rule based on the IP header information including the source IP, destination IP, and information about the port number of using TCP or UDP. The buildup of data packet IP header refers to RFC791 relavent 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**} [*destination-protocol-port*]	**ip-access-list:** set the Access Control List of IP address. ***list-number*** **IP**: the serial number of ACL, range is 0-399. **deny|permit**: deny|permit the access. ***Protocol*** *is the* bindled protocol type ***source-address mask*** **| any** is the souce IP address and its mask, format is A.B.C.D; dotted decimal; **any** stands for any address. ***source-protocol-port*** is the TCP/UDPprotocol source port. *destination -address mask* | **any** *is the target IP address and its mask,* format is A.B.C.D; dotted decimal; **any** stands for any address. *destination -protocol-port* is the destination port ofTCP/UDP.
exit	Withdraw global configuration mode and enter privileged user mode.
show ip-access-list *list-number*	Show IP ACL relevant information. *list-number:* to show the serial number of IP ACL, range is 0-399.
no ip-access-list *list-number*	Delete IP ACL *list-number:* the list serial number that will be deleted.

Example:

The source IP address is 192.168.1.0 network section, destination IP address is in any network section, protocol type is IP, access type is deny.
Source IP address is 10.168.1.19, mask is 255.255.255.255, source protocol port is 80, destination address is any, any port, protocol type is TCP; access type is deny.
The source IP address is 10.168.1.19, mask is 255.255.255.255, destination address is 10.168.0.0 network section, protocol type is TCP, and access type is permit.

```
raisecom#config
raisecom(config)#ip-access-list 0 deny ip 192.168.1.0 255.255.255.0 any
raisecom(config)#ip-access-list 1 deny tcp 10.168.1.19 255.255.255.255 80 any
raisecom(config)#ip-access-list 2 permit tcp 10.168.1.19 255.255.255.255 80 10.168.0.0
255.255.0.0 80
raisecom(config)#exit
raisecom#show ip-access-list
Src Ip: Source Ip Address
Dest Ip: Destination Ip Address
```

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

3 Set the ACL map table

User can define 400 ACL map table as the maximum (the range of digital mark is 0~399). ACL map table can define protocol field in detail, and it's better in detail than IP ACL and MAC ACL. Based on any byte in the front 64 bytes of the second layer data frame, ACL map table can also match and takes corresponding actions to the data packet based on the matching result.

ACL map table uses **match** command to set desired field. The matching fields should not conflict with others in the same ACL map table, the field that can be configured as following:

- Mac destination address
- Mac source address
- Ethernet protocol type
- CoS
- ARP protocol type
- The hardware address of ARP protocol sender
- The hardware address of ARP protocol receiver.
- The IP address of ARP protocol sender.
- The IP address of ARP protocol receiver.
- The destination address of IP
- The source address of IP
- IP priority
- IP ToS
- IP dscp

- IP segment mark
- IP protocol type
- TCP destination port
- TCP protocol source port
- TCP protocol mark
- UDP protocol destination port
- UDP protocol source port
- ICMP protocol message type
- ICMP protocol message code
- IGMPprotocol message type

User can pick up any byte from the front 64 bytpes in the data frame based on regular mask and regular, and then compare it with user defined byte to filter out the matching data frame for corresponding actions. The user-defined rule can be some fixed attributes of data.

Note: the rule should be hex decimal figure, offset includes 802.1Q VLAN TAG field, that is switch received the untag packet.

Command	Description
config	Enter global configuration mode
access-list-map *list-number* {**deny** | **permit**}	*list-number*:the serial number of the list,range is 0-399. **deny|permit** deny|permit data packet pass.
match mac {destination|source} *HHHH.HHHH.HHHH*	**destination|source** matching source mac or destination mac. *HHHH.HHHH.HHHH* is mac address
match cos <0-7>	<0-7> match cos value
match ethertype *HHHH [HHHH]*	*HHHH[HHHH]* match Ethernet frame 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 flowcontrol protocol **ip**——match ip **ipv6**——match ipv6 **loopback**——match loopback **mpls**——match mpls unicast protocol **mpls-mcast**——match mpls multicast protocol **pppoe**——match pppoe protocol **pppoedisc**——match pppoe discovery protocol **x25**——match x25 protocol **x75**——match x75 protocol
no match mac {destination|source}	Do not match MAC address **destination|source** match source mac or desitnation mac
no match cos	Do not match cos value
no match ethertype	Do not match Ethernet frame type
match arp opcode {request | reply}	Match arp protocol type **request | reply** arp protocol response packet/request packet
match arp {sender-mac| target-mac}	Match arp hardware address **sender-mac| target-mac** match arp

HHHH.HHHH.HHHH	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	Do not match arp protocol type
no match arp {sender-mac| target-mac}	Do not match arp hardware address **sender-mac| target-mac** match arpsender/target mac address
no match arp {sender-ip| target-ip}	Do not match arp protocol IP address **sender-ip| target-ip** sender/receive IP address
match ip {destination-address | source-address} *A.B.C.D [A.B.C.D]*	Match IP address **destination-address | source-address** IP source address | destination 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 priority <0-7>—— IP priority value **routine**—— IP priority value 0 **priority**—— IP priority value 1 **immediate**—— IP priority value 2 **flash**—— IP priority value 3 **flash-override**—— IP priority value4 **critical**—— IPpriority value5 **internet**—— IPpriority value6 **network**—— IPpriority value7
match ip tos {<0-15> **| normal | min-monetary-cost | min-delay | max-reliability | max-throughput}**	Match IP priority ToS value <0-15>——TOS value **normal**——normal TOS value(0) **min-monetary-cost**——*least expense* TOS value(1) **min-delay**——minimum delay TOS value(8) **max-reliability**——*max-realiable* 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(priority 1) dscp value(001000) **cs2**——CS2(priority 2) dscp value(010000) **cs3**——CS3(priority 3) dscp value(011000) **cs4**——CS4(priority 4) dscp value(100000)

	cs5——CS5(priority 5) dscp value(101000) **cs6**——CS6(priority 6) dscp value(110000) **cs7**——CS7(priority 7) dscp value(111000) **default**——default dscp value(000000) **ef**——EF dscp value(101110)
match ip no-fragments	Match but do not 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}	Matck IP protocol **ahp**——*authentication header protocol* **esp**——*encapsulation security protocol* **gre**——一 general route encapsulation protocol **icmp**——internet information control protocol **igmp**——*internet group message protocol* **igrp**——*interfal network gateway protocol* **ipinip**——IP-in-IP tunnel **tcp**——transmission control protocol **udp**——user data packet protocol
no match ip {destination-address | source-address}	Do not match IP address **destination-address | source-address** IP
no match ip precedence	Do not match IPpriority
no match ip tos	Do not matchIP ToS value
no match ip dscp	Do not match IP dscp value
no match ip no-fragments	Do not match IP, no gragments
no match ip protocol	Do not match Ip protocol
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** TCPprotocol port destination-port|source-port **<**0-65535>——tcp port number **bgp**——*bounder gateway protocol (*179) **domain**——*domain name server protocol(*53) **echo**——echo protocol(7) **exec**——Exec (rsh, 512) **finger**——Finger (79) **ftp**——*file transmission protocol*(21) **ftp-data**——FTP data connection(20) **gopher**——Gopher (70) **hostname**——NIC hostname server (101) **ident**——identification protocol (113) **irc**——IRC protocol (194) **klogin**——Kerberos login (543) **kshell**——Kerberos shell (544) **login**——Login (rlogin, 513) **lpd**——printer server protocol (515) **nntp**——network news transmission protocol **pim-auto-rp**——PIM Auto-RP (496) **pop2**——*electronic postoffice protocol v2* (109) **pop3**——electronic postoffice protocol v3(110)

	smtp——*simple mail transmission protocol* (25) **sunrpc**——Sun remote process control(111) **syslog**——system log (514) **tacacs**——TAC achieve control system (49) **talk**——Talk (517) **telnet**——Telnet (23) **time**——Time (37) **uucp**——Unix-to-Unix complex program(540) **whois**——Nicname(43) **www**—— *global www* (HTTP, 80)
match ip tcp {ack | fin | psh | rst | syn | urg }	Match TCP protocol mark **ack**——matchACK digit **fin**——matchFIN digit **psh**——matchPSH digit **rst**——matchRST digit **syn**——matchSYN digit **urg**——matchURG digit
no match ip tcp { destination-port | source-port}	Do not match Tcp protocol port **destination-port | source-port** TCP desination/source port.
no match ip tcp {ack | fin | psh | rst | syn | urg }	Do not match TCP protocol mark digit **ack**——matchACK digit **fin**——matchFIN digit **psh**——matchPSH digit **rst**——matchRST digit **syn**——matchSYN digit **urg**——matchURG digit
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 }**	Matchudp protocol port number **destination-port | source-port** TCP protocol destination-port| sourc-port. <0-65535>——udp port number **biff**——Biff (mail notification, comsat, 512) **bootpc**—— boot protocol(BOOTP) client end (68) **bootps**——boot protocol (BOOTP) server end (67) **domain**——*domain name service protocol(*53) **echo**——echo protocol(7) **mobile-ip**——mobileIP registeration(434) **netbios-dgm**——NetBios data message server(138) **netbios-ns**——NetBios name service(137) **netbios-ss**——NetBios section server 139) **ntp**——*network time protocol*(123) **pim-auto-rp**——PIM Auto-RP (496) **rip**——*route information protocol*(520) **snmp**——*simple network management protocol management protocol*(161) **snmptrap**——SNMP Traps (162) **sunrpc**——Sun remote process control (111)

	syslog——*system log* (514) **tacacs**——TAC achieve control system (49) **talk**——Talk (517) **tftp**——*simple file transmission protocol* (69) **time**——Time (37) **who**——Who service (rwho, 513)
no match ip udp { destination-port | source-port}	Do not match udp protocol port number **destination-port | source-port** TCP protocol destination-port| source port
match ip icmp <0-255> [<0-255>]	Match icmp protocol message type. <0-255> [<0-255>] the type of message [message code]
match ip igmp {<0-255> **| dvmrp | query | leave-v2 | report-v1 | report-v2 |report-v3 | pim-v1 }**	Match the message type of igmp protocol <0-255>——IGMP message type **dvmrp**——*distance vector multicast route protocol* **leave-v2**——IGMPv2 leaving group **pim-v1**——*protocol individual multicast version 1.* **query**——IGMP member request **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-define string. *rule-string:* the user-defined rule string, should be hex-decimal figure, characters should not be more than 64. *rule-mask:mask rule*,used for the "and" operation with the data packet. <0-64>*:*offset,take the header of the data packet as the norm, specify the "and" operation from which character.
no match user-define	Do not match user-define string
exit	Withdraw global configuration mode and enter privilege configuration mode.
show access-list-map [*list-number*]	Show the ACL map table of the port *list-number:* the serial number of port ACL map table, range is 0-399.
no access-list-map *list-number*	Delete user-defined ACL *list-number* the list number that will be deleted.

Example:

Set the begging filter data to 123456 at the 40 byte of physical frame, and access type is deny.

Filter ARP protocol request packet.

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. use ACL at second layer physical interface or on the VLAN

The configuration steps for using ACL at second layer interface or VLAN as following:

A. Define ACL

Refer to previous part

B. Set the fileter

User are needed to set filter when the setting for ACL has been done. When the filter is effected, whether the configuration is effective or not will up to the on-off of global status. There is a special command to effective ACL, or delete the filter that has been effectived. Use no filter command to delete corresponding rules. If the filter rule has been written into the hardware, delete the filter rule from the hardware and delete it from the configuration.

The filter rules on a physical port or VLAN are made up of several “permit|deny” commands. The ranges of designated data packet are different. There are problems in the matching sequence when match a data packet and access control rule. The matching sequences of ACL are based on the sequence of filter rule: the later it is in the sequence, the higher priority it has.

There are four types of configuration methods, one is based on the switch, one is based on the port, one is based on the traffic from ingress port and egress port, and another one is based on VLAN.

1 based on the switch

Command	Description
config	Enter global configuration mode
[no] filter (**ip-access-list | mac-access-list | access-list-map**) {*acllist* | **all**}	Based on the filtering of the switch **ip-access-list**: the filter use IP ACL **mac-access-list**: the filter use MAC ACL **access-list-map**: filter is using user-defined ACL *acllist* | **all***:* the range of filter used ACL, all means that all the configured ACLs.
exit	Withdraw global configuration mode and enter privilege configuration mode.
show filter	Show all the filtering status

2 based on the 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* }	The filtering based on the port **ip-access-list**: filter uses IP ACL. **mac-access-list** filter uses MAC ACL. **access-list-map**: filter is using user-defined ACL. *acllist* | **all** *:* the range of serial number list, all

	means that all the configured ACL. **ingress | egress** filter at the ingress direction and egress direction. **port-list**: is used to filter at physical port. *portlist*: range of physical port list
exit	Withdraw global configuration mode and enter privilege user mode.
show filter	Show all the setted filtering status.

3 Based on traffic 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 traffic filtering from ingress port to egress port. **ip-access-list** the filter uses IP ACL. **mac-access-list** filter uses MAC ACL. **access-list-map**: filter uses user-defined ACL. *acllist* | **all***: the range of serial number list that is used by the filter, all the ACL that have been configured.* **from to** direction *ingress-port* *egress-port*
exit	Withdraw global configuration mode and enter privilege user mode.
show filter	Show the filter status for all the settings

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 that is based on VLAN. **ip-access-list** the filter uses IP ACL. **mac-access-list**: filter uses mac ACL. **access-list-map** filter uses user-defined ACL. *acllist* | **all**: *the range of serial number list that is used by the filter, all the ACL that have been configured.* **Vlan** filter is based on VLAN. *vlanid* VLAN.
exit	Withdraw global configuration mode and enter privilege user mode.
show filter	Show all the configured filter status.

C. Enable the filter

This command is used to enable or disable the corresponding ACL, and default status is disabled. If the configuration is enabled, user is needed to enable privously defined filter rule immediately, but also should enable all the filter rules immediately that are configured after the configuration.

Command	Description
config	Enter global configuration mode
filter (enable | disable)	**enable** the filter function is just enabled. **disable** the filter function is going to be disabled.
exit	Withdraw global configuration mode and enter privilege user mode.
show filter	Show all the configured filter status.

Example:

1 the switch deny the TCP packet passthrough at 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 deny any ARP packet that is sent from port 2-8 to destination with mac address 000e.3842.34ea

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 only allow the IP packet passthourgh for the source IP address at 10. 0.0.0/8 network section.

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. Use ACL on third layer interface

Use ACL configuration on third layer interface:

A. Define ACL.

Refer to 28.2

B. Set ACL

The ACL on the third layer interface are made up of several “permit|deny” commands. To these commands, the ranges of designated data packet are different. There are problems in the matching sequence when match a data packet and access control rule. The matching sequences of ACL are based on the sequence of filter rule: the later it is in the sequence, the higher priority it has.

Command	Description
config	Enter global configuration mode
interface ip <0-14>	Enter Ethernet third layer interface configuration mode
[no] ip ip-access-list {**all**| *acllist*}	Set the filter based on third layer interface. **ip-access-list** filter uses IP ACL *acllist* | **all** *the sequence list range of filter used ACL, all is all the configured ACL.*
exit	Withdraw Ethernet third layer interface configuration mode and enter global configuration mode.
exit	Withdraw global configuration mode and enter privilege user mode.
show interface ip ip-access-list	Show all the layer interface filter status.

Example:

1 The switch only allow the IP packet access of 10.0.0.0/8 network section:

```
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
```

29. QoS Configuration

This chapter introduces the QoS function of ISCOM switches and their configuration method. Use OoS function to realize the traffic management, and it also privode end-to-end service quanlity assurance for customers' business.

29.1. QoS Introduction

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

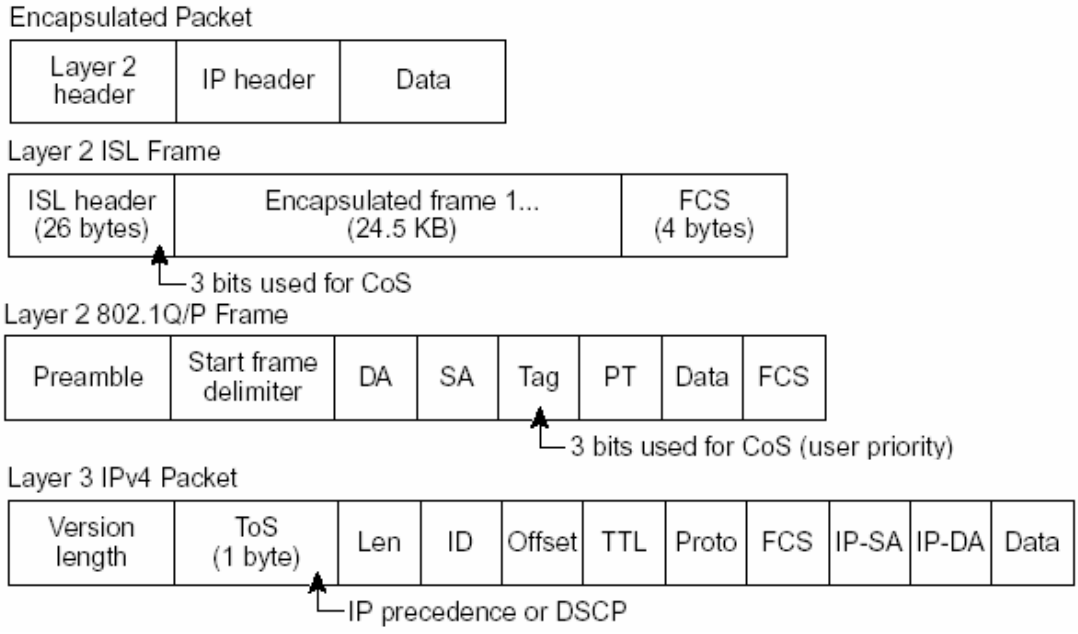
When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to give preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The realization of QoS mechanism on ISCOM2800 is based on 802.1P, 802.1Q standards and classify on layer-2 packets.

• Prioritization values in Layer 2 frames
Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the class of service (CoS) value in the three most-significant bits, which are called the User Priority bits.

• Prioritization bits in Layer 3 packets
Layer 3 IP packets can carry a Differentiated Services Code Point (DSCP) value. The supported DSCP values are 0-63

The following figure shows QoS classification Layers in frames and packets:



CoS defined eight kinds of priority can be used for the classification for following eight messages:

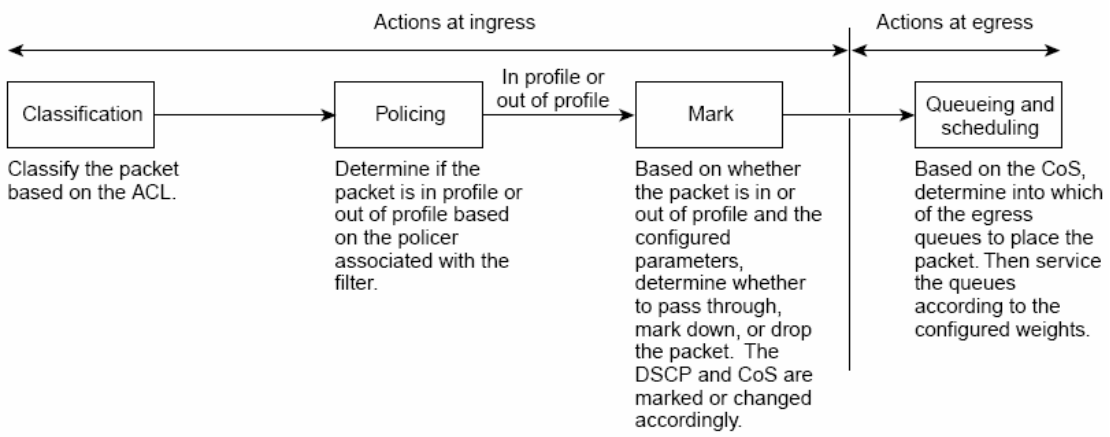
000	Routine
001	Priority
010	Intermediate
011	Flash
100	Flash Override
101	Critical
110	Internet Control
111	Network Control

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

Following is the basic model for QoS:
The action as ingress port includes traffic Classifying, Policing and Marking:

1. Classifying distinguishes one kind of traffic from another.
2. Policing determines whether a packet is in or out of profile according to the configured policer, and the policer limits the bandwidth consumed by a flow of traffic. The result of this determination is passed to the marker.
3. Marking evaluates the policer and configuration information for the action to be taken when a packet is out of profile and decides what to do with the packet (pass through a packet without modification, mark down the DSCP value in the packet, or drop the packet).

Actions at the egress interface include queueing and scheduling:
• Queueing evaluates the CoS value and determines which of the four egress queues in which to place the packet.
• Scheduling services the four egress queues based on their configured weighted round robin (WRR) weights.



29.1.1. Classification

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet. Only when global QoS is enabled, the classification can be enabled. QoS is disabled by default.
User can specify particular domain in the frame or packet to classify incoming traffic, to non-IP traffic, the classification process as following:

For non-IP traffic, you have these classification options:

1. Use the port default. If the frame does not contain a CoS value, the switch assigns the default port CoS value to the incoming frame, then with the CoS-to-DSCP map, the port CoS will be mapped to interval DSCP value.
2. Trust the CoS value in the incoming frame (configure the port to trust CoS). Layer 2 802.1Q frame headers carry the CoS value in the three most-significant bits of the Tag Control Information field. CoS values range from 0 for low priority to 7 for high priority.
3. Classify the ingrass packets based on layer 2 MAC ACL, check source MAC, destination MAC address and Ethertype domain. If there is no configuration for ACL, distribute default DSCP value 0 to the packet. Otherwise, distribute DSCP value for ingress packets based on policing map table.

The trust DSCP configuration is meaningless for non-IP traffic. If you configure a port with this option and non-IP traffic is received, the switch assigns the default port CoS value and classifies traffic based on the CoS value.

For IP traffic, you have these classification options:

1. Trust the IP DSCP in the incoming packet (configure the port to trust DSCP). The switch assigns the same DSCP to the packet for internal use. The IETF defines the 6 most-significant bits of the 1-byte ToS field as the DSCP. The priority represented by a particular DSCP value is configurable. The supported DSCP values are 0-63.
2. Trust the IP Priority in the incoming packets (configure the port to trust IP Priority), using IP-precedence-to-DSCP mapping table to interval DSCP value.
3. Trust the CoS value (if present) in the incoming packet. The switch generates the DSCP by using the CoS-to-DSCP map.
4. Classify incoming packets based on the configured ACL entries, and check different fields in IP header. If there is no configured ACL, distribute default DSCP value 0 to the packet. Otherwise, distribute DSCP value for input frame based on policing map table.

Classification based on QoS ACL

1 If a matched ACL entry with permit is found out (the first matched), designated QoS actions are triggered
2 If a matched ACL entry with deny is found out, jump over this one and go on next one.
3 If there is no matched permit ACL is found out, do not apply any QoS to the packets.
4 If configure several of ACL entries are matched on the port, apply QoS action when

the first ACL entry with permit is found out.

After a traffic class has been defined with the ACL, you can attach a policy to it. A policy might contain multiple classes with actions specified for each one of them. A policy might include commands to classify the class as a particular aggregate (for example, assign a DSCP) or rate-limit the class. This policy is then attached to a particular port on which it becomes effective.

The classification based on class- map and policy-map:

A class map is a mechanism that you use to isolate and name a specific traffic flow (or class) from all other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it; the criteria can include matching the access group defined by the ACL. 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 setting a specific DSCP value in the traffic class or 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.

A policy map also has these characteristics:

1. A policy map can contain multiple class statements.
2. A separate policy-map class can exist for each type of traffic received through an interface.
3. A policy-map configuration state supersedes any actions due to an interface trust state.

29.1.2. Policying and marking

Policing involves creating a policer that specifies the bandwidth limits for the traffic. Packets that exceed the limits are *out of profile* or *nonconforming*. Each policer specifies the action to take for packets that are in or out of profile. These actions, carried out by the marker, include dropping the packet or marking down the packet with a new user-defined value.

You can create an individual policer. QoS applies the bandwidth limits specified in the policer separately to each matched traffic class. You configure this type of policer within a policy map by using the **policy-map** configuration command.

When configuring policing and policers, keep these items in mind:

1. By default, no policers are configured.
2. Policers can only be configured on a physical port. There is no support for policing at a VLAN level.
3. One policer can only be applied to one direction.
4. Policers can be configured on both ingress port and egress port, the ingress policer

can be single or aggregated.

5. On an interface configured for QoS, all traffic received through the interface is classified, policed, and marked according to the policy map attached to the interface.

   User can create following policies:

   1 single-policer

   Each of the matching condition in the policier uses that policer;

   2 class-policer

   All the matching conditions in the policier uses that policer;

   3 aggregate-policer

   All the class-map in one policer use the policer

29.1.3. Mapping table

In the process to managing QoS, the switch descripe the internal DSCPpriority for all the traffics:

1. In the process for classification, QoS uses configured mapping table (CoS-to-DSCP,IP-precedence-to-DSCP) to derive an interval DSCP value based on received CoS or IPpriority; when configure the DSCP trust status on the port and the two QoS domain have different DSCP value, use DSCP-to-DSCP-mutation to derive a new DSCP value.
2. In the process of policing, QoS can configure new DSCP value to IP or non-IP packet (if the packet is out of profile, and the policing demonstrates mark down action), then the mapping table is called policed-DSCP mapping.
3. Before the traffic reaches the scheduling stage, QoS uses the configurable DSCP-to-CoS map to derive a CoS value from the internal DSCP value. The CoS value is used to select one of the four egress queues.

CoS-to-DSCP, DSCP-to-CoS and IP-precedence-to-DSCP mapping table have default value: DSCP-to-DSCP-mutation and policed-DSCP map table are empty,defaultly uses DSCP value of ingress packet;

DSCP-to-DSCP-mutation map table is applied to the port, other map tables are applied to the whole switch.

29.1.4. Queueing and scheduling

After policing and marking, enter queuing and scheduling.

To above two types of message, ISCOM2800 realizes two kinds of management:

1） Based on the defined rule, recreate CoS value for message, but it does not change the CoS value of the packets;

2） This policy is only effective when the rule is applied with TOS value, that is change the CoS value of the message based on TOS value;

The switch supports four CoS queues for each egress port. For each queue, you can specify these types of scheduling:

1. Strict priority scheduling

Strict priority scheduling is based on the priority of queues. Packets in the high-priority queue are always sent first, and packets in the low-priority queue are not sent until all the

high-priority queues become empty.

The default scheduling method is strict priority.

2. Weighted round-robin (WRR) scheduling

WRR scheduling requires you to specify a number that indicates the importance (weight) of the queue relative to the other CoS queues. WRR scheduling prevents the low-priority queues from being completely neglected during periods of high-priority traffic. The WRR scheduler sends some packets from each queue in turn. The number of packets it sends corresponds to the relative importance of the queue. For example, if one queue has a weight of 3 and another has a weight of 4, three packets are sent from the first queue for every four that are sent from the second queue. By using this scheduling, low-priority queues have the opportunity to send packets even though the high-priority queues are not empty.

29.2. Configure QOS list

The configuration for QoS includes following contents:

1,QoS enable and disable

2,configure QoS trust status and CoS default value.

3,Configure QoS map table

4,Configure QoS class-map

5,Configure QoS policy-map

6,Configure QoS classification

7,apply the policy on the port

8,Set the scheduling mode for egress queue.

9,Monitor and monitor

29.2.1. QOS Default setting

Attributes	Default configuration
QoS enable	disabled
Port trust status	UNTRUST
Port default CoS	0
Port default DSCP	0
Port default OVERRIDE of DSCP	Disable
DSCP Mutation Map	default-dscp
Queue scheduling policing	Strict priority scheduling SP

CoS-DSCP default map relationship:

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

IP-Precedence-DSCP default map relationship:

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

DSCP-COS default map relationship:

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

DSCP-to-DSCP-Mutation default map relationship default-dscp):

DSCP value	0	1	2	3	4	5	6	7
0	8	9	10	11	12	13	14	15
1	16	17	18	19	20	21	22	23
2	24	25	26	27	28	29	30	31
3	32	33	34	35	36	37	38	39
5	40	41	42	43	44	45	46	47
6	48	49	50	51	52	53	54	55
7	56	57	58	59	60	61	62	63

Internal default map relationship fromm COS to the queue:

Support 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

Defaultly QoS is disabled on the switch. apply following commands under global configuration mode use enable QoS setting:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mls qos**	Start QOS
3	**exit**	Back to privilege user mode
4	**show mls qos**	Show QOS configuration

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

In order to check whether the configuration is corrent or not, uses show command:

Raisecom#show mls qos

QoS is enabled.

When the QoS hasn't been enabled, some functions are still effective, for instance, port default CoS, port default DSCP, queue scheduling mode, CoS to queue mapping. We suggest disable the flow control function before the enablization of QoS.

29.2.3. Configure QoS trust status and CoS default value

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

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port 1**	Enter port configuration mode
3	**mls qos default-cos** *cos-value*	Set default CoS value.
4	**mls qos default-dscp** *dscp-value*	Set default DSCP value.
5	**mls qos default-dscp override**	Start DSCP override function
6	**exit**	Back to global configuration mode
7	**exit**	Back to privilege user mode
4	**show mls qos port 1**	Show QOS port configuration mode

Configuration example:

Raisecom#config

Raisecom(config)#inter port 1

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

Raisecom(config-port)#mls qos default-dscp 3

Raisecom(config-port)#exit

Raisecom(config)#exit
Raisecom# show mls qos port 1

In order to check whether the configuration is corrent or not, use show command:
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 default configuration for the port, use no command:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port 1**	Enter port configuration mode
3	**no mls qos default-cos**	Recover default CoS value to 0
4	**no mls qos default-dscp**	Recover default DSCP value to 0
5	**no mls qos default-dscp override**	Recover DSCO override function to default setting:
6	**exit**	Back to global configuration mode
7	**exit**	Back to privilege user mode.
4	**show mls qos port 1**	Show QoS port configuration information

In order to check whether the configuration is corrent or not, use show command:
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. Configure QoS mapping table:

1 COS-DSCP mapping table:

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

Default mapping relationship is:

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

If want to modify the map relationship, use following steps for the configuration:

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 relationship
3	**exit**	Back to privilege user mode

4	**show mls qos maps cos-dscp**	Show COS-DSCP mapping table for QoS

Configuration example:

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

Raisecom#config

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

Raisecom(config)#exit

Raisecom# show mls qos maps cos-dscp

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

Raisecom#show mls qos maps cos-dscp

Cos-dscp map:

cos: 0 1 2 3 4 5 6 7

---

dscp: 2 3 4 5 6 7 8 9

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

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

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

Raisecom#show mls qos maps cos-dscp

Cos-dscp map:

cos: 0 1 2 3 4 5 6 7

---

dscp: 0 8 16 24 32 40 48 56

2 IP-Procedence-DSCP map table

IP-Procedence-DSCP map table map the TOS value of ingress packet to a DSCP value, QoSuses it to descripe the priority of data flow: default map relationship is:

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

If want to modify the relationship, use following steps for the configuration:

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

Configuration example:

Configure **ip-prec-dscp mapping to 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 whether the configuration is correct or not, use show command:

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 IP-procedence-DSCP map to default map relationship, use no command for settings:

step	Command	Description
1	**config**	Enter global configuration mode
2	**no mls qos map ip-prec-dscp**	Recover to default mapping relationship
3	**exit**	Back to privilege configuration mode.
4	**show mls qos maps ip-prec-dscp**	Show the IP-Procedence-DSCP map table of QoS.

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

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 table:

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

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

If want to modify this kind of map relationship, use following steps:

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

Configuration example:

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

Raisecom#config

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

Raisecom(config)#exit

Raisecom# show mls qos maps dscp-cos

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

Raisecom#show mls qos maps dscp-cos

Dscp-cos map:

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

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

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

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

Raisecom#show mls qos maps dscp-cos

Dscp-cos map:

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

4 DSCP-MUTATION map table

If you want to realize QoS between two individual QoS domain, you can set the port of domain bounder to DSCP trust status, then the receiving port trusts the DSCP value and avoid the procedure of traffic classification. If the two domain have different DSCP value, user can use DSCP-to-DSCP map table for the mutation.

DSCP-MUTATION map table can map the DSCP value to a new DSCP value, QoS uses it to describe the priority of data flow. There is a default map table “default-dscp” in the system, this table cannot be changed and deleted.

If want to modify this kind of relationship, use following steps for configuration:

Step	Command	Description

1	**config**	Enter global configuration mode
2	**mls qos map dscp-mutation** *dscpname dscplist* **to** *dscp*	Create new DSCP map relationship
3	**exit**	Back to privilege configuration mode
4	**show mls qos maps dscp-mutation**	Show DSCP-MUTATION map table of QoS.

Configuration example:

Configure **dscp-mutation** map,map 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 whether the configuration is correct or not, use show command:

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 delete DSCP-MUTATION map table,use **no** command:

step	Command	Description
1	**config**	Enter global configuration mode
2	**no mls qos map dscp-mutation** *dscpname*	Delete DSCP map relationship
3	**exit**	Back to privilege configuration mode
4	**show mls qos maps**	Show DSCP-COS map table of

	dscp-mutation	QoS

If want to apply this DSCP-mutation map table, user should use it under port configuration mode. Port uses default-dscp map relationship as the default.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port 1**	Enter port mode
3	**mls qos dscp-mutation** *dscpname*	Apply DSCP map relationship
4	**exit**	Back to configuration mode.
5	**exit**	Back to privilege mode.
6	**show mls qos port 1**	Show QOS port configuration information

Configuration 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 whether the configuration is correct or not, use show command:

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 is realized by filter in the hardware, and the 1-8 ports use the same filter table (similarly 9-16,7-24, port 25, port 26 use one filter table respectively and five filter tables), so if any port among port 1-8 uses DSCP-MUTATION map table, other ports among port 1-8 will also use this DSCP-MUTATION map table.

In order to cancel the application of DSCP-MUTATION map table, use **no** command.

Step	Command	Descripton
1	**config**	Enter global configuration mode
2	**interface port 1**	Enter port configuration mode
3	**no mls qos dscp-mutation** *dscpname*	Cancel DSCP map relationship
4	**exit**	Back to configuration mode.
5	**exit**	Back to privilege mode.
6	**show mls qos port 1**	Show QOS port configuration information.

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

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 dscp-mutation map table is applied to particular port, this map table can not be deleted; it can be deleted only when the map table doesn't be used

5, Configure COS value to select the queue
Based on the CoS value of ingress packet, CoS-queue decides output queue, QoS uses it to descripe the priority of data flow. The default map relationship is:

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

If want to modify this map relationship, use following steps:

Step	command	description
1	**config**	Enter global configuration mode
2	**queue cos-map** *queueid coslist*	Set the new map relationship, the packet with cos value 1-4 are sent to queue 1:
3	**exit**	Back to privilege mode
4	**show mls qos queuing**	Show queue map table of the QoS

Configuration example:
Raisecom#config
Raisecom(config)# **queue cos-map 1 1-4**
Raisecom(config)#exit
Raisecom#show mls qos port 1

In order to check whether the configuration is correct or not, use show command:
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 relationship from CoS-queue map table to default map table, use no command:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**no queue cos-map**	Recover to default map relationship

3	**exit**	Back to privilege configuration mode
4	**show mls qos queuing**	Show the map queue of QOS

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

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. Configure the class map of QoS

1 Create or delete class-map

Use **class-map** command to isolate special data flow, the matching conditions includes ACL, IPpriority, DSCP,VLAN and class-map.

Create **class-map** as following steps:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**class-map** *class-map-name* **[match-all | match-any]**	Create the name of class-map to aaa and enter config-cmap mode.
3	**description WORD**	Description information
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege configuration mode.
6	**show class-map [WORD]**	Show CLASS MAP

Class map has two matching types, match-all is to execute AND operation, that is the AND operation among several match announcement, if there is confliction, match announcement fail; match-any is to execute OR operation, default is match-all.

Configuration 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 whether the configuration is correct or not, use show command:

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 **no** command **no class-map** class-map-name.

Note:when you want to delete a class-map, if it is cited by policy and applied on the port, it cannot be deleted.

2 configure match announcement

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 global configuration mode
9	**exit**	Back to privilege configuration mode
10	**show class-map [WORD]**	Show CLASS MAP

When match ACL entries, ACL should be created previously.

When match class-map, class-map should be created previously.

If the type of class-map is match-all, configuration maybe failture because the matching conditions conflict with each other.

If this class-map has been applied to a particular port, it is not allowed to modify match announcement.

Configuration 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 whether the configuration is correct or not, use show command:

```
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 want to delete particular match announcement:

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 privilege mode
10	**show class-map [WORD]**	Show CLASS MAP

If this class-map has been applied to particular port, do not allow to delete match announcement.

29.2.6. configure QoS policy map

1 create and delete policy-map

Use **policy-map** command to encapsulate and classify class-map defined data flow.

Create **policy-map** as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**policy-map** *policy-map-name*	Create the policy map with name bbb and enter config-pmap mode.
3	**description WORD**	Descripe information
4	**exit**	Back to global configuration mode
5	**exit**	Back to privilege configuration mode
6	**show policy-map [WORD]**	Show POLICY MAP

Configuration example:

Raisecom#config

Raisecom(config)# **policy-map** *bbb*

Raisecom(config)# **exit**

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

Raisecom#show policy-map

Policy Map bbb

Description:this-is-test-policy

If you want to delete a **policy-map**, use **no** command, **no policy-map** policy-map-name.

Note:when you want to delete a policy-map, and if it has been applied to the port, it cannot be deleted.

29.2.7. configure QoS flow classification

1 create and delete policer

policer is used to the rate limitation and shaping for the traffic, at the same time, it also do DSCP modification for data packet, or byte dropped. Currently, there are three types of policers:

single-policer:each rule within this class-map use this policer;

class-policer:all the rules withing this class-map one class-map share this policer;

aggregate-policer:all the class-map within a policy-map share this policy;

If the rate exceeds the set value (out profile), each policer has two actions: dropped or decrease the dscp value (marked down)

Create policer as following steps:

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 the policer with type single.
3	**mls qos class-policer** *policer-name rate burst* **exceed-action {drop | policed-dscp-transmit** *marked-dscp* **}**	Create the policer with type class
4	**mls qos aggregate-policer** *policer-name rate burst* **exceed-action {drop | policed-dscp-transmit** *marked-dscp* **}**	Create the policer with type aggregate rate—the average speed of the traffic,range is 8－2000000kbps. Burst- specify burst value, range is from 8－512000k characters. 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

Configuration 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 whether the configuration is correct or not, use show command:

Raisecom#show mls qos policer

single-policer aaa 44 44 exceed-action policed-dscp-transmit 4

Not used by any policy map

If the aaa is applied to the 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 want to delete a policer, use no command, **no {single-policer | class-policer | aggregate-policer }** *placer-name***.**

Note:if the policer is cited by the policy and applied on the port, it will not be deleted.

2 define traffic classification

If want to define one or more defined class map to a policy, use following steps:

Ste[	Command	Description

1	**config**	Enter global configuration mode
2	**policy-map** *policy-map-name*	Enter config-pmap mode
3	**class-map** *class-map-name*	Encapsulate class-map aaa to policy aaa and enter config-pmap-c mode.
4	**exit**	Back to global configuration mode
4	**exit**	Back to privilege configuration mode
5	**show policy-map [WORD]**	Show POLICY MAP

One class can be applied to several policies.

Configuration 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 chech whether the configuration is correct or not, use show command:

Raisecom#show policy-map

Policy Map aaa

Class aaa

If want to delete a policy from class-map:

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 the policy.
4	**exit**	Back to privilege configuration mode
5	**show policy-map [WORD]**	Show POLICY MAP

If this policy-map has been applied to particular port, class-map cannot be deleted.

3 Define traffic action

Currently, there are three actions:

trust:the trust status of the traffic, that is trust CoS, DSCP or TOS;

set:modify the data packet in the traffic to the new value, including CoS, DSCP and TOS;

police:rate limitation and shaping for the traffic.

Use following steps:

step	Command	Description
1	**config**	Enter global configuration mode
2	**policy-map** *policy-name*	Enter config-pmap mode
3	**class-map** *class-name*	Put class-map encapsulation to the policy, and enter config-pmap-c mode.
4	**police** *policer-name*	Appliy policer for the traffic on this policy
5	**trust** [**cos** | **dscp** | **ip-precedence**]	The trust status for the traffic, defaultly uses dscp.

6	**set** {**ip dscp** *new-dscp* | **ip precedence** *new-precedence* | **cos** *new-cos* }	Set the new value for the traffic.
7	**exit**	Back to config-pmap mode
8	**exit**	Back to global configuration mode
9	**exit**	Back to privilege configuration mode
10	**show policy-map [WORD]**	Show POLICY MAP

Note:ISCOM2800 do not support trust command currently. Set command is conflict with trust command. User can only set one type in a single class-map, the later set one will be in effective.

Configuration 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
```

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

```
Raisecom#show policy-map
  Policy Map aaa
     Class aaa
          police aaa
          set ip precedence 4
```

If want to delete or modify traffic action:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**policy-map aaa**	Enter config-pmap mode
3	**class-map aaa**	Encapsulate class-map aaa to policy aaa and enter config-pmap-c mode.
4	**no police** *policer-name*	Apply policer on this policy traffic.
5	**no trust** [**cos** | **dscp** | **ip-precedence**]	The trust status of the traffic, default setting is dscp.
6	**no set** {**ip dscp** | **ip precedence** | **cos** }	Set the new value for the traffic.
7	**exit**	Back to config-pmap mode
8	**exit**	Back to global configuration mode
9	**exit**	Back to privilege configuration mode.
10	**show policy-map [WORD]**	Show POLICY MAP

If this policy-map has been applied to particular port, do not allow to modify the action.

29.2.8. Apply the policy on the port

when all the traffics and policies are defined, actually, they are not in effective. User should apply them on the ports.

The steps for applying policies as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**service-policy** *policy-name* **ingress** *portid* **[egress** *portlist* **]**	Apply the policy to the ingress port or egress port.
5	**exit**	Back to privilege port
6	**show mls qos port** *portid*	Show QoS port information.

Note: before appling the policy, QoS should be enabled; the policy and the trust of the port conflict with each other. Before the policy application, the trust status is trust, then the status will change to untrust after appling the policy.

Application 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 whether the configuration is correct or not, use show command:

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 the application of the policy, use **no service-policy** *policy-name* **ingress** *portid.*

29.2.9. Set the scheduling mode for egress queue

currently, the device only support four types of scheduling mode: Strict priority, weighted round robin, and bound-delay mode and SP+WRR mix mode. default setting is strict priority mode.

Configuration steps as following:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**queue strict-priority**	Configure to strict priority
3	**queue wrr-weight** *weight0 weight1 weight2 weight3*	Set the scheduleing mode of the port to WRR
4	**queue bounded-delay** *weight0 weight1 weight2 weight3 delaytime*	Set the scheduling mode of the port to BOUNDDELAY

		delaytime——delay time.
5	**queue preemp-wrr** *weight1 weight2 weight3*	Set the scheduling port of the port to PREEMP-WRR mode, that is to say, queue one has strict priority, other queue based on the weight round.
6	**exit**	Back to privilege configuration mode
7	**show mls qos queuing**	Show qos queue information

currently,do not support SP+WRR mix mode(**preemp-wrr**).

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

Raisecom#config

Raisecom(config)# queue wrr-weight 1 2 4 8

Raisecom(config)#exit

Raisecom#show mls qos queuing

Command execution echo:

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

Set the queue to BOUNDDELAY mode, weights are 1:3:5:7 respectively, delay is100ms:

Raisecom#config

Raisecom(config)# queue bounded-delay 1 2 4 8 100

Raisecom(config)#exit

Raisecom#show mls qos queuing

Command execution echo:

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

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

Command and mode	Following command should be executed in priviledged EXEC.
show mls qos	Show the enable and disable status of Qos
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 configuration content for different table.
show mls qos queueing	Show ingress/egress configuration information.
show mls qos port *portid* [**policers**]	Show the configuration policy for the port, and policer information etc.
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 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

If you want to know which port is using policer, use following commands:

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 map information

Raisecom#show mls qos maps

Dscp-cos map:

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

Cos-dscp map:

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

```
  ------------------------------------------
    dscp:      0    8    16   24   32   40   48   56

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 queue 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 QOS port 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

If want to check all the port 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
```

If want to show class-map for designated name, use following commands:

```
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
```

show the policy-map information for designated name:

```
Raisecom#show policy-map aaa
  Policy Map aaa
      Class aaa
            police aaa
            set ip precedence 4
      Class bbb
            police aaa
```

If you want to show the name of designated policy-map and class-map name:

```
Raisecom#show policy-map aaa class-map aaa
  Policy Map aaa
      Class aaa
            police aaa
            set ip precedence 4
```

29.3.8. Show QOS policy-map application information

If you want to know which policy-map information is being used on a particular 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)
```

If you want to know which policy-map information is being used on all the 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:

1 Port TRUST status and policy configuration conflict with each other;
2 The TRUST status of the traffic and the SET action conflict with each other;
3 If you want to delete class-map, policy-map, police and they have been applied on the ports, operation will fail;
4 When class-map, policy-map have been applied on the port, modify match announcement and flow action, for instance, set action will fail.
5 If apply the traffic policy, QoS should be enabled preconditionly; when the QoS is disabled, the traffic policy will fail;
6 If the matching type of class-map is match-all, the configuration can be failure due to the confliction between matching conditions.
7 ACL should be defined preconditionly when match an ACL, and type should be permit;
8 When match a class-map, sub class-map should be match-all type;
9 If there are many configured traffic, they may fail. The possible reason is that there is a maximum rule capacity, because 8 ports have 256 rules;
10 When start QoS policy, we suggest disable the flow control function.

29.5. QOS command reference

Command	Description
[no] mls qos	Enable or disable QoS
[no] mls qos trust [**cos** | **dscp** | **ip-precedence**]	Set the TRUST status of the port.
mls qos default-cos *default-cos*	Set the defaut COS value of the QOS port
no mls qos default-cos	Recover the default COS value of QOS port.
mls qos default-dscp { *default-dscp* | **override }**	Set the default DSCP value of QoS port.

no mls qos default-dscp [override]	Recover the default DSCP value of QOS port.
mls qos map dscp-mutation *dscp-name dcp-list* **to** *dscp*	Create dscp-mutaion map table
no mls qos map dscp-mutation *dscp-name*	Delete dscp-mutaion map table
[no] mls qos dscp-mutation *dscp-name*	Apply or cancel dscp-mutaion map application
class-map *class-map-name* **[match-any | match-all]**	Create class-map
no class-map *class-map-name*	Create class-map
[no] policy-map *policy-map-name*	Create and delete policy map
description *WORD*	Set policy map and class-map description information
[no] class *class-map-name*	Apply policy on the class map
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 announcement.
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 announcement
[no] trust [**cos** | **dscp | ip-precedence**]	Set the trust status of the flow
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 application policy
mls qos map cos-dscp *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Configure the map from cos to dscp.
no mls qos map cos-dscp	Recover the map from cos to dscp
mls qos map ip-prec-dscp *dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8*	Configure the map from TOS to dscp.
no mls qos map ip-prec-dscp	Recover the map from TOS to dscp.
mls qos map dscp-cos *dscp-list* **to** *cos*	Configure the map from dscp to switch internal priority.
no mls qos map dscp-cos	Recover the map from dscp to switch

	internal priority.
queue cos-map *queue-id cos-list*	Configure the map from switch internal priority to the queue.
no queue cos-map	Recover the map from switch priority to the queue.
queue wrr-weight *weight0 weight1 weight2 weight3*	Configure switch scheduling mode to WRR.
queue bounded-delay *weight0 weight1 weight2 weight3 delaytime*	Set the switch scheduling mode to BOUNDDELAY
queue preemp-wrr *weight1 weight2 weight3*	Set the scheduling mode of the port to PREEMP-WRR.
queue strict-priority	Set the port scheduling mode to strict priority mode.
show mls qos	Show QoS enable/disable.
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 configuration content for different map table.
show mls qos queueing	Show the configuration information for ingress/egress queue.
show mls qos port *portid* [**policers**]	Show the policy configuration, and policer information.
show class-map [*class-map-name*]	Show class-map information
show policy-map [*policy-map-name* | [**port** *portId*] [**class** *class-name*]	Show policy information

30. MVR configuration

This chapter introduces the MVR function and IGMP filter function of ISCOM2800 switch and their configuration method.

30.1. About MVR

Multicast VLAN Registration (MVR) is designed for applications using wide-scale deployment of multicast traffic across an Ethernet ring-based service provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

MVR assumes that subscriber ports subscribe and unsubscribe (join and leave) these multicast streams by sending out IGMP join and leave messages. These messages can originate from an IGMP version-2-compatible host with an Ethernet connection. Although MVR operates on the underlying mechanism of IGMP snooping, the two features operate independently of each other. One can be enabled or disabled without affecting the behavior of the other feature. However, if IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping.

MVR has two operation modes:

1 Compatible mode: It works the same as dynamic mode for all multicast data packets and IGMP query and leave packets. However, received IGMP report packets for MVR groups are not sent out on the multicast VLAN source ports. In contrast to dynamic mode, the switch does not send join messages to the router. The router must be statically configured for the interface to receive the multicast stream. Therefore, in this mode, MVR does not support dynamic membership joins on source ports.

2 Dynamic mode: When operating in MVR dynamic mode, the switch performs standard IGMP snooping. IGMP information packets are sent to the switch CPU, but multicast data packets are not sent to the CPU. Dynamic mode allows the multicast router to run normally because the switch sends the IGMP join messages to the router, and the router forwards multicast streams for a particular group to an interface only if it has received a join message from the interface for the group. Receiver ports are treated as members of the multicast VLAN for MVR multicast control and data traffic. IGMP reports for MVR groups are sent out source ports in the multicast VLAN.

30.2. IGMP filter introduction

In some application, administrator need to limit multicast users, for instance, allow some users to receive multicast data but deny others. By configuring IGMP profile, administrator can configure the port flexibly. One IGMP proffile includes one or several multicast group, and whether these groups can be accessed. If a denied IGMP profile is applied on the port, port will drop the data when it get the IGMP join message. IGMP profile can only be applied to dynamic multicast group, not available for static group.
By the way, administrator can set the maximum multicast groups on the port.

30.3. Configure MVR function

Configuration includes following contents:

1, MVR global configuration

2, Configure MVR port information

3, MVR monitor and monitor

30.3.1. MVR default configuration

attributes	Default configuration
MVR enable	disabled
Multicast address	No configuration
MVR aging time	600 seconds
Multicast VLAN	1
MVR mode	compatible
Interface MVR enable	disabled
Interface default configuration	Non MVR (not the source port, not the receiving port)
Immediate-leave	disabled

Follow these rules for the configuration:

1 Receiving port can only be ACCESS port, not the TRUNK port. The receiving port can belongs to different VLAN, but it should not be the multicast VLAN.

2 The maximum MVR multicast address is 256;

3 Because 2800 series switch support L2 multicast, that is several IP multicast corresponding to one MAC multicast address, do not use the same name when configuring MVR multicast address.

4 MVR and IGMP snooping can be enabled at the same time.

5 Source port should be in multicast VLAN.

30.3.2. MVR global configuration

In default situation, MVR is disabled on the switch, execute following commands under global configuration mode to enable MVR settings. Users can also set multicast VLAN, multicast address, and operation mode etc. User is allowed to configure MVR if it has not been enabled, if the MVR is enabled, all these setting will take into effect.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mvr enable**	Enable MVR
3	**mvr group** *ip -adress* [*count*]	Configure IP multicast address, if

		count parameter is specified, user can configure a continous MVR group (the range of the count is from 1 to 256, default is 1)
4	**mvr timeout** *timeout*	optional,the maximum exceed time of MVR multicast entity, unit is second, range is from 60 to 36000, default is 600 seconds.
5	**mvr vlan** *vlanid*	optional,specify the VLAN that will receive multicast data, all the source ports should belong to this VLAN, range is from 1 to 4094, default is 1.
6	**mvr mode { dynamic | compatible }**	optional,specify the operation modeof MVR. Dynamic——dynamic mode Compatible——concurrent mode
7	**exit**	Back to privilege configuration mode
8	**show mvr**	Show MVR configuration information
9	**show mvr members**	Show MVR multicast address information

In order to disable MVR, execute **mvr disable** command under global configuration mode. If you want to recover the default value, use **no mvr {mode | group** *ip-address* **| timeout | vlan}** command.

mvr group *ip –adres* command is used to specify which multicast traffic will be received by the switch, if do not specify it, all the traffic will be received.

Following example is used to show how to enable MVR, configure multicast address, and set the query time to 2 seconds, specify multicast VLAN to 22, set the MVR operation mode to static:

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**

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

```
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
```

Check MVR multicast address configuration:

```
Raisecom#show mvr members
MVR Group IP       Status          Menbers
------------------------------------------------------------
234.5.6.7          Inactive        none
```

30.3.3. Configure MVR port information

Default situation, every port of the switch is not the receiving port or souce port. Set them under port configuration mode:

Step	Command	Description
1	**config**	Enter global configuration mode
2	**mvr**	Enable MVR
3	**interface port 3**	Enter port configuration mode
4	**mvr**	Enable port MVR
5	**mvr type { source | receiver }**	Set the MVR type of the port: Source——configure the uplink port as the source port of receiving multicast data, user can not directly connect to the source, all the source port should in multicast VLAN. Receiver——configure the receiving port that directly to the subscribers, which should not belong to the multicast VLAN.
6	**mvr vlan** *vlanid* **group** *ip-address*	Optional, staticly add this port to multicast group. Under compatible mode, this command can only be applied to the receiver port; under dynamic mode, it can be applied on source port or receiver port.
7	**mvr immediate**	Enable automaticly leave function on this port. This command can only be applied to the receiver port.
8	**exit**	Back to global configuration mode
9	**exit**	Back to privilege configuration mode
10	**show mvr**	Show MVR configuration information
11	**show mvr port [***portid***]**	Show port configuration information
12	**show mvr port [***portid***] members**	Show port member information

In order to recover default MVR configuration, use command **no mvr** [**type** | **immediate** | **vlan** *vlan-id* **group**]. If you want to delete all the configured static multicast group under this port, use **no mvr vlan** *vlan-id* **group**. Specify the multicast address if you want to delete one multicast address. Following commands show us how to configure port 3 to MVR receiver, enable immediate-leave function and add it into 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

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

```
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

Use some show command to check MVR running and configuration information of the switch. Use following commands to show:

Command, mode	Following commands should be executed un 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 port statis 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

If want to show information for designated port:

```
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. Configure IGMP filter table

In some environments, for example, metropolitan or multiple-dwelling unit (MDU) installations, you might want to control the set of multicast groups to which a user on a switch port can belong. You can control the distribution of multicast services, such as IP/TV, based on some type of subscription or service plan. You might also want to limit the number of multicast groups to which a user on a switch port can belong.

With the IGMP filtering feature, you can filter multicast joins on a per-port basis by configuring IP multicast profiles and associating them with individual switch ports. An IGMP profile can contain one or more multicast groups and specifies whether access to the group is permitted or denied. If an IGMP profile denying access to a multicast group is applied to a switch port, the IGMP join report requesting the stream of IP multicast traffic is dropped, and the port is not allowed to receive IP multicast traffic from that group. If the filtering action permits access to the multicast group, the IGMP report from the port is forwarded for normal processing.

IGMP filtering controls only group specific query and membership reports, including join and leave reports. It does not control general IGMP queries. IGMP filtering has no relationship with the function that directs the forwarding of IP multicast traffic. The filtering

feature operates in the same manner whether MVR is used to forward the multicast traffic.

1 IGMP profile configuration

2 Apply IGMP profile

3 The configuration for maximum group number of the port.

4 IGMP filter monitor and maintenance

30.4.1. IGMP filter default configuration

Attributes	Default configuration
IGMP filter enabled	enable
Port application	disable
Maximum group number	No limitation
Maximum group number action	refused
IGMP profile	No definition
IGMP profile action	refused

30.4.2. profile configuration

Execute **ip igmp profile** command under global configuration mode, it can create IGMP profile, and enter profile configuration mode. Under this mode, user can set the range, and other parameters like actions.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**ip igmp profile** *profile-number*	Create profile and enter profile configure mode. Range of the profile is from 1 to 65535.
3	**permit | deny**	Optional, set the action, permit|deny the access for multicast group. Default is deny.
4	**range** *start-ip* [*end-ip*]	Set the IP multicast address or the range of address. If input the scale of the address, starting address, space, ending address. This address should be within the scale of multicast group address.
5	**exit**	Back to privilege configuration mode
6	**exit**	Back to privilege configuration mode
8	**show ip igmp profile [** *profile-number***]**	Show IGMP profile configuration information.

In order to delete profile, execute **no ip igmp profile** command under global configuration mode. In order to delete a multicast address of the profile, use **no range** *start-ip command.*

Following example is to show how to create profile 1, and configure individual 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**

In order to chech whether the configuration is corrent or not, use show command:

```
Raisecom#show ip igmp profile 1
IGMP profile 1
        permit
        range 234.5.6.7
        range 234.5.6.9
```

30.4.3. Apply IGMP profile

Execute **ip igmp filter** command under port configuration mode, it can apply previously created IGMP profile to the designated port. An IGMP profile can be applied to several ports, but each port only has one IGMP profile.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port 1**	Enter port mode
3	**ip igmp filter** *profile-number*	Apply IGMP profile on the port,profile range is from 1 to 65535.
4	**exit**	Back to global configuration mode.
5	**exit**	Back to privilege configuration mode
6	**show ip igmp filter port [** *portid* **]**	Show the IGMP profile on the port.

In order to cancel the IGMP profile application, execute **no ip igmp filter** command under port configuration mode. If the port doesn't apply IGMP profile, return 0.

Following example show us 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**

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

```
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
```

If just want to show the information for port 1:

```
Raisecom#show ip igmp filter port 1
IGMP Filter: 1
```

Max Groups: 20
Current groups: 0
Action: Deny

30.4.4. The maximum port number configuration

Type ip igmp max-groups command under port configuration mode to limit the number of port group.

Step	Command	Description
1	**config**	Enter global configuration mode
2	**interface port 1**	Enter port mode
3	**ip igmp max-groups** *group-number*	Limit the maximum group number, scope is from 0 to 65535, 0 stands for no limitation.
4	**ip igmp max-groups action { deny | replace }**	Optional. The action takes when the group added is exceed the limitation of max. Default is deny. Do not support **replace** currently.
5	**exit**	Back to global configuration mode
6	**exit**	Back to privilege mode
7	**show ip igmp filter port [** *portid* **]**	Show port configuration information

In order to recover default setting, execute **no ip igmp max-groups [action]** command under port configuration mode.

Following command show users how to configure the max-groups.

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**

In order to check whether the configuration is corrent or not, use show command.

```
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
```

If only want to display the information on port 1:

Raisecom#show ip igmp filter port 1
IGMP Filter: 1
Max Groups: 20
Current groups: 0
Action: Deny

30.4.5. The monitor and maintenance of IGMP filtering

Use some show command to check the running and configuration information of IGMP filtering, which can make monitor and maintenance conviently. To the monitor and maintenance of IGMP filtering, use following show command:

Command mode	Following command should be execute under ENABLE mode.
show ip igmp filter	Show the global configuration information of IGMP filtering.
show ip igmp profile [*profile-number***]**	Show IGMP profile information
show ip igmp filter port [*portid* **]**	Show IGMP filtering port configuration information

Show global configuration information of IGMP filtering

Raisecom# **show ip igmp filter**

IGMPfilter: Enable

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
```

If want 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
```

Show port configuration information of IGMP filtering

```
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
```

If want to show information for designated port:

```
Raisecom#show ip igmp filter port 1
IGMP Filter: 1
Max Groups: 20
```

Current groups: 0
Action: Deny

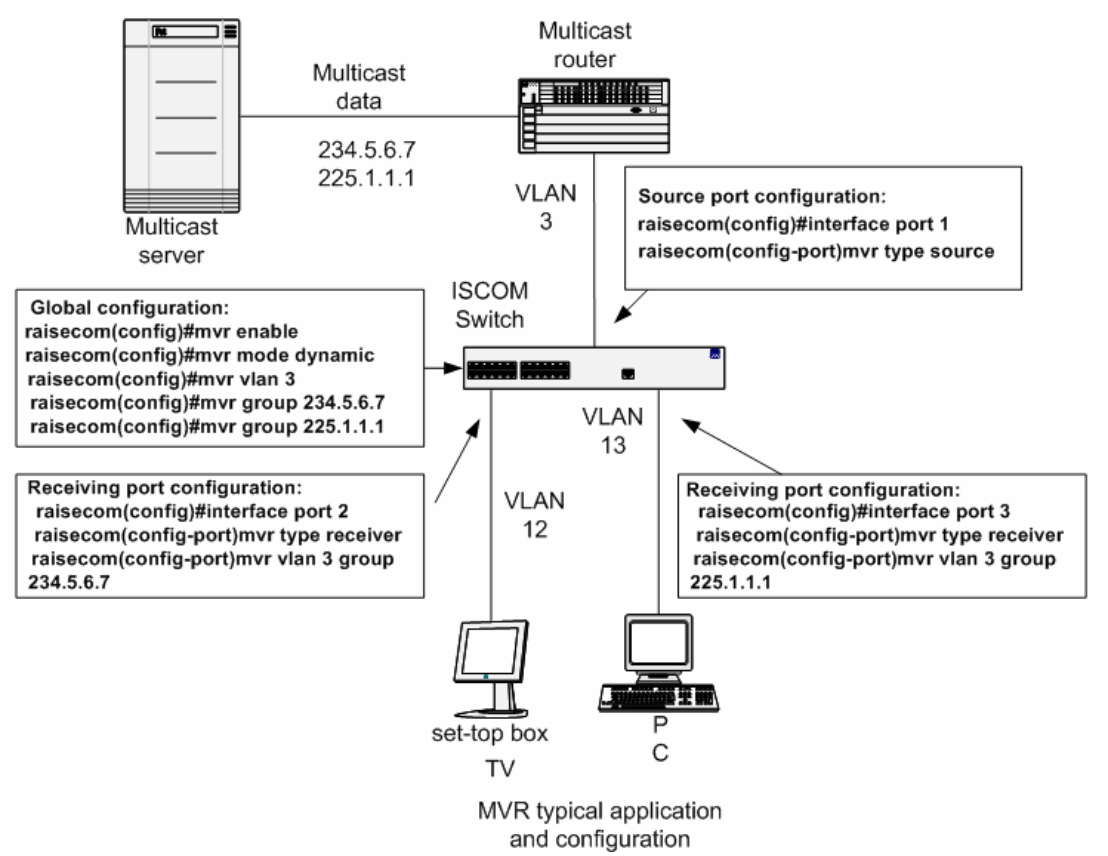
30.5. Typecial configuration for MVR application

In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. DHCP assigns an IP address to the set-top box or the PC. When a subscriber selects a channel, the set-top box or PC sends an IGMP report to the S1 switch to join the appropriate multicast. If the IGMP report matches one of the configured multicast MAC addresses, the switch CPU modifies the hardware address table to include this receiver port and VLAN as a forwarding destination of the specified multicast stream when it is received from the multicast VLAN. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

When a subscriber changes channels or turns off the television, the set-top box sends an IGMP leave message for the multicast stream. The switch CPU sends an IGMP group-specific query through the receiver port VLAN. If there is another set-top box in the VLAN still subscribing to this group, that set-top box must respond within the maximum response time. If the CPU does not receive a response, it eliminates the receiver port as a forwarding destination for this group.

If the Immediate-Leave feature is enabled on a receiver port, the port leaves a multicast group more quickly. Without Immediate Leave, when the switch receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership. With Immediate Leave, an IGMP query is not sent from the receiver port on which the IGMP leave was received. As soon as the leave message is received, the receiver port is removed from multicast group membership, which speeds up leave latency. Enable the Immediate Leave feature only on receiver ports to which a single receiver device is connected.

If using MVR, the multicast data is not needed to be transmitted in each VLAN, but only be transmitted in the Multicast VLAN for one time. So the bandwidth is saved.



30.6. Trouble shooting of MVR and IGMP filtering

1 When configure the source port, source port doesn't exist in multicast VLAN;

2 When configure receiving port, port is in the multicast VLAN.

3 When configure MVR group, there is confliction in the group because several IP multicast address corresponding to one MAC multicast address;

4 When configure static group on the port, address is not in the scope of MVR group.

5 Under MVR mode, configuring static multicast on the source port.

30.7. MVR and IGMP filter command reference

command	description
mvr { enable | disable }	Start/stop MVR
mvr vlan *vlanid*	Set multicast VLAN
no mvr vlan	Recover default setting of multicast VLAN
mvr timeout *timeout*	Set MVR timeour
no mvr vlan	Recover MVR timeout
mvr mode { dynamic | compatible }	Set MVR mode
[no] mvr group *ip -adress* [*count*]	Set MVR multicast group
[no] mvr	Enable/disable port MVR
mvr type { source | receiver}	Configure port MVR
no mvr type	Recover port MVR
[no] mvr immediate	Configure immediate-leave
mvr vlan *vlanid* **group** *ip-address*	Configure port to static multicast group member.
no mvr vlan *vlanid* **group [***ip-address***]**	Delete static multicast group member

[no] ip igmp filter	Enable/disable IGMP filtering function
[no] ip igmp profile [*profile-number***]**	Create IGMP profile information
permit | deny	Set IGMP profile action
[no] range *start-ip* [*end-ip*]	Set the range of IGMP profile
ip igmp filter *profile-number*	Apply IGMP profile on the port
no ip igmp filter	Cancel IGMP profile on the port.
ip igmp max-groups *group-number*	Add max-group number that can be added on the port.
no ip igmp max-groups	Recover the default setting of ip igmp max-group.
ip igmp max-groups action { deny | replace }	The action that will be taken when group added exceeds the max-group.
no ip igmp max-groups action	Recover default configuration to deny.
show mvr	Show MVR configuration information
show mvr member [*ip-address* **]**	Show MVR configured multicast group information.
show mvr port [*portid***]**	Show MVR port config information
show mvr port *portid* **members**	Show MVR port static multicast group member information
show ip igmp filter	Show the configuration information of IGMPfiltering
show ip igmp profile [*profile-number***]**	Show configuration information of IGMP profile
show ip igmp filter port [*portid* **]**	Show port configuration information of IGMP filtering.

BROADBAND

to RAISECOM