RAISECOM ISCOM Series Switch
Command Reference

Software Version-ISCOMOS 3.0

Raisecom Technology Co., Ltd

(11/2005)

Contents

1. Preface

1.1. Audience

The *Raisecom ISCOM series switch command reference* is for the networking professional who is responsible for configuring, managing and maintaining ISCOM series switches. This guide provides information of command-line interface and the application examples of ISCOM series switches. 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 Switch Software Configuration Guide>

2. How to use command-line

2.1. Environment

Software: ROS 3.0

2.2. Command 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. Command-line of system

3.1. access-list-map

Command is NOT AVAILABLE FOR 2126/2016/2008/2026

[Introduction]

Use **access-list-map** command to configure a Access Control List (ACL) and use no form to delete an access list (ACL)

[Command format]

access-list-map <0-399> {**permit** | **deny**}
no access-list-map <0-399>

[Parameter]

0-399: number of access-list-map.

permit: permit access if conditions are matched.

deny: deny access if conditions are matched.

[Default]

N/A

[Command Modes]

Global configuration mode. Privileged user.

[Usage Guide]

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.

[Explanation of command execution echo]

Raisecom(config)# access-list-map 1 deny
Raisecom(config-aclmap)#exit
Raisecom(config)# no access-list-map 1

[Related command]

Command	Description
show access-list-map	Show access-list-mapinformation

3.2. arp

[Default]

N/A

[Command Modes]

Privileged EXEC

[Usage Guide]

ARP able is maintained by dynamic ARP protocol. ARP searches the resolving

result of IP address that maps to MAC address. It is automatical. When it is required to add static ARP entries, manually operation of ARP table is required.

Use **no arp add** ip-address to delete ARP entries.

[Explanation of command execution echo]

set successfully!

Adding static ARP entry successfully

set fail!

Adding static ARP entry unsuccessfully

[Example]

Add a static ARP entry. Map IP address 10.0.0.1 to MAC address 0050.8d4b.fd1e

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

Delete ARP entry which IP address is 10.0.0.1 in ARP table

*Raisecom(config)# **no arp add** 10.0.0.1*

[Related command]

Command	Description
clear arp	Clear ARP table
show arp	Show ARP table

3.3. arp aging-time

[Introduction]

Setting the aging time of ARP dynamic entries, the dynamic ARP entries will be removed frome the table according to ARP aging time. The **no** form of this command is used to recovery the default aging time of dynamic ARP

arp aging-time secs

[Parameters]

secs integer 0 or 30-2147483

[Default]

ARP aging time is 1200 secs.

[Command mode]

Global configuration mode Privileged user.

[Usage Guide]

Use this command to set dynamic ARP entries aging time, the maximum time of resolution result, if the existing time of any entry exceeds this time limitation, it will be removed automatically. If the time limitation is set to zero, the dynamic ARP entries will not be removed.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Setting the aging time of ARP table to 1500 secs.

*Raisecom(config)# **arp aging-time 1500***

Recover the aging time of ARP table to 1200 secs.

*Raisecom(config)# **no arp aging-time***

[Related command]

Command	Description
clear arp	Cleare ARP table

show arp	Show ARP table

3.4. Chinese

[Introduction]

Show the command line help information in Chinese.

chinese

[Parameter]

N/A

[Default]

Show the command line help information in English.

[Command Modes]

User EXEC, Privileged EXEC, Global configuration mode, VLAN configuration exec, interface configuration mode; common user, privileged user

[Usage Guide]

Display the help information in Chinese. Help users to get accurate information in Chinese.

[Explanation of command execution echo]

N/A

[Example]

chinese

[Related command]

Command	Description
english	Display the command line help information in English

3.5. class-map

This command is NOT AVAILABLE FOR 2126/2016/2008/2026.

[Introduction]

Use the **class-map** command to create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode.

[Command format]

class-map class-map-name [**match-all** | **match-any**]

no class-map class-map-name

[Parameters description]

class-map-name——specify the name of a class-map, the maximum character is 16.

match-all——Perform a logical-AND of all matching statements under this class map. All criteria in the class map must be matched. Default status.

match-any——Perform a logical-OR of all matching statements under this class map. One of the criteria in the class map should be matched.

[Default]

N/A

[Command format]

Global configuration mode, privileged user.

[Usage Guide]

Use the **class-map** command to specify the name of a class and enter class-map condiguration mode. In the mode, you can enter **match** command to configure the match critiera for this class. And the match critiera include ACL, IP priority, DSCP, another class-map match critiera, VLAN.

[Explanation of command execution echo]

Create the class map successfully
Create the class map unsuccessfully
Delete the class map successfully
Delete the class map unsuccessfully
The input name is too long.
The class map does not exist.
The class map has existed.

[Example]

Raisecom(config)# ***class-map*** *aaa*
*Raisecom(config)#****match*** *vlan 3*
*Raisecom(config-cmap)#****exit***
Raisecom(config)# ***no class-map*** *aaa*

[Related commands]

command	description
show class-map class-map-name	Show class-map information

3.6. class-map

[Introduction]

In policy-map configuration mode, using **class-map** command to specify a typical class-map and the service policy , the prompt will change to config-pmap-c after typing this command.

[Command format]

[no] class class-map-name

[Parameters description]

class-map-name specify the name of class-map, maximum character is 16.

[Default]

N/A

[Command format]

Policy-map (PMAP) configuration mode; privileged user.

[Usage Guide]

In policy-map configuration mode using the command **class-map** to specify flow, the prompt will change to config-pmap-c after typing this command. Then, service policies for a class map can be specified.

[Explanation of command execution echo]

Set the class map successfully
Set the class map unsuccessfully
The input name is too long.
The class map does not exist.

[Example]

Raisecom(config-pmap)# ***class-map*** *aaa*

*Raisecom(config-pmap-c)#**exit***
*Raisecom(config-pmap)#no **class-map** aaa*

[Related information]

command	description
show policy-map [policy-map-name**]**	Show policy-map information

3.7. clear

[Introduction]

Clear all the information on the screen.

[Parameter]

N/A

[Command Modes]

User EXEC, Privileged EXEC, Global configuration mode, VLAN configuration mode, interface configuration mode, router protocol configuration mode; common user, and privileged user

[Usage Guide]

Clear the shown information on the screen.

[Explanation of command execution echo]

N/A

[Example]

*Raisecom> **clear***

[Related command]

N/A

3.8. clear arp

[Introduction]

Clear all entries of ARP table

clear arp

[Parameter]

N/A

[Default]

N/A

[Command Modes]

Privileged EXEC and privileged users

[Usage Guide]

If it is required to delete ARP table, use **clear arp.**

[Explanation of command execution echo]

set successfully!

Clear ARP entries successfully

set fail!

Clear ARP entries unsuccessfully

[Example]

Clear ARP table

*Raisecom(config)#**clear arp***

[Related command]

command	Description
arp add	Add a static MAC address entries
show arp	Show all entries of ARP table

3.9. clear interface port statistics

[Introduction]

Clear port statistical information

clear interface port statistics [**schedule-list** list-no]

[Parameters]

Schedule-list set the starting time, the ending time and the interval time of seasonal operation time.

list-no schendule list number <0-99>;

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

The port is the unit of statistical information.

[Explanation of command execution echo]

Successfully

Port X set unsuccessfully!

[Example]

Clear port 5 statistical information

*Raisecom# **clear interface port 5 statistics***

[Related command]

Command	Description
show interface port port-number **statistics**	Show the statistical information of particular port.

3.10. clear mac-address-table

[Introduction]

Clear the specified MAC address in switch.

clear mac-address-table {**all | dynamic | static**} [**schedule-list** list-no]

[Parameters Introduction]

all Clear dynamic/static MAC address table of a switch.

dynamic Clear dynamic MAC address table only.

static Clear dynamic static MAC address table only.

schedule-list Set the starting time, ending time and periodical operation time.

list-no specigy the certain schedule list<0-99>.

[Default]

N/A

[Command mode]

Global configuration mode

[Usage Guide]

N/A

[Explanation of command execution echo]

N/A

[Example]

Delete all dynamic MAC addresses

*Raisecom#**clear mac-address-table dynamic***

[Related command]

Command	Description
mac-address-table static	Configure static MAC-address-table

3.11. clear rmon

[Introduction]

Use **clear rmon** command to clear all RMON information

[Parameter Introdcution]

N/A

[Default]

N/A

[Command mode]

Global configuration mode.

[Example]

N/A

[Explanation of command execution echo]

N/A

[Example]

*Raisecom(config)#**clear rmon***

[Related command]

N/A

3.12. clock set

[Introduction]

Use **clockset** to modify system data and time

clockset <1-24> <0-60> <0-60> <2000-2199> <1-12> <1-31>

[Parameter]

· <1-24> hour

· <0-60> minute

· <0-60> second

· <2000-2199> year

· <1-12> month

· <1-31> date

[Command Modes]

Privilege EXEC and privilege users

[Usage Guide]

Use **clockset** to modify system date and time. The configured data and time information will always be effective no matter power is on or off.

[Explanation of command execution echo]

Set successfully.

[Example]

*Raisecom# **clockset** 8 30 0 2003 9 30*

System date is modified as 30th Sep, 2003, 8:30:00

[Related command]

command	Description
show clock	Show the current time of system

3.13. clock summer-time

[Introduction]

Enable summer time configuration

[Command line]

clock summer-time {enable | disable}

[Parameter]

enable enable summer time
disable disable summer time

[Default]

Summertime disable.

[Command format]

Privilege exec; privileged user.

[Usage Guide]

N/A

[Explanation of command execution echo]

Set successfully
Set unsuccessfully

[Example]

Raisecom#clock summer-time enable

[Related command]

Command	Description
show clock	Show clock information
clock summer-time recurring	Set the starting time and end time of summer clock

3.14. clock summer-time recurring

[Introduction]

Configure the starting time and the ending time of summertime recurring

[Command format]

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**>**

[Parameter]

·**<1-4>** summer time starting from which week
·**last** summer time starting from the last week of the month
·**week day** summer time starting from what date of the week
·**<1-12>** summer time starting from which month
·**MONTH** input the starting month
·**<0-23>** summer time starting hour
·**<0-59>** summer time starting minute
·**<1-4>** summer time ending at which week of the month
·**last** summer time ending at the last week
·**week day** summer time ending at which day of the week
·**<1-12>** summer time ending month
·**MONTH** input the ending month
·**<0-23>** summer time ending hour
·**<0-59>** summer time ending minute
·**<1-1440>** summer time recurring minute

[Default]

N/A

[Command format]

Privilege exec, privileged user.

[Usage Guide]

This command is used to set the starting time, the ending time and recurring of summer time. The format for starting time and the ending time is: xx month, xx week (or the last week), xx hour and xx minute.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

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

[Related command]

command	description
clock summer-time	Enable summer time function
show clock	Show clock information

3.15. clock timezone

[Introduction]

Configure time zone

[Command format]

clock timezone {+|-} <0-11> <0-59>

[Parameter]

- **+** East Earth time zone
- **-** West Earth time zone
- **<0-11>** time zone recurring hour
- **<0-59>** time zone offset minute

[Default]

The default time is Beijing local time, which is eastern offset 8 hours

[Command format]

Privilege exec; privileged user.

[Usage Guide]

[Explanation of command execution echo]

Set successfully

[Example]

Set the time-offset direction to West Earth, offset time is 5 hours and 40 minutes.

Raisecom#clock timezone – 5 40

[Related command]

Command	Description
show clock	Show the clock information

3.16. cluster

[Introduction]

Enable the cluster function, and enter the cluster management mode. The **no cluster** command can stop the cluster function.

[**no**] **cluster**

[Parameter]

N/A

[Default]

The switch is a cluster candidate.

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

With this command a switch can set itself as a commander and enter cluster management function. Generally speaking, in order to manage a layer-2 network only one commander is required. When start cluster management, user can take some actions like add, enable and delete cluster members. When the cluster manager is stopped, all the cluster members will be deleted, and recover themselves back to candidates.

[Explanation of command execution echo]

This switch has been a member, it can not be a COMMANDER.
Cluster management startup unsuccessfully.
Cluster management shutdown successfully.
Cluster management shutdown unsuccessfully.

[Example]

- Start cluster management
  Raisecom(config)#cluster
- Stop cluster management
  Raisecom(config)#no cluster

[Related command]

command	description
show cluster	Show cluster management related information

3.17. Cluster-autoactive

[Introduction]

Enable automatically activing cluster function. **no cluster-autoactive** command will disable automatically activing cluster function.

[**no**] **cluster-autoactive**

[Parameter]

N/A

[Default]

Default configuration is autoactive function disabled.

[Command mode]

Global configuration mode; Privileged user.

[Usage Guide]

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.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

start the **autoactive** function

Raisecom(config)#cluster-autoactive

stop the **auto active** function

Raisecom(config)#no cluster-autoactive

[Related command]

Command	Description
cluster-autoactive commander-mac	Configure the MAC address of the command associated switch
show cluster	Show the cluster management related information.

3.18. cluster-autoactive commander-mac

[Introduction]

Configure cluster commander MAC address. **no cluster-autoactive commander-mac-command** will recover commander MAC address to default value: 0000.0000.0000.

[**no**] **cluster-autoactive**

[Parameter]

N/A

[Default]

Default configuration is 0000.0000.0000.

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

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.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Configure the MAC address of autoactive associated switch to 1111.1111.1111.

Raisecom(config)#cluster-autoactive commander-mac 1111.1111.1111

Recover MAC address of the commander MAC address.

Raisecom(config)#no cluster-autoactive commander-mac

[Related command]

command	description
[**no**] **cluster-autoactive**	Enable or disable the autoactive function
show cluster	Show cluster management related information

3.19. cmd-str schedule-list

[Introduction]

Specify a schedule-list to a command.

cmd-str **schedule-list** list-no

no schedule-list list-no **command** cmd-no

[Parameter]

list-no schedule-list number <0-99>;

cmd-no the specified command which will be assigned the schedule list

schedule-list set the starting time, ending time, and the time interval

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

The specified command will be operated automatically at the appointed time according to the schedule-list configuration

[Explanation of command execution echo]

Set successfully

Current schedule list not existed.

[Example]

*Raisecom# **storm-control dlf schedule-list 1***

*Raisecom# **no schedule-list 1 command 0***

[Related command]

Command	Description
schedule-list list-no	Configure a schedule list
Show schedule-list	Show schedule-list information

The following commands support schedule-list function:

[no]filter {ip-access-list|mac-access-list| access-list-map} (all|<0-399>) port-list (all|{1-26}) {ingress|egress|both}

filter {enable|disable}

[no]filter {ip-access-list|mac-access-list| access-list-map}{all|<0-399>} vlan-list {all|{1-4094}}

clear arp

dhcp-relay disable

dhcp-relay enable

dhcp-relay listen

no dhcp-relay listen

dhcp-server authentication

dhcp-server enable

dhcp-server disable

dhcp-server active

dhcp-server ip-pool name WORD A.B.C.D A.B.C.D mask A.B.C.D vlan {1-4094} [gateway A.B.C.D] [dns A.B.C.D]

no dhcp-server ip-pool name WORD

dhcp-server relay-ip A.B.C.D A.B.C.D

flowcontrol {on | off }

ip igmp-snooping

no ip igmp-snooping

ip igmp-snooping

no ip igmp-snooping

no shutdown

shutdown
duplex {full-duplex | half-duplex }
speed { auto | 10 | 100 |1000}
clear interface port statistics
clear interface port <1-"MAX_PORT_STR"> statistics
switchport protect
no switchport protect
rate-limit port-list (all | {1-"MAX_PORT_STR"}) ingress
rate-limit port-list (all | {1-"MAX_PORT_STR"}) egress
no rate-limit port-list (all | {1-"MAX_PORT_STR"}) (ingress | egress | both)
sntp server A.B.C.D
no sntp server
spanning-tree (enable|disable)
write
dhcp-server deactive
mac-address-table aging-time
no mac-address-table aging-time
mac-address-table learning (enable | disable) port-list (all | {1-"MAX_PORT_STR"})
mac-address-table static HHHH.HHHH.HHHH vlan <1-4094> port <1-"MAX_PORT_STR">
clear mac-address-table (all | dynamic | static)
mirror (enable | disable)
svl (enable|disable)
dlf-forwarding (enable | disable)
no relay (bpdu | dot1x | lacp | garp | gmrp | gvrp | all) port-list [{1-"MAX_PORT_STR"}]
relay (bpdu | dot1x | lacp | garp | gmrp | gvrp | all) port-list {1-"MAX_PORT_STR"}
storm-control ratio <1-100> <0-512>
storm-control ratio <1-100>
storm-control bps <0-1000> <0-512>
storm-control pps <0-262143>
storm-control all (enable | disable)
storm-control dlf (enable | disable)
storm-control multicast (enable | disable)
storm-control broadcast (enable | disable)

3.20. config

[Introduction]

Use **config** to enter Global configuration mode.

config [terminal]

[Parameter]

terminal

[Command Modes]

Privileged EXEC and privileged user

[Usage Guide]

N/A

[Explanation of command execution echo]

Set successfully.

Command executed successfully

[Example]

*Raisecom#**config terminal***

[Related command]

Command	Description
exit	Return to parent mode or exit
Quit	Return to parent mode or exit

3.21. debug

[Introduction]

[no] debug (all | system | ospf | rip | gvrp | igmp-snooping | cli | driver | dhcp | snmp | stp | lacp | radius | dot1x | qos | rmon | sntp | telnet | arp | ip |config)

[Parameter]

all	debug all functions
arp	arp debug
cli	cli debug
config	system config information
dhcp	dhcp debug
driver	driver debug
gvrp	gvrp debug
igmp-snooping	igmp-snooping debug
ip	ip debug
lacp	lacp debug
ospf	ospf debug
qos	qos debug
radius	radius debug
rip	rip debug
rmon	rmon debug
snmp	snmp debug
sntp	sntp debug
stp	stp debug
system	system debug
telnet	telnet debug

[Default]

Config module is enabled

System module is enabled

Others debug functionalities are disabled

[Command Modes]

Privileged EXEC and privileged user

[Usage Guide]

Use this command to enable some or all module debug functionalities.

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#**debug all***

[Related command]

Command	Description
logging	Configure system log

3.22. description (class-map)

[Introduction]

Configure or modify the description of class-map.

[Command format]

description WORD

[Parameter]

WORD set the description information of class-map, the maximum character is 255, can not separate with a space.

[Default]

N/A

[Command format]

CMAP configuration mode; Privileged user.

[Usage Guide]

Add class-map description information.

[Explanation of command execution echo]

Set the class map description successfully

Set the class map description unsuccessfully

The input name is too long.

[Example]

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

[Related command]

command	description
show class-map class-map-name	Show class-map information

3.23. description (policy-map)

[Description]

Configure or modify the description information of policy-map

[Command format]

description WORD

[Parameter

WORD set the description information of policy-map, the maximum character is 255, can not be separated with a space.

[Default]

N/A

[Command format]

PMAP configuration mode; privileged user.

[Usage Guide]

Add the description information for policy map.

[Explanation of command execution echo]

Set the policy map description successfully

Set the policy map description unsuccessfully

The input name is too long.

[Example]

Raisecom(config-pmap)# ***description*** *this-is-a-policy-map*

[Related command]

Command	Description
show policy-map [policy-map-name**]**	Show policy-map information

3.24. dhcp-relay enable

NOT AVAILABLE FOR ISCOM2826/2126/2016/2008/2026/2826E.

[Introduction]

Enable DHCP Relay function. **dhcp-relay disable** command can stop DHCP Relay function.

dhcp-relay {enable | disable**}** [**schedule-list** list-no]

[Parameter]

schedule-list set the starting time, ending time and time interval.

list-no schedule-list table scale <0-99>;

[Default]

DHCP disables.

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

By using dhcp-relay enable command to start DHCP function. **dhcp-relay disable** command can stop the function of DHCP Relay protocol.

[Explanation of command execution echo]

Enable DHCP Relay successfully
Enable DHCP Relay unsuccessfully
Disable DHCP Relay successfully
Disable DHCP Relay unsuccessfully

[Example]

- enable DHCP Relay protocal

  Raisecom(config)# ***dhcp-relay enable***

- disable DHCP Relay protocal0254747

  Raisecom(config)# ***dhcp-relay disable***

[Related command]

command	description
dhcp-relay listen	Start DHCP Relay on VLAN
show dhcp-relay	Show DHCP Relay configuration and statistical information

3.25. dhcp-relay listen

NOT AVAILABLE FOR ISCOM2826/2126/2016/2008/2026/2826E.

[Introduction]

Start DHCP Relay function on VLAN. **no dhcp-relay listen** command stop the DHCP Relay function on VLAN.

[no] dhcp-relay listen vlan-list vlan-list [**schedule-list** list-no]

[Parameter]

vlan-list VLAN-list, range from 1-4094;

schedule-list set the starting time, ending time and time interval of dispatching task.

list-no schedule-list table scale<0-99>;

[Default]

When global DHCP Relay started, the default configuration of DHCP Relay protocol is enabled.

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

By **dhcp-relay listen command,** start DHCP Relay function on VLAN. no dhcp-relay listen command can set the state of DHCP Relay protocol to disable.

[Explanation of command execution echo]

Enable DHCP Relay on this VLAN successfully
Enable DHCP Relay on this VLAN unsuccessfully
Disable DHCP Relay on this VLAN successfully
Disable DHCP Relay on this VLAN unsuccessfully

[Example]

Enable DHCP Relay protocol on VLAN1

Raisecom(config)# ***dhcp-relay listen vlan-list 1***

Disable DHCP Relay protocol on VLAN1

Raisecom(config)# ***no dhcp-relay listen vlan-list 1***

[Related command]

command	description
dhcp-relay enable	Start global DHCP Relay
show dhcp-relay listen	Show the configuration information of DHCP Relay

3.26. dhcp-relay server-ip

NOT AVAILABLE FOR ISCOM2826/2126/2016/2008/2026/2826E.

[Introduction]

Configure the IP address of DHCP Relay target server. **no dhcp-relay server-ip** command is used to delete the IP address of DHCP RELAY target server

[no] dhcp-relay server-ip ip-address

[Parameter]

ip-address. Set the IP address of server, format is decimal system, Example A.B.C.D

[Default]

There is no IP address of DHCP Relay target server, it needs to configure when DHCP Relay start.

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

Dhcp-relay server-ip command can configure the IP address of DHCP Relay target server IP. No dhcp-relay server-ip command is used to delete DHCP Relay target server IP address. There can be 8 DHCP Relay server IP addresses at maximum.

[Explanation of command execution echo]

Set DHCP Relay server IP address successfully
Set DHCP Relay server IP address unsuccessfully
Delete DHCP Relay server IP address successfully
Delete DHCP Relay server IP address unsuccessfully

[Example]

Set DHCP relay server IP address as 10.0.0.1

Raisecom(config)# ***dhcp-relay server-ip*** *10.0.0.1*

Delete DHCP relay server IP address

Raisecom(config)# ***no dhcp-relay server-ip*** *10.0.0.1*

[Related command]

command	description
show dhcp-relay server-ip	Show the address information of DHCP server

3.27. dhcp-server active

[Introduction]

In assigned VLAN, enable DHCP SERVER.Use **dhcp-server deactive** to disable DHCP SERVER.

dhcp-server active vlan-list vlan-list [**schedule-list** list-no]

dhcp-server deactive vlan-list vlan-list [**schedule-list** list-no]

[Parameter]

vlan-list VLAN list, range from 1-4094;
schedule-list set the starting time, ending time and time interval of dispatching task.
list-no list number<0-99>

[Default]

When the DHCP SERVER is enabled, DHCP protocol is available in VLAN by default.

[Command Modes]

Global configuration mode; Privileged user.

[Usage Guide]

Start DHCP server function on VLAN with **dhcp-server active** command. DHCP server can be stopped by **dhcp-server deactive** command.

[Explanation of command execution echo]

active DHCP server success on VLAN
active DHCP server failure on VLAN
deactive DHCP server success on VLAN
deactive DHCP server failure on VLAN

[Example]

Set DHCP SERVER available on VLAN 1

Raisecom(config)# ***vlan 1***

Raisecom(config-vlan)# ***dhcp-server active***

Set DHCP SERVER unavailable on VLAN1

Raisecom(config-vlan)# **dhcp-server deactive**

[Related command]

command	description
dhcp-server enable	Start DHCP SERVER
show dhcp-server	Show the configuration and statistical information of DHCP SERVER

3.28. dhcp-server default-lease

[Introduction]

Set the default lease of DHCP server. **no dhcp-server default-lease** can recover the default lease value.

[no] dhcp-server default-lease

[Parameter]

timeout specify the time limitation, minute as unit, range from 30 minutes to 10080 minutes.

[Default]

Default lease is 30 minutes.

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

DHCP lease is the amount of time that the DHCP server grants to the DHCP client permission to use a particular IP address. Please use **no** form of this command to recover default lease value

[Explanation of command execution echo]

Set DHCP server default lease timeout successfully
Set DHCP server default lease timeout unsuccessfully
Set DHCP server default lease timeout successfully
Set DHCP server default lease timeout unsuccessfully

[Example]

Set the default lease time of DHCP server to 60 minutes.

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

Recover the lease time of DHCP Server leasing time table.

*Raisecom(config)# **no dhcp-server default-lease***

[Related command]

Command	Description
show dhcp-server	Show the configuration and statistical information of DHCP SERVER

3.29. dhcp-server enable

[Introduction]

Start DHCP Server function. Use **dhcp-server disable** to stop DHCP server function.

dhcp-server {enable | disable**}** [**schedule-list** list-no]

[Parameter]

schedule-list set the starting time, ending time and task operation period.

list-no list number range from <0-99>;

[Default]

Default situation is DHCP server protocol disable.

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

Use **dhcp-server enable** command to start DHCP SERVER function. **dhcp-server disable** command can stop DHCP server function.

[Explanation of command execution echo]

Enable DHCP server successfully
Enable DHCP server unsuccessfully
Disable DHCP server successfully
Disable DHCP server unsuccessfully

[Example]

- To enable DHCP server protocol
  Raisecom(config)# ***dhcp-server enable***
- To disable DHCP server protocal
  Raisecom(config)# ***dhcp-server disable***

[Related command]

command	description
dhcp-server active	Start DHCP SERVER on VLAN
show dhcp-server	Show the configuration and statistical information of DHCP SERVER

3.30. dhcp-server ip-pool

[Introduction]

Set DHCP SERVER ip-pool.

dhcp-server ip-pool pool-name start-ip end-ip mask-ip **vlan-list** vlanlist **[gateway** gtw-address **] [dns** dns-address **] [secondary-dns** dns-address**]** [**schedule-list** list-no]

no dhcp-server ip-pool pool-name [**schedule-list** list-no]

[Parameter]

pool-name ip-pool name, 16 charaters.

start-ip ip-pool start IP address, e.g. A.B.C.D

end-ip ip-pool end IP address, format is dotted decimal, eg:A.B.C.D.

vlanlist VLAN list, format as 1,5-40,55; This property means that certain ip-pool belongs to one VLAN.

gateway optional, set IP address of default gateway for user, format is dotted decimal, eg: A.B.C.D.

dns optional, set IP address of customer specified DNS, format is dotted decimal, eg: A.B.C.D

secondary-dns optional, set the sencomdary DNS IP address, format is dotted decimal, eg: A.B.C.D

schedule-list set the staring time, ending time and task operation period.

list-no number <0-99>;

[Default]

N/A

[Command mode]

Privileged EXEC, privileged user.

[Usage Guide]

Use **dhcp-server ip-pool** to set DHCP SERVER ip pool. Gateway and DNS are optional. If they are not set, the default is 0.0.0.0; note: ip-pool name is 16 characters, and it is exclusive. Start IP can not be over end IP; The IP must belong to same network segment, and total number cannot exceed 4k. The can be 20 IP pool at most.

[Explanation of command execution echo]

set DHCP server ip pool success.
set DHCP server ip pool failure.
name length must is 8 chars.
the input address range too big ,the free is X
the input parameters are error!
the vlan are error!
delete DHCP server ip pool success.
delete DHCP server ip pool failure.
delete DHCP server ip pool failure, name isn't exist.

[Example]

Set DHCP SERVER ip pool:

Raisecom(config)# ***dhcp-server ip-pool name*** *abcdefgh 192.168.1.80 192.168.1.100* ***mask*** *255.255.255.0* ***vlan*** *2,20-30,48* ***gateway*** *192.168.1.1* ***dns*** *192.168.1.1*

delete DHCP SERVER ip pool abcdefgh:

Raisecom(config)# ***no dhcp-server ip-pool name*** *abcdefgh*

[Related command]

Command	Description
show dhcp-server ip-pool	Show ip-pool config information

3.31. dhcp-server max-lease

[Introduction]

Set DHCP SERVER max-lease. **no dhcp-server max-lease** recover the default value

[no] dhcp-server max-lease timeout

[Parameter]

timeout unit is minute,range from 30 minutes to 10080 minutes,integer.

[Default]

The default time is 10080 minutes.

[Command mode]

Global configuration mode, privileged user.

[Usage Guide]

Use **dhcp-server max-lease** to set DHCP SERVER max lease. Use **no dhcp-server max-lease** to recover the default setting.

Note: max-lease time can not be less than min-lease time. if the designated value of client is more than this value, the maximum timeout value is applied.

[Explanation of command execution echo]

Set DHCP server max lease timeout success.
the previous message is displayed, when it is successful;
Set DHCP server max lease timeout failure.
the previous message is displayed, when it fails;
DHCP server max lease timeout is less than min lease timeout.
the previous message is displayed, when DHCP server max lease timeout is less than min lease timeout

[Example]

Set DHCP SERVER max-lease time of lease table as 3600 minutes:

Raisecom(config)# ***dhcp-server max-lease 3600***

recover DHCP SERVER max-lease time:

Raisecom(config)# ***no dhcp-server max-lease***

[Related command]

Command	Description
show dhcp-server	Show DHCP SERVER configuration and statistical information

3.32. dhcp-server min-lease

[Introduction]

Set DHCP SERVER min-lease. Use **no dhcp-server min-lease** command to recover to default time value

[no] dhcp-server min-lease timeout

[Parameter]

timeout, unit is minute, range from 30 minutes to 10080 minutes,integer.

[Default]

The default time is 30 minutes.

[Command Modes]

Global configuration mode, privileged user.

[Usage Guide]

Use **dhcp-server default-lease** to set DHCP SERVER default lease time for lease table. Use **no dhcp-server default-lease** to recover the default setting.

[E*xplanation of command execution echo]*

set DHCP server min lease timeout success.
the previous message is displayed, when it is successful;
set DHCP server min lease timeout failure.
the previous message is displayed, when it fails;
DHCP server max lease timeout is less than min lease timeout.
the previous message is displayed, when DHCP server max lease timeout is less than min lease timeout.

[Example]

Set DHCP SERVER min-lease timeout value as 3600 minutes:

Raisecom(config)# ***dhcp-server min-lease 3600***

Recover DHCP SERVER min-lease timeout value:

Raisecom(config)# ***no dhcp-server min-lease***

[Related command]

Command	Description
show dhcp-server	Show DHCP SERVER config and statistical information

3.33. dhcp-server relay-ip

[Introduction]

Set neighbor DHCP Relay address. Use **no dhcp-server relay-ip** command to delete DHCP Relay address

dhcp-server relay-ip ip-address ip-mask

no dhcp-server relay-ip ip-address

[Parameter]

ip-address set neighboring DHCP Relay IP address, format is dotted decimal,eg:A.B.C.D.

ip-mask set neighboring DHCP Relay IP mask, format is dotted decimal,eg:A.B.C.D.

schedule-list set the starting time, ending time and time interval of dispatching task.

list-no list range from <0-99>;

[Default]

No DHCP Relay neighbor IP address.

[Command Modes]

Global configuration mode, privileged user.

[Usage Guide]

Use **dhcp-server relay-ip** to set neighbor DHCP Relay address. **no dhcp-server relay-ip** delete neighboring DHCP Relay address. The max number of neighboring DHCP Relay address is 8.

[Explanation of command execution echo]

Set DHCP Server IP address success
the previous message is displayed, when set neighboring DHCP Server IP address successfully;
Set DHCP Server IP address failure
The previous message is displayed, when set neighboring DHCP Server IP address failure, the possible reason is the address number exceeds maximal limit.
Delete DHCP Server IP address success
the previous message is displayed, when delete neighboring DHCP Server IP address success
Delete DHCP Server IP address failure
The previous message is displayed, when delete neighboring DHCP Server IP address failure, the possible reason is the address is N/Axistent.

[Example]

Set neighbor DHCP Relay IP address to 10.0.0.1,mask as 255.0.0.0:

*Raisecom(config)# **dhcp-server relay-ip** 10.0.0.1 255.0.0.0*

Delete neighbor DHCP Relay IP address 10.0.0.1:

*Raisecom(config)# **no dhcp-server relay-ip** 10.0.0.1*

[Related command]

Command	Description
show dhcp-server relay-ip	Show neighbor DHCP Relay address information

3.34. dir

[Introduction]

Use **dir** to show flash file storage system.

dir

[Parameter]

N/A

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#**dir***

*The below information is displayed when **dir** is operated:*

size date time name

----

32 Dec-31-2000 00:00:14 durable.

32 Dec-31-2000 00:00:14 durable

[Related command]

Command	Description
Write	Save the current system config
Erase	Delete the designated file in falsh
Download	Download system config file or start-up file
Upload	Upload system config file or start-up file

3.35. disable

[Introduction]

Use **disable** to exit from Privileged EXEC.

disable

[Parameter]

N/A

[Command Modes]

Privileged EXEC, privileged user.

[Usage Guide]

N/A

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#**disable***

[Related command]

Command	Description
Enable	Access priviledged exec from normal exec

3.36. dlf-forwarding

[Introduction]

Enable or disable DLF.

dlf-forwarding {**enable** | **disable**} [**schedule-list** list-no]

[Parameter]

enable transmit DLF message;

disable do not transmit DLF message;
schedule-list set the starting time, ending time and time interval of the dispatching task.
list-no list number <0-99>;

[Default]

DLF is enabled.

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

Only the user with priority 15 can use this command.

[Explanation of command execution echo]

Set successfully
Set unsuccessfully

[Example]

Transmit DLF message
Raisecom(config)# ***dlf-forwarding enable***

[Related command]

Command	Description
show dlf-forwarding	Show DLF status

3.37. download

[Introduction]

Use **download** to download system config file or start-up file to flash file system.

download {system-boot|startup-config} {tftp | ftp}

[Parameter]

system-boot boot file
startup-config config file
tftp tftp download
ftp ftp download

[Default]

N/A

[Command Modes]

Privileged EXEC and privileged user

[Usage Guide]

Use **download** to download boot file and config file to flash file system. When the switch is restarted, the downloaded file will execute automatically. This command can be realized with different file transport protocols for example **ftp** protocol and **tftp**. Before using these two protocols, ftp server or tftp server must be set properly and connected to the switch.

[Explanation of command execution echo]

· *Read error.*

Errors occurred when read the server

·*Invalid input file name*

Errors occurred when input a wrong file name

· *User name is empty!*

FTP user name is empty.

· *User password is empty!*

FTP user password is empty

[Example]

*Raisecom# **download system-boot ftp***
Please input server IP Address:1.0.0.1
Please input FTP User name:test
Please input FTP Password:test
Please input FTP Server File Name:system_boot.Z

Use **ftp** to download boot file from ftp server

[Related command]

Command	Description
Upload	Upload start-up file or boot file

3.38. Duplex

[Introduction]

Use duplex command to set duplex mode of the physical ports

duplex { full | half } [**schedule-list** list-no]

[Parameter]

full duplex;
half half-duplex;
schedule-list starting time, ending time and time interval of dispatching task.
list-no list range from <0-99>;

[Default]

Auto negotiation

[Command format]

Ethernet physical interface configuration mode and physical interface range configuration mode; privileged user.

[Usage Guide]

Only the user with priority 15 can use this command.

[Explanation of command execution echo]

Set successfully
Port X set unsuccessfully

[Example]

Configure the Ethernet port 4 as half-duplex

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

[Related command]

Command	Description
show interface port	Show the state of particular port or all the ports

3.39. enable

[Introduction]

Use **enable** to access the Privileged EXEC.

enable

[Parameter]

N/A

[Command Modes]

User EXEC and normal user

[Usage Guide]

Access Privileged EXEC from normal exec.

[Explanation of command execution echo]

N/A

[Example]

*Raisecom>**enable***
Password:

[Related command]

Command	Description
enable password	Change the password for privileged user
disable	Exit privileged user mode and back to the starting mode

3.40. enable login

[Description]

Use **enable login** command to set the users in privileged user mode.

enable login { local-user | radius-user }

[Parameter]

local-user to set **enable** password for local-user

radius-user the **enable** password for radius server

[Format command]

Privileged EXEC; privileged user.

[Usage Guide]

Enable user of this switch, the default password is ‘raisecom’

When using the user for radius server, the name of enable user is ‘iscom_admin’,so if you want to login successfully, must add the user ‘iscom_admin’to radius server.

The maximum length of password is 16 characters.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

*Raisecom# **enable login local-user***

[Related command]

Command	Description
enable password	Change the password for access privileged user mode.
enable	From starting mode to privilege user mode.

3.41. enable password

[Introduction]

Use **enable password** to set the password for access Privileged EXEC.

no enable password recover password to default value.

enable password

no enable password

[Parameter]

- **null** password is empty
- PASSWORD password string

[Default]

Default password is“raisecom” from User EXEC to Privileged EXEC.

[Command Modes]

Privileged EXEC and privileged user

[Usage Guide]

Use this command to change the user password for entering privileged EXEC

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#**enable password***

[Related command]

Command	Description
Enable	Access privileged mode from normal mode
disable	Exit privileged mode to normal mode

3.42. english

[Introduction]

Display the command line help information in English

english

[Parameter]

N/A

[Default]

Display the command line help information in English

[Command Modes]

User EXEC, Privileged EXEC, Global configuration mode, VLAN configuration mode, interface configuration mode; common user, privileged user

[Usage Guide]

Display the command line help information in English.

[Explanation of command execution echo]

Set successfully.

Command executed successfully.

[Example]

*Raisecom#**english***

[Related command]

Command	description
chinese	Show the help information as the format of command-line in Chinese

3.43. erase

[Introduction]

Use **erase** to delete the designated file in flash file system.

erase [FILENAME]

[Parameter]

FILENAME

[Default]

Delete the current startup_config.conf

[Command Modes]

Privileged EXEC and privileged user

[Usage Guide]

N/A

[Explanation of command execution echo]

Erase current specified file successfully!

Command executed successfully

Erase current specified file Fail!

Command executed unsuccessfully

[Example]

*Raisecom#**erase** aaa*

Delete 'aaa' file in flash file system.

[Related command]

Command	Description
Write	Save the current system config file

3.44. exit

[Introduction]

Use **exit** to return to previous mode or exit login

exit

[Parameter]

N/A

[Command Modes]

User EXEC, Privileged EXEC, global configuration mode, VLAN configuration mode, interface configuration mode, routing protocol configuration mode, normal user, and privileged user

[Usage Guide]

N/A

[Explanation of command execution echo]

N/A

[Example]

*Raisecom>**exit***

[Related command]

Command	Description
Quit	Return to parent mode or exit login

3.45. help

[Introduction]

Use "help" to show the help information of system.

help

[Parameter]

N/A

[Command Modes]

User EXEC, Privileged EXEC, global configuration mode, VLAN configuration mode, interface configuration mode, routing protocol configuration mode, normal user, and privileged user

[Usage Guide]

Use this command to show help information of command line.

[Explanation of command execution echo]

ROS software provides advanced help feature. When you need help, anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show?') and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show me?').

[Example]

*Raisecom>**help***

[Related command]

N/A

3.46. filter

NOT AVAILABLE FOR: 2126/2016/2008/2026.

[Introduction]

This command is used to add the filter rules. Use **no** form of this command to delete a filter rule.

[Command format]

[no] filter (ip-access-list | mac-access-list | access-list-map) (all | {0-399}**)**

[no] filter (ip-access-list | mac-access-list | access-list-map) (all | {0-399}**) (ingress | egress) port-list** {1-26}

[no] filter (ip-access-list | mac-access-list | access-list-map) (all | {0-399}) vlan <1-4094>

[no] filter (ip-access-list | mac-access-list | access-list-map) (all | {0-399}**) from** <1-26> **to** <1-26>

[Parameter]

ip-access-list|mac-access-list| access-list-map: the type of ACL for filtering rule linked list

all|{0-399}:Serial number of ACL, if “all”, it is the defined ACL.

port –list{1-26} physical port control list;

ingress: filter at the receiving port

egress: **filter at the sending port**

from: the filtering receiving port at receiving port and transmission port

to: the filtering sending port at receiving port and transmission port.

Vlan-list<1-4094>: VLAN number

[Default]

N/A

[Command Modes]

Global configuration mode; privileged use exec.

[Usage Guide]

This command is used to add one or more filter rules, the filter rule contains an ordered list of previous defined ACL or VLAN, the priority of these rules is decided by sequence of these filtering rules, the later the filtering rule is added, the higher

priority it has. If there is conflicts when the switch tests the packets against the conditions in access list one by one, the higher priority filter rule will be effective (the later added rule). User should properly use all of these rules to limit the incoming packets.

The filter rules will be effective only if filter function is globally enabled.

[Explanation of command execution echo]

Set access list XX unsuccessfully

Delete access list XX unsuccessfully, there is no this filter!

Set successfully

Set unsuccessfully

[Usage Guide]

filter ip-access-list 0 ingress portlist 5

[Related command]

Command	Description
show filter	Show the relevant information for the matching rule filter.
filter enable | disable	Start/cancel the filtering function.

3.47. filter {enable|disable}

NOT AVAILABLE FOR: 2126/2016/2008/2026.

[Introduction]

This command is used to enable filter function globally. Only filter function is enabled globally, the switch will test the packets against the conditions in an access list one by one.

[Command format]

filter enable | disable

[Parameter]

Enable:Enable filtering function.

Disable:Disable filtering function

[Default]

Disable

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

N/A

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

filter enable

[Related command]

command	description
filter	Configure filter rules
show filter	Show related filter information

3.48. flowcontrol

[Introduction]

Enable or disable the flow control function at the physical port

flowcontrol { **on** | **off** }

[Parameter]

- **receive:** flow control at the receiving direction
- **sent**: flow control at the sending direction
- **on** Enable flow control function
- **off** Disable flow control function
- **schedule-list:** set the starting time, ending time and time interval of periodical execution.
- **list-no:** dispatching list number range from <0-99>.

[Default]

The flow control function is disabled at physical port by default.

[Command Modes]

The physical interface Ethernet/range configuration mode; privileged user.

[Usage Guide]

Only the privileged user who has priority 15 can use this command.

[Explanation of command execution echo]

Set successfully

Port X set unsuccessfully

[Example]

- Enable the flow control function at the RX direction.
  Raisecom(config-port)# ***flowcontrol receive on***
- Disable the flow control function at the TX direction.
  Raisecom(config-port)# ***flowcontrol send off***

3.49. history

[Introduction]

Use this command to show history command.

history

[Parameter]

N/A

[Default]

The number of history command in memory is 20.

[Command Modes]

User EXEC, Privileged EXEC, global configuration mode, VLAN configuration mode, interface configuration mode, routing protocol configuration mode, normal

user, and privileged user

[Usage Guide]

Use this command to show history command of each mode.

[Explanation of command execution echo]

· ter time-out 65535

enable

chin

enable

help

eng

[Example]

*Raisecom>**history***

[Related command]

Command	Description
terminal history	Change the number of history command in memory.

3.50. hostname

[Introduction]

Use “hostname” command to configure system name of current user.

Use “no hostname” command to restore default system name.

hostname HOSTNAME

no hostname

[Parameter]

HOSTNAME: System name of new appoint to user.

[Default]

The default value of hostname is raisecom.

[Command Modes]

Privileged EXEC and privileged user

[Usage Guide]

This command is easy to different user to use different hostname, and different host can be marked with different hostname.

[Explanation of command execution echo]

· *Hostname length must less than 32!*

It means the character length of the hostname is out of the defined scale.

Set successfully

[Example]

*Raisecom#**hostname** switch*

Change the hostname to “switch”

[Related command]

N/A

3.51. interface ip

[Introduction]

to IP interface mode.

interface ip <0-14>

[Parameter]

<0-14> **IP interface number.**

[Default]

all the system IP interfaces have no address

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use **interface ip** command to enter IP configuration mode.

[Example]

To the configuration mode for IP interface 4

*rc026(config)# **interface ip** 4*

[Related command]

Command	Description
ip address	Set the IP address
show interface vlan	Show the layer-3 interface

3.52. interface port

[Introduction]

Enter physical interface mode.

interface port <1-26>

[Parameter]

<1-26> Physical interface

[Default]

N/A

[Command Modes]

Global configuration mode and privileged user

[Usage Guide]

Use "**interface port**" to enter physical interface configuration mode.

[Example]

Enter physical interface 4 configuration mode.

*Raisecom (config)# **interface port** 4*

[Related command]

Command	Description
show interface port	Show information of physical port

3.53. interface range

[Introduction]

Enter Physical port range configuration mode

interface range {port-list | all}

[Parameter]

- **range** physical port range configuration mode.
- **port-list** physical port number range from 1-26, use "," and "-" to configure several ports at one time.
- **all** all the ports.

[Default]

N/A

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use **interface range** command to enter physical range configuration mode. In this mode, you can configure more than one physical port at one time.

[Example]

Enter the configuration mode for physical port 4-10

*Raisecom (config)# **interface range** 4-10*

[Related command]

Command	description
show interface port	Show the physical ports information

3.54. ip-access-list

[Introduction]

Set IP access control list, use “no” to delete this operation.

[command format]

ip-access-list <0-399> **(deny | permit) (ip|tcp|udp|icmp|igmp|<0-255>) (**A.B.C.D A.B.C.D | **any)** [<1-65535>] **(**A.B.C.D A.B.C.D | **any)** [<1-65535>]

[Parameter]

0-399: serial number for IP Access Control List.

permit: Permit access if conditions are matched.

deny:Deny access if conditions are matched.

protocol: define protocol type in the packet head. Protocol type can be icmp, igmp, tcp, udp, ip, protocol number from 0-255, if set the value to IP or 0, it stands for all IP packets.

A.B.C.D A.B.C.D **| any**:The first A.B.C.D denotes source IP address, the second A.B.C.D denotes mask of source address, all of them use dotted decimal notation; **any** stands for all the source IP address.

1-65535:it is the source port number of TCP or UDP packet, 1~65535.

[Default]

N/A.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to define an IP ACL, the parameter **permit | deny** is used to permit or deny the access of packets. This command only set the data filter conditions, and need to be applied to physical port or VLAN to let it be effective.

[Explanation of command execution echo]

The mask is wrong.

Set successfully

Set unsuccessfully

[Example]

ip-access-list *50* ***deny icmp*** *192.168.1.19 255.255.255.255* ***any***

[Related command]

command	description
no ip-access-list ({0-399}**|all)**	Delete all IP ACL entries
show ip-access-list [{0-399}]	Show all the IP ACL entries

3.55. ip address

[Introduction]

Set IP address of current interface.

Use “no ip address” to delete IP address of current interface.

ip addreass ip-address [ip-mask] vlan-id

no ip addreass ip-addres

[Parameter]

- ip-address Set IP address of current interface, format is dotted decimal, eg:A.B.C.D
- ip-mask Set IP mask, format is A.B.C.D
- vlan-id VLAN ID of corresponding layer 3 interface.

[Default]

N/A.

[Command Modes]

Ethernet-layer 3 interface configuration mode and privileged user

[Usage Guide]

This command is used to configure IP address for management interface. Before the configuration of the interface IP address, the interface of concerned VLAN must be configured. The IP address of interface should be A, B or C class.

[Explanation of command execution echo]

Set successfully
Set unsuccessfully
Too many VLAN Set in the interface.
VLAN not exist or no member port.
The total number of IP subnet and static routes have exceeded the max value(14).
Can't add ip interface for cluster member.
Invalid network mask.
Invalid IP address or network mask.
VLAN X already associated with interface Y (ifIndex: 1100003).
A.B.C.D overlaps with interface X (ifIndex: 1100003).

[Example]

- set current interface IP address to 192.168.1.2, associated VLAN ID is 2.
  Raisecom(config-ip)# ***ip address*** *192.168.1.2 255.255.255.0 2*
- erase interface IP address
- *Raisecom(config-ip)#* ***no ip address*** *192.168.1.2*

[Related command]

command	description
state	Enable current VLAN.
vlan-access	Add current interface toVLAN
show ip route	Show the route
show interface vlan	Show VLAN interface

3.56. ip default-gateway

[Introduction]

Use **ip default-gateway** command to set default gateway, **no ip default-gateway** to delete default gateway.

ip default-gateway A.B.C.D

no ip default-gateway

[Parameter]

A.B.C.D the ip address of default gateway.

[Default]

N/A.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

When a packet do not find the router of the network, use this command can let the system transfer all the packets to the default gateway.

[Explanation of command execution echo]

Invalid next-hop IP address.

Can't Set gateway for cluster member.

Set successfully

[Example]

- set the default gateway to 10.0.0.1
  *Raisecom(config)# **ip default-gateway** 10.0.0.1*
- delete the configuration of default gateway.
  *Raisecom(config)# **no ip default-gateway***

[Related command]

command	description
show ip route	Show the system routing information

3.57. ip igmp filter

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Enable or disable IGMP filter function.

[Command format]

[no] ip igmp filter

[Description]

N/A

[Default]

IGMP filtering function enable

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to start the IGMP filtering function. use **no ip igmp filter** command to stop IGMP filter function.

[Explanation of command execution echo]

Enable IGMP filter successfully

Enable IGMP filter unsuccessfully

Disable IGMP filter successfully

Disable IGMP filter unsuccessfully

[Example]

start IGMP filter function

*Raisecom(config)#**ip igmp filter***

Stop IGMP filter function

*Raisecom(config)#**no ip igmp filter***

[Related command]

command	description
show ip igmp filter	Show IGMP filter configuration information

3.58. ip igmp filter

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Apply IGMP profile to physical port.

[command format]

ip igmp filter profile-number

no ip igmp filter

[Parameter]

profile-number——serial number of IGMP profile, range from 1 to 65535.

[Default]

Do not apply IGMP profile, shown as 0.

[Command Modes]

Physical port configuration mode; privileged user.

[Usage Guide]

Use this command to set the IGMP profile on ports. One IGMP profile can be applied to many ports, but each port can only apply one profile. Use **no ip igmp profile** command to delete IGMP profile.

[Explanation of command execution echo]

Set IGMP filter profile number successfully

Set IGMP filter profile number unsuccessfully

Cancel a IGMP profile number on the port successfully

Cancel a IGMP profile number on the port unsuccessfully

[Example]

Create IGMP profile:

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

*Raisecom(config-port)# **ip igmp filter** 1*

[Related command]

command	description
show ip igmp profile	Show IGMP profile configuration information
show ip igmp filter port	Show the applied IGMP profile information of the port

3.59. ip igmp max-groups

NOT AVAILABLE FOR: ISCOM2026.

[Description]

Set the maximum number for multicast groups.

[Command format]

ip igmp max-groups group-number

no ip igmp max-groups

[Parameter]

Group-number——maximum group number, range from 0 to 65535. 0 stands for no limitation.

[Default]

No limitation on max-groups number

[Command Modes]

Physical port configuration mode; privileged user.

[Usage Guide]

Use this command to set the max-groups. Apply this limitation to MVR and IGMP snooping.

[Explanation of command execution echo]

Set the IGMP max group number on the port successfully

Set the IGMP max group number on the port unsuccessfully

Unlimited the IGMP max group number on the port successfully

Unlimited the IGMP max group number on the port unsuccessfully

[Example]

Set the max-groups of the port permitted to 10

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

*Raisecom(config-port)# **ip igmp max-groups** 10*

[Related command]

command	description
show ip igmp filter port	Show the IGMP profile which applied on the port

3.60. ip igmp max-groups action

NOT AVAILABLE FOR: ISCOM2026.

[Description]

Actions that will be taken when the number of multicast group members exceeds max-group number.

[Command format]

ip igmp max-groups action { deny | replace }

no ip igmp max-groups action

[Parameter]

deny——when number of multicast group members exceed max-groups number, IGMP packets will be denied, that is to say no more subscribers are not allowed to add in multicast group.

replace——when number of multicast group members exceed max-groups number, original groups member will be replaced. NOT AVAILABLE FOR THIS VERSION.

[Default]

Deny.

[Command Modes]

Physical port configuration mode; privileged user.

[Usage Guide]

Actions to be taken when multicast group number exceeds max-groups number. If there is no limitation on maximum multcast group number, no action will be taken.

Use **no ip igmp max-group** action to recover to default status.

[Explanation of command execution echo]

Set the action that the port takes when exceed the max groups successfully

Set the action that the port takes when exceed the max groups unsuccessfully

[Example]

set the maximum multcast group number as 10, action is deny.

*Raisecom(config)#**interface port 1***
*Raisecom(config-port)# **ip igmp max-groups** 10*
*Raisecom(config-port)# **ip igmp max-groups action deny***

[Related command]

command	description
show ip igmp filter port	Show IGMP profile information which applied on the ports.

3.61. ip igmp profile

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Create or delete IGMP profile.

[Command format]

[no] ip igmp profile profile-number

[Parameter]

profile-number——IGMP profile number, range from 1 to 65535.

[Default]

N/A.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to create IGMP profile and enter IGMP profile configuration mode. User **no ip igmp profile** command to delete IGMP profile. IGMP profile can only be applied to physical ports, and each port can only apply one profile.

[Explanation of command execution echo]

Create the IGMP profile successfully

Create the IGMP profile unsuccessfully

Delete the IGMP profile successfully

Delete the IGMP profile unsuccessfully

[Example]

create IGMP profile:

*Raisecom(config)#**ip igmp profile** 1*

Erase IGMP profile:

*Raisecom(config)#**no ip igmp profile** 1*

[Related command]

command	description
show ip igmp profile	Show IGMP profile configuration information

3.62. ip igmp snooping

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Use this global command to enable IGMP Snooping, use “**no ip igmp-snooping**” to disable this function.

[no] ip igmp snooping [**schedule-list** list-no]

[Parameter]

Schedule-list set the starting time, ending time and time interval of periodical task.
list-no periodical list number range from<0-99>;

[Default]

IGMP Snooping function disables.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

When start IGMP snooping, IGMP snooping function will be enabled on all current VLAN; When the function is disabled, IGMP snooping function will be disabled on all current VLAN.

[Explanation of command execution echo]

Enable IGMP snooping successfully
Enable IGMP snooping unsuccessfully
Disable IGMP snooping successfully
Disable IGMP snooping unsuccessfully

[Example]

Start IGMP snooping

Raisecom(config)# ***ip igmp snooping***

Stop IGMP Snooping

*Raisecom(config)#****no ip igmp snooping***

[Related command]

command	description
show ip igmp snooping	Show IGMP Snooping config information

3.63. ip igmp snooping

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Use this global command to enable IGMP Snooping, use “**no ip igmp-snooping**” to disable this function.

[no] ip igmp snooping [**schedule-list** list-no]

[Parameter]

Schedule-list set the starting time, ending time and time interval of periodical task.
list-no dispatching list number range from<0-99>;

[Default]

IGMP Snooping is enabled in all active VLAN.

[Command Modes]

VLAN configuration mode; privileged user.

[Usage Guide]

Use this command to enable IGMP snooping function on VLAN, use no igmp

snooping to stop IGMP snooping function on VLAN.

[Explanation of command execution echo]

- *Enable IGMP snooping on VLAN 1 successfully*
- *Enable IGMP snooping on VLAN 1 unsuccessfully*
- *Disable IGMP snooping on VLAN 1 successfully*
- *Disable IGMP snooping on VLAN 1 unsuccessfully*

[Example]

- start IGMP snooping of VLAN 1.

  Raisecom(config-vlan)# ***ip igmp snooping***

- stop IGMP Snooping on VLAN 1.

  *Raisecom(config-vlan)#****no ip igmp snooping***

[Related command]

Command	Description
show ip igmp snooping	Show IGMP Snooping config information
show ip igmp snooping vlan	Show IGMP Snooping config information of assigned VLAN

3.64. ip igmp snooping immediate-leave

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Use this command to enable IGMP snooping immediate-leave function on assigned VLAN, use **no ip igmp snooping immediated-leave** to stop the IGMP snooping immediate-leave function on designated VLAN.

[Command format]

ip igmp snooping immediate-leave

[no] ip igmp snooping immediate-leave

[Parameter]

N/A

[Default]

IGMP Snooping immediate-leave function is disabled by default.

[Command Modes]

VLAN configuration mode; Privileged user.

[Usage Guide]

Use this command to start IGMP snoop immediate-leave function on designated VLAN, use **no ip igmp snooping immediate-leave** to stop IGMP snoop immediate-leave function.

[Explanation of command execution echo]

- *Enable IGMP immediate-Leave processing on the VLAN 1 successfully*
  Enable IGMP Immediate-Leave processing on the VLAN 1 unsuccessfully
  Disable IGMP Immediate-Leave processing on the VLAN 1 successfully
  Disable IGMP Immediate-Leave processing on the VLAN 1 unsuccessfully

[Example]

- start the IGMP snooping immediate-leave on VLAN1

  ISCOM2016(config-vlan)# ***ip igmp snooping immediate-Leave***

- stop the IGMP snooping immediate-leave on VLAN1

  *ISCOM2016(config-vlan)#****no ip igmp snooping immediate-Leave***

[Related command]

command	description
show ip igmp snooping	Show IGMP Snooping config information
show ip igmp snooping vlan	Show IGMP Snooping config information on designated VLAN

3.65. ip igmp snooping mrouter

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Use this command to set the multicast router port on designated VLAN, use **no ip igmp snooping mrouter** to delete.

[Command format]

ip igmp snooping mrouter vlan <1-4094**> port <**1-26**>**

[no] ip igmp snooping mrouter vlan <1-4094**> port <**1-26**>**

[Parameter]

N/A

[Default]

N/A

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to set the router port on designated VLAN, use **no ip igmp snooping mrouter** to delete router port. use this command to set the router port manually, so igmp packet can be transferred to this port.

[Explanation of command execution echo]

Set multcast router port successfully
Set multcast router port unsuccessfully
Set multcast router port successfully
Set multcast router port unsuccessfully

[Example]

Set the IGMP Snooping router port on VLAN 1 manually.

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

Erase the IGMP Snooping router port on VLAN 1 manually

*ISCOM2826(config)#****no ip igmp snooping mrouter vlan 1 port 2***

[Related commands]

command	description
show ip igmp snooping mrouter	Show IGMP Snooping mrouter information
show ip igmp snooping vlan mrouter	Show VLAN IGMP Snooping mrouter config information

3.66. ip igmp snooping vlan-list

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Use this command to start the IGMP snooping function on particular VLAN, use no ip igmp snooping vlan to stop the IGMP snooping function on particular VLAN.

[Command format]

ip igmp snooping vlan-list vlanlist

[no] ip igmp snooping vlan-list vlanlist

[Parameter]

vlanlist——VLAN list, range from 1-4094, format is{1-4094}, Example 2-100,120.The longest parameter is 50 characters.

[Default]

When the IGMP Snooping has been started, all the VLAN will start IGMP Snooping function as the default situation.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to start IGMP snooping on particular VLAN, use no ip igmp snooping vlan to stop IGMP Snooping function on particular VLAN. Use this command to start/stop the IGMP snooping on many VLAN.

[Explanation of command execution echo]

Enable IGMP snooping on VLAN 1 —10 successfully
Enable IGMP snooping on VLAN 1 —10 unsuccessfully
Disable IGMP snooping on VLAN 1 —10 successfully
Disable IGMP snooping on VLAN 1 —10 unsuccessfully

[Example]

- start the IGMP Snooping function on VLAN 1-10 and 12,15.

  ISCOM2016(config)# ***ip igmp snooping vlan-list 1-10,12,15***

- stop the IGMP Snooping function on VLAN 1-10 and 12, 15.

  *ISCOM2016(config-vlan)#****no ip igmp snooping vlan-list 1-10,12***

[Related command]

command	Description
show ip igmp snooping	Show IGMP Snooping config information
show ip igmp snooping vlan	Show VLAN IGMP Snooping config information

3.67. ip igmp snooping vlan-list *vlanlist* immediate-leave

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Use this command to start the IGMP snooping immediate leave function on particular VLAN, use no ip igmp snooping vlan to stop the IGMP snooping immediate leave function.

[Command format]

ip igmp snooping vlan-list vlanlist **immediate-leave**

[no] ip igmp snooping vlan-list vlanlist **immediate-leave**

[Parameter]

vlanlist——VLAN list, range from 1-4094, the format is{1-4094}, Example 2-100,120.The longest parameter has 50 characters.

[Default]

Disable by default.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to start IGMP snooping immediate leave function on designated VLAN, use **no ip igmp snooping vlan** to stop the IGMP snooping immediate leave

function on designated VLAN. Use this command to start/stop IGMP snooping immediate leave function on VLAN.

[Command execution mode]

Enable IGMP immediate-Leave processing on the VLAN 1 —10 successfully
Enable IGMP Immediate-Leave processing on the VLAN 1 —10 unsuccessfully
Disable IGMP Immediate-Leave processing on the VLAN 1 —10 successfully
Disable IGMP Immediate-Leave processing on the VLAN 1 —10 unsuccessfully

[Example]

Start the IGMP snooping immediate leave function on VLAN 1-10 and 12, 15.

ISCOM2016(config)# ***ip igmp snooping vlan-list 1-10,12,15 immediate-Leave***

Stop the IGMP snooping immediate leave function on VLAN 1-10 and 12,15.

*ISCOM2016(config)#****no ip igmp snooping vlan-list 1-10,12 immediate-Leave***

[Related command]

command	description
show ip igmp snooping	Show IGMP Snooping information
show ip igmp snooping vlan	Show VLAN IGMP Snooping information on assigned VLAN

3.68. ip igmp snooping timeout

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Use this command to configure time of IGMP snooping timeout. Use “no ip igmp-snooping timeout” to resume default configuration.

ip igmp-snooping timeout timeout

[no] ip igmp-snooping timeout

[Parameter]

timeout IP IGMP Snooping aging time, unit is second, range from 30 to 3600 second.

[Default]

Default value of timeout is 300 seconds.

[Command Modes]

Global configuration mode and privileged user

[Usage Guide]

This command configure valid time of multicast route in IGMP Snooping, multicast route is deleted when timer is overtime.

[Explanation of command execution echo]

set igmp snooping aging success
set igmp snooping aging failure
set igmp snooping aging default success
set igmp snooping aging default failure

[Example]

- Set time of IGMP snooping timeout is 3000 second.

  Raisecom(config)# ***ip igmp-snooping timeout*** *3000*

- Set time of IGMP snooping timeout is default value.

  Raisecom(config)# ***no ip igmp-snooping timeout***

[Related command]

Command	Description
show ip igmp-snooping	Show configuration information of IGMP Snooping.

3.69. ip ip-access-list

[Introduction]

The command is used to add the filter rule into layer-3 interface, use **no** command to delete filtering rule.

[Command format]

[no] ip ip-access-list (all | {0-199})

[Parameter]

Ip-access-list: IP access list.

All |{0-399}:the serial number of ACL, if it is “all”, then that is all the defined IP ACL.

[Default]

N/A

[Command mode]

Ethernet layer-3 interface mode; privileged user.

[Usage Guide]

Use this command to apply one or more previously defined IP ACL to layer-3 interface.

The previously defined IP ACL applies on layer-3 interface, and will be effective whne receives packets.

[Explanation of command execution echo]

Set access list XX failed

Set successfully

Set unsuccessfully!

[Example]

Raisecom(config-ip): ip ip-access-list 0

[Related command]

command	description
show interface ip ip-access-list	Show layer-3 access control configuration
ip-access-list	IP access list configuration

3.70. ip route

NOT AVAILABLE FOR: ISCOM2826/2126/2016/2008/2026/2826E.

[Introduction]

Use “ip route”to add static route,use “no ip route ”to delete static route.

ip route A.B.C.D_1 E.F.G.H_2 a.b.c.d_3

no ip route[A.B.C.D_1 [E.F.G.H]]

[Parameter]

- A.B.C.D_1 network prefix;
- A.B.C.D_2 max;
- A.B.C.D_3 next hop IP address

[Default]

If command of “no” form has no network prefix,then delete all static route.

If command of “no”form has no network mask,then delete all static route that match to the mask.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Static route is configurated by network administrator,this route path will change with network topology, next-hop route must be direct route when use “**ip route**”to add route.

[Explanation of command execution echo]

Invalid destination IP address.

Invalid destination MASK.

Invalid next-hop IP address.

Can not set Connected Route to Static.

The total number of IP subnet and static routes has exceed the max value(14).

Can't add static route for cluster member

Inconsitent prifix and mask

No such static route !

Set successfully

[Example]

Add a route that its destination network is 10.0.0.0,through interface of local 4.0.0.1 transmit.

*Raisecom(config)#**ip route** 10.0.0.0 255.0.0.0 4.0.0.1*

Delete all static route.

*Raisecom(config)#**no ip route***

[Related command]

Command	Description
show ip route	Show information of route

3.71. ip routing

NOT AVAILABLE FOR: ISCOM2826/2126/2016/2008/2026

[Introduction]

Use the command ip routing to start the IP transfer function, use **no** command to deny this action.

[no] ip routing

[Parameter]

N/A.

[Default]

The system disables ip packet transfer by software.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

N/A

[Explanation of command execution echo]

Set successfully.

[Example]

start the ip transfer function of software.

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

[Related command]

N/A

3.72. list

[Introduction]

Use this command to show all commands in one mode.

list

[Parameter]

N/A

[Command Modes]

User EXEC, Privileged EXEC, Global configuration mode, VLAN configuration exec, interface configuration mode, routing protocol configuration mode; normal user and privileged user

[Usage Guide]

Use this command to show particular parameter of all commands under the mode.

[Explanation of command execution echo]

chinese
clear
enable
english
exit
help
history
list
quit
terminal history <1-20>
terminal time-out <0-65535>

[Example]

*Raisecom>****list***

[Related command]

N/A

3.73. logging console

[Introduction]

Configure and start to print the log information and parameters of console, the “no” command will disable the logging information print.

logging console {<0-7> | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings}

no logging console

[Parameter]

<0-7>	log severity	
alerts	need action immediately	(severity=1)
critical	serious state	(severity =2)
debugging	debug information	(severity =7)
emergencies	system can not use	(severity =0)
errors	error condition	(severity =3)
informational	informational event	(severity =6)
notifications	normal event under critical condition	(severity=5)
warnings	warning condition	(severity=4)

[Default]

Enable and the severity is **informational**

[Command Modes]

Global configuration mode and privileged user

[Usage Guide]

Use this command to configure print logging information to console. And the severity level will decide which level information will be print to console. E.g. if the severity is 0, only when system is unusable there will be logging information printed to console; if the severity level is 7, all logging information will be printed to console. Severity of logging information.

Grade key word	Severity	Description
emergencies	0	System can not use
alerts	1	Need action immediately
critical	2	Serious event
errors	3	Error event
warnings	4	Warning event
notifications	5	Normal but critical
informational	6	Inform message
debugging	7	Debug information

[Explanation of command execution echo]

set successfully!
set fail!

[Example]

Configure the severity level of logging console as alerts

Raisecom(config)#logging console alerts

[Related command]

Command	Description
Logging monitor	Enable output direction of log monitor.
logging host	Enable output direction of log host.
logging file	Enable output direction of log file
logging on	Enable log function
logging time-stamp	Set time stamp of log information
logging rate	Set output speed of log
show logging	Show log information

3.74. logging file

[Introduction]

Configure and start to log events and parameters to log file, the “no” command will disable events to be logged in log file.

logging file

no logging file

[Parameter]

N/A

[Default]

Enable log information to logging file.

The mode of output is config.

[Command Modes]

Global configuration mode and privileged user

[Usage Guide]

Use this command to log information in logging file.

[Explanation of command execution echo]

set successfully!

set fail!

[Example]

Use this command to record log information in logging file.

logging file

[Related command]

Command	Description
Logging console	Enable output direction of log console
logging monitor	Enable output direction of log monitor.
logging file	Enable output direction of log file.
logging on	Enable log function
logging time-stamp	Set time stamp of log information
logging rate	Set output speed of log
show logging	Show log information

3.75. logging host

[Introduction]

Configure and start to log events and parameters to assigned PC, the “no” command will disable the log.

logging host A.B.C.D { local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7} { <0-7> | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings }

no logging host A.B.C.D

[Parameter]

local0-local7	equipment name of log host	
·**<0-7>**	log grade	
·**alerts**	need action immediately	(severity=1)
·**critical**	serious state	(severity =2)
·**debugging**	debug information	(severity =7)
·**emergencies**	system not available	(severity =0)

·**errors** error condition (severity =3)
·**informational** informational event (severity =6)
·**notifications** normal and critical event (severity =5)
·**warnings** warning condition (severity=4)

[Default]

No assigned log host

[Command Modes]

Global configuration mode and privileged user

[Usage Guide]

Use this command to configure the assigned log host and the log severity.

Log description of log host

Grade keywords	Grade	Description
emergencies	0	System not available
alerts	1	Need action immediately
critical	2	Serious event
errors	3	Error event
warnings	4	Warning event
notifications	5	Normal but critical event
informational	6	Inform message
debugging	7	Debug information

[Explanation of command execution echo]

set successfully!
set fail!

[Example]

Raisecom(config)# logging host 10.0.0.1 local7 alerts

[Related command]

Command	Description
Logging console	Enable output direction of log console
logging monitor	Enable output direction of log monitor
logging file	Enable output direction of log file
logging on	Enable log function
logging time-stamp	Set time stamp of log information
logging rate	Set output speed of log
show logging	Show log information

3.76. logging monitor

[Introduction]

Configure and start to display the log information and parameters in the PC terminal when use Telnet management, the “no” command will disable.

logging monitor {<0-7> | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings}

no logging monitor

[Parameter]

<0-7> log grade
alerts need action immediately (severity=1)
critical serious state (severity =2)
debugging debug information (severity =7)
emergencies system can not use (severity =0)
errors error condition (severity =3)

informational informational event (severity =6)
notifications normal but critical event (severity =5)
warnings warning condition (severity =4)

[Default]

Disable

[Command Modes]

Global configuration mode and privileged user

[Usage Guide]

Configure and start to display the log information and parameters in the PC terminal when use Telnet management.

Severity description

Grade keywords	Grade	Description
emergencies	0	System not available
alerts	1	Need action immediately
critical	2	Serious event
errors	3	Error event
warnings	4	Warning event
notifications	5	Normal but critical
informational	6	Inform message
debugging	7	Debug information

[Explanation of command execution echo]

set successfully!
set fail!

[Example]

This command set record log grade of monitor is alters, all message that is lower than it will output to monitor.

logging monitor alerts

[Related command]

Command	Description
Logging console	Enable output direction of log console
logging host	Enable output direction of log host
logging file	Enable output direction of log file
logging on	Enable the log function
logging time-stamp	Set time stamp of log information
logging rate	Set output speed of log
show logging	show log information

3.77. logging on

[Introduction]

Use “logging on” to enable log function, use “no logging on” to disable log function.

[no] logging on

[Parameter]

N/A

[Default]

Log function is enabled

[Command Modes]

Global configuration mode and privileged user

[Usage Guide]

Enable log function

[Explanation of command execution echo]

set successfully!
set fail!

[Example]

Enable log function

logging on

[Related command]

Command	Description
Logging console	enable output direction of log console
logging monitor	enable output direction of log monitor
logging file	enable output direction of log file
logging time-stamp	Set time stamp of log information
logging rate	set output speed of log
show logging	show log information

3.78. logging rate

[Introduction]

Set sending speed of log information, use “no” to restore default setting.

logging rate <1-65535>

no logging rate

[Parameter]

<1-1000> Log number of every second send

[Default]

Not limit sending speed of log

[Command Modes]

Global configuration mode and privileged user

[Usage Guide]

Set send speed of log information

[Explanation of command execution echo]

· *set successfully!*
·*set fai*l!

[Example]

Set every second to send 100 item logs most.

Raisecom(config)# logging rate 100

[Related command]

Command	Description
Logging console	Enable output direction of log console
logging monitor	Enable output direction of log monitor
logging file	Enable output direction of log file
logging time-stamp	Set time stamp of log information
show logging	Show log information

3.79. logging time-stamp

[Introduction]

Set time stamp of log information, use no to restore default value.

logging time-stamp { standard | relative-start | null }

[no] logging time-stamp

[Parameter]

date-time	Absolute time after startup
relative-start	relative time of system enabled
null	not add time stamp

[Default]

Use date-time

[Command Modes]

Global configuration mode and privileged user

[Usage Guide]

Use this command to set time stamp information of system using.

Date-time mmm-dd-yyyy hh-mm-ss

Relative time hh-mm-ss

[Explanation of command execution echo]

set successfully!
set fail!

[Example]

Enable log relative time

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

[Related command]

Command	Description
Logging console	Enable output direction of log console
logging monitor	Enable output direction of log monitor
logging file	Enable output direction of log file
logging rate	Set output speed of log
show logging	show log information

3.80. logout

[Introduction]

Use “logout” to exit login state.

logout

[Parameter]

N/A

[Command Modes]

Privileged EXEC and privileged user

[Usage Guide]

When finish configuring system, use this command to exit login state, if other user want to configure switch again in console, it need to login afresh.

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#**logout***

[Related command]

N/A

3.81. loopback-detection

[Introduction]

Start/close the loopback-detection on designated port.

loopback-detection { enable | disable **} port-list {** portlist | all **}**

[Parameter]

enable enable loopbak-detection function.
disable disable loopback detection function.
portlist physical port number, range from 1-26, use “, ”and“-”to set the input of different ports;
all all the ports;

[Default]

Enable the loopback-detection for all the ports.

[Command Modes]

Global configuration mode; privileged user (priority 15).

[Usage Guide]

User with priority 15 can use this command.

[Explanation of command execution echo]

Failed to set loopback-detection on port X!
Set successfully
Set unsuccessfully

[Example]

start the loopback-detection function for port 6~10
*Raisecom(config)# **loopback-detection** enable **port-list** 6-10*
start the loopback-detection function for all the ports.
*Raisecom(config)# **loopback-detection** enable **port-list** all*
Close the loopback-detection function for port 7~9
*Raisecom (config)# **loopback-detection** disable **port-list** 7-9*
Close the loopback-detection function for all the ports
Raisecom (config)# **loopback-detection** disable **port-list** all

[Related command]

command	description
show loopback-detection	Show the state information of all the ports

3.82. loopback-detection hello-time

[Introduction]

Set the hello time of loopback-detection (the time interval of sending loopback-detection packet). Use no command to recover the default setting.

loopback-detection hello-time <1-65535>

no loopback-detection hello-time

[Parameter]

1-65535 time interval of loopback-detection, second as the unit.

[Default]

The loopback detection packets will be sent every 4 seconds.

[Command Modes]

Global configuration mode; privileged user (priority 15).

[Usage Guide]

Only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Failed to set sending interval !

Set successfully

[Example]

set the loopback-detection interval to 3 seconds.

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

recover the loopback-detection interval to default setting.

Raisecom (config)# ***no loopback-detection hello-time***

[Related command]

command	description
show loopback-detection	Show state of port loopback-detection.

3.83. loopback-detection destination-address

[Introduction]

Set the mac type of loopback-detection, it could be unit cast , multicast or broadcast address, and the mac aging time will be zero. The default loopback-detection mac is broadcast.

loopback-detection destination-address [mac-address **vlan** vlan-id **]**

[Parameter]

mac-address configure the target MAC address.

vlan-id VLAN ID;

[Default]

Broadcast address.

[Command Modes]

Global configuration mode; privileged user（priority 15）.

[Usage Guide]

only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Failed to set loopback-detection destination address!

Set successfully

[Example]

Set the loopback-detection packet to broadcasting packet.

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

Recover the loopback-detection packet to particular MAC.

Raisecom (config)# ***loopback-detection destination-address*** *1234.1234.1234* ***vlan*** *1*

[Related command]

command	description
show loopback-detection	Show the status of loopback-detection

3.84. loopback-detection down-time

[Introduction]

When the loop is detected on a switch, the relative port will be shutdown, and this time will decide the shutdown time.

loopback-detection down-time {<0-65534> | infinite**}**

[Parameter]

<0-65534> time when the state of loopback port is “down”, second as the unit, 0 stands for do not shutdown the port which has loop;

infinite stands for shutdown the relative port and will not recover automatically

[Default]

Infinite.

[Command Modes]

Physical Physical port configuration mode; privileged user(priority 15).

[Usage Guide]

only the user with priority 15 can use this command.

[Explanation of command execution echo]

Set unsuccessfully on port X!

Set successfully

[Example]

N/A

[Related command]

command	description
show loopback-detection	Show state of port loopback-detection

3.85. mac-access-list

[Introduction]

Set MAC access control list, use "**no**" command to delete.

[Command format]

mac-access-list <0-399> **(deny|permit) (ip|arp|rarp|any|**HHHH**)** (HHHH.HHHH.HHHH | **any**) (HHHH.HHHH.HHHH | **any**)

[Parameter]

0-399 The number of MAC access control list,range from 0 to 399

permit: permit access if conditions are matched.

deny deny access if conditions are matched

Protocol: protocol type in the frame head which is denoted by name or numerical value. The protocol type can be i**p, arp, rarp, any**, and the number value is from 0-0xFFFF. If the value is set to any or 0, it stands for all the protocols.

[Default]

N/A

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to define a MAC ACL, parameter permit | deny is used to set the switch whether to permit or deny the access of the packet. This command is only used to set the filter rule, generally speaking, and it should be applied to physical port or VLAN to be effective.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully!

[Example]

***mac-access-list** 10 **deny any** 1234.1234.1234 1111.2222.3344*

[Related command]

command	description
no mac-access-list ({0-399}**|all)**	Delete all MAC access control list
show mac-access-list [{0-399}]	Show one or all MAC access control list

3.86. mac-address-table aging-time

[Introduction]

Set aging time of MAC address,use “no”command to recover to default configuration.

mac-address-table aging-time {0 | time} [**schedule-list** list-no]

no mac-address-table aging-time [**schedule-list** list-no]

[Parameter]

aging-time aging time;
0 the mac address will not be aged;
time aging time, unit is second, range from 3-765;
schedule-list set the starting time, ending time, time interval of periodical task.
list-no range from <0-99>;

[Default]

Aging time is 300 second.

[Command Modes]

Global configuration mode, privileged user.

[Usage Guide]

Only users whose priority is 15 can use the command.

[Explanation of command execution echo]

SUCCESS!
This operation failed !

[Example]

Set aging time of MAC address is 500 second.
*Raisecom(config)# **mac-address-table aging-time** 500*
Set forbid MAC address to age
*Raisecom(config)# **mac-address-table aging-time** 0*
Resume default value of MAC address aging time.
*Raisecom(config)# **no mac-address-table aging-time***

[Related command]

Command	Description
show aging-time	Show aging time of MAC address

3.87. mac-address-table learning

[Introduction]

Enable and disable MAC address study function of physical port.

mac-address-table learning {**enable** | **disable**} **port-list** {**all** | port-number} [**schedule-list** list-no]

[Parameter]

enable enable study function
disable disable study function
port-list physical port list
all **all the physical ports**
port-number the number of port, range from 1 to 26; use comma to separate, ie: 1,85,23;
schedule-list set the starting time, ending time, time interval of periodical task
list-no range from <0-99>;

[Default]

By default, the study function of MAC address is enabled.

[Command Modes]

Global configuration mode, privileged user.

[Usage Guide]

Only users whose priority is 15 can use the command.

[Explanation of command execution echo]

Set successfully
Set port XX unsuccessfully!
The input port list is wrong!

[Example]

Disable MAC address study function of port 5,10
*Raisecom(config)#**mac-address-table learning disable port-list** 5,10*
Enable MAC address study function of port 5,10
*Raisecom(config)#**mac-address-table learning enable port-list** 5,10*

[Related command]

Command	Description
show interface port	Show one or all port state.

3.88. mac-address-table static unicast

[Introduction]

Set the static MAC address, no command to delete.

[**no**] **mac-address-table static unicast** HHHH.HHHH.HHHH **vlan** vlan_id **port** port-number [**schedule-list** list-no]

[Parameter]

static static address
HHHH.HHHH.HHHH MAC address, hexadecimal number, each four characters to be point separate;
vlan VLAN;
vlan_id VLAN ID, range from 1-4094;
port physical ports;
port-number physical port, range from 1-26;
schedule-list set the starting time, ending time and time interval of the dispatching task;
list-no range from <0-99>;

[Default]

No static MAC address.

[Command Modes]

Global configuration mode;

[Usage Guide]

N/A.

[Explanation of command execution echo]

Set successfully
VLAN X does not exist or not active!
Port X is not in vlan Y!
Join port X in a assigned group Y on assigned VLAN Z unsuccessfully!
Warning! This MAC address has already existed.

[Example]

set the static MAC address for port 3 which is associated with VLAN 1
*Raisecom(config)#**mac-address-table static unicast** 1234.abcd.0000 **vlan** 1* **port** 3
Delete delete the static MAC address for port 3 which is associated with VLAN 1;
*Raisecom(config)#**no mac-address-table static unicast** 1234.abcd.0000 **vlan** 1 **port** 3*

[Related command]

command	description
show mac-address-table static	Show the static address information for one or all(ports or VLAN)

3.89. mac-address-table static multicast

[Introduction]

Use this command to add a layer-2 ports as the multicast group member. Use **no** command to delete.

[no] mac-address-table static multicast mac-address **vlan** vlan_id **port** portlist [**schedule-list** list-no]

[Parameter]

mac-address set the MAC address for static multicast group, format as 0100.5eHH.HHHH;

vlan VLAN;

vlan_id VLAN ID, range from 1-4094;

port physical ports;

portlist set the number for the ports which is designated as the static router, range from 1-26;

schedule-list set the starting time, ending time and time interval of periodical task;

list-no range from <0-99>;

[Default]

N/A.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to add a two layer ports as the multicast group member. Use no command to delete the configuration.

[Explanation of command execution echo]

VLAN X does not exist or not active.
Port is not in vlan.
IGMP snooping on VLAN is disable!
Join port in a assigned group on assigned VLAN successfully
Join port in a assigned group on assigned VLAN unsuccessfully
Disable join port in a assigned group on assigned VLAN successfully
Disable join port in a assigned group on assigned VLAN unsuccessfully

[Example]

add the port 1-5 into group 0100.5e02.0203

*Raisecom(config)#**mac-address-table static multicast** 0100.5e02.0203 **vlan** 1 **port** 1-5*

delete the operation for adding the port 1-5 into multicast group 0100.5e02.0203

*Raisecom(config)#**no mac-address-table static multicast** 0100.5e02.0203 **vlan** 1 **port** 1-5*

[Related command]

Command	description
show mac-address-table static	Show one or all the static address information (ports or VLAN)

3.90. mac-address-table threshold

NOT AVAILABLE FOR: ISCOM3026/2826/2126/2026

[Introduction]

Configure the threshold for dynamic MAC address learning of ports. Use **no** command to delete the configuration.

[no] mac-address-table threshold <0-4095**>**

[Parameter]

threshold the threshold for dynamic MAC address learning of the ports.

0-4095 upper bond

[Default]

Do not set the threshold

[Command Modes]

Physical ports/range configuration mode; privileged user.

[Usage Guide]

Use this command to limit the MAC address number for each port.

[Explanation of command execution echo]

Set port X unsuccessfully
Set successfully

[Example]

Set the threshold for port 1 learning MAC address to 100

*Raisecom(config-port)#**mac-address-table threshold** 100*

Cancel the threshold for port 1 learning MAC address.

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

[Related command]

Command	Description
show interface mac-address-table threshold	Show the threshold of port learning MAC address.

3.91. match (CMAP)

[Introduction]

This command is used to define Traffic Classification.

[Command format]

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}

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 }

[Parameter]

ip-access-list acl-index—— specify the number of IP ACL.

mac-access-list acl-index— specify the number of MAC ACL.

access-list-map acl-index——specify user defined number of ACL.

ip dscp dscp-list——specify DSCP value for incoming packets, the range is from 0 to 63.

ip precedence ip-precedence-list——specify IP priority range from 0 to 7.

calss calss-map——specify a class map, this classmap can only be the type of match-all.

vlan vlanlist——specify vlan id, range from 1 to 4094.

[Default]

N/A.

[Command Modes]

CMAP configuration mode; Privileged user.

[Usage Guide]

match is used to define the traffic classification under the class-map configuration mode. Be attention that there maybe conflict among different matching types when classify incoming packets. When use previous defined ACL entries for classification, ACL type should be **permit**.

[Explanation of command execution echo]

Set the match statement for the class map successfully.

Set the match statement for the class map unsuccessfully.

The input parameter error.

The input name is too long.

[Example]

Raisecom(config)# ***ip-access-list 1 permit any any dscp 10***
Raisecom(config)# ***class-map*** *class1*
Raisecom(config-cmap)# ***match ip-access-list*** *1*
Raisecom(config-cmap)# ***no match ip-access-list*** *1*

[Related command]

command	description
show class-map [class-map-name**]**	Show class-map information

3.92. match (ACLMAP layer 2)

Define the layer-2 user define access list

[Command format]

match mac {destination|source} HHHH.HHHH.HHHH

match cos <0-7>

match ethertype HHHH [HHHH]

match {arp | eapol | flowcontrol | ip | ipv6 | loopback | mpls | mpls-mcast | pppoe | pppoedisc | x25 | x75}

no match mac {destination|source}

no match cos

no match ethertype

[Parameter]

mac——match layer 2 MAC address.

destination——match layer 2 MAC address.

source——match layer 2 MAC address.

HHHH.HHHH.HHHH——MAC address.

cos——match cos value

ethertype——match the protocol type of layer2
arp— match ARP
eapol——match eapol
flowcontrol——match flowcontrol
ip——match ip
ipv6——match ipv6
loopback——match loopback
mpls——match mpls unitcast protocol.
mpls-mcast——match mpls multicast protocol.
pppoe——match pppoe
pppoedisc——match pppoe discovery protocol
x25——match x25 protocol.
x75——match x75 protocal

[Default]

N/A

[Command Modes]

Access-list configuration mode; privileged user.

[Usage Guide]

Match is used to define the match conditions of user define access-list. With this command our users can define the layer-2 ACL entries flexibly, and all the first 64 bytes can be set as the match conditions.

[Explanation of command execution echo]

Conflict with previous matches.

[Example]

Raisecom(config)# ***access-list-map*** *101 deny*
Raisecom(config-aclmap)# ***match mac destination*** *000e.5e11.2344*
Raisecom(config-aclmap)# ***match cos*** *3*
Raisecom(config-aclmap)# ***match ethertype*** *0800 ff00*
Raisecom(config-aclmap)# ***match ipv6***
Raisecom(config-aclmap)# ***no match cos***

[Related command]

command	description
show access-list-map [acl-index **]**	Show access-list-map information

3.93. match arp

[Introduction]

Use to define arp data matching of map table for ACL.

[Command format]

match arp opcode {request | reply}
match arp sender-mac HHHH.HHHH.HHHH
match arp target-mac HHHH.HHHH.HHHH
match arp sender-ip A.B.C.D [A.B.C.D]
match arp target-ip A.B.C.D [A.B.C.D]

no match arp opcode
no match arp sender-mac
no match arp target-mac HHHH.HHHH.HHHH
no match arp sender-ip
no match arp target-ip

[Parameter]
opcode——match ARP packet type.
request——match arp request packet.
reply——match arp reply packet.
sender-mac——match mac address of ARP sender.
target-mac——match ARP target hardware address.
HHHH.HHHH.HHHH——MAC address.
sender-ip——match IP address of ARP sender.
target-ip——match ARP target IP address.
ethertype——match layer 2 protocol type
A.B.C.D [A.B.C.D]——IP 地址（掩码）
[Default]
N/A
[Command mode]
Access-list configuration mode; Privileged user.
[Usage Guide]
Under access-list-map configuration mode, **match** command is used to define arp protocol match conditions. Note: there may be conflict during matching different types.
[Explanation of command execution echo]
Conflict with previous matches.
[Example]
Raisecom(config)# ***access-list-map*** *101 deny*
Raisecom(config-aclmap)# ***match arp opcode request***
Raisecom(config-aclmap)# ***match sender-mac*** *000e.5e23.4553*
Raisecom(config-aclmap)# ***match sender-ip*** *10.0.0.0 255.0.0.0*
Raisecom(config-aclmap)# ***no match arp opcode***

[Related command]

command	description
show access-list-map [acl-index **]**	Show access-list-map information

3.94. match ip

[Introduction]
Use to define ip protocol data matching of map table for ACL.
[Command format]
match ip {destination-address | source-address} A.B.C.D [A.B.C.D]

match ip precedence {<0-7> **| routine| priority| immediate| flash| flash-override | critical | internet | network}**

match ip tos {<0-15> **| normal | min-monetary-cost | min-delay | max-reliability | max-throughput}**

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 no-fragments

match ip { ahp | esp | gre | icmp | igmp | igrp |ipinip | ospf | pcp | pim | tcp | udp}

match ip protocol <0-255>

no match ip {destination-address | source-address}

no match ip precedence

no match ip tos

no match ip dscp

no match ip no-fragments

no match ip protocol

[Parameter]

destination-address——match IP target address.

source-address——match IP source address.

precedence——match IP priority

<0-7>—— IP priority value

routine—— IP priority value is 0

priority—— IP priority value is 1

immediate——IP priority value is 2

flash—— IP priority value is 3

flash-override—— IP priority value is 4

critical—— IP priority value is 5

internet—— IP priority value is 6

network—— IP priority value is 7

tos——match IP TOS value

<0-15>——TOS value

normal——normal TOS value(0)

min-monetary-cost——minimum monetary cost TOS value (1)

min-delay——minimum delay TOS value（8）

max-reliability——maximum reliable TOS value（2）

max-throughput——maximum throughput rateTOS value（4）

dscp——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）
no-fragments——match no-fragments packet
protocol——match IP protocol type.
<0-255>——P protocol type value.
ahp——Authentication Header protocol
esp——encapsulation security protocol
gre——general router encapsulation protocol
icmp——Internet Control Message Protocol
igmp— Internet Group message protocol
igrp——Interior gateway protocol
ipinip——IP-in-IP tunnel
ospf——Open Shortest-Path First
pcp——IP Payload Compression protocol
pim——Protocol Independent Multicast protocol
tcp——Transmission Control Protocol
udp——User Datagram Protocol

[Default]
N/A
[Command format]
Access-list configuration mode; privileged user.
[Usage Guide]
Under access-list-map configuration mode, **match** command is used to define IP protocol match conditions. Note: there may be conflict during matching different types. ToS or IP precedence and dscp confliction.
[Explanation of command execution echo]
Conflict with previous matches.
[Example]
Raisecom(config)# ***access-list-map*** *101 deny*
Raisecom(config-aclmap)# ***match ip destination-address 10.1.23.4.5***
Raisecom(config-aclmap)# ***match ip precedence priority***

Raisecom(config-aclmap)# ***match ip tos normal***
Raisecom(config-aclmap)# ***match ip dscp 34***
Raisecom(config-aclmap)# ***match ip no-fragments***
Raisecom(config-aclmap)# ***match ip no-fragments***
Raisecom(config-aclmap)# ***match ip ospf***
Raisecom(config-aclmap)# ***no match ip protocol***

[Related command]

command	description
show access-list-map [acl-index **]**	Show access-list-map information

3.95. match ip tcp

[Introduction]

Define the tcp protocol match conditions for ACL.

[Explanation of command execution echo]

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 ip tcp {ack | fin | psh | rst | syn | urg }

no match ip tcp { destination-port | source-port}
no match ip tcp {ack | fin | psh | rst | syn | urg }

[Parameter]

destination-port——match ip tcp Destination Port
source-port——match ip tcp source port
<0-65535>——tcp port number
bgp——Border Gateway Protocol（179）
domain——Domain Name Service（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 service protocol(515)
nntp——Network News Transfer Protocol
pim-auto-rp——PIM Auto-RP (496)

pop2——Post Office Protocol Version 2(109)
pop3——Post Office Protocol Version 3 (110)
smtp——Simple Mail Transfer Protocol (25)
sunrpc——Remote Procedure Call protocol (111)
syslog——system log (514)
tacacs——TAC Acquisition and Control System (49)
talk——Talk (517)
telnet——Telnet (23)
time——Time (37)
uucp——Unix-to-Unix copy program (540)
whois——Nicname(43)
www——World Wide Web (HTTP, 80)
ack——match ACK
fin——match FIN
psh——match PSH
rst——match RST
syn——match SYN
urg——match URG

[Default]
N/A
[Command format]
Access-list configuration mode; privileged user.
[Usage Guide]
Under access-list-map configuration mode, **match** command is used to define TCP protocol match conditions.
[Explanation of command execution echo]
conflict with previous matchs.
[Example]
Raisecom(config)# ***access-list-map*** *101 deny*
Raisecom(config-aclmap)# ***match ip tcp destination-port smtp***
Raisecom(config-aclmap)# ***match ip tcp source-port 6201***
Raisecom(config-aclmap)# ***match ip tcp ack***
Raisecom(config-aclmap)# ***match ip tcp fin***
Raisecom(config-aclmap)# ***no match ip tcp destination-port***
Raisecom(config-aclmap)# ***no match ip tcp fin***
[Related]

command	description
show access-list-map [acl-index **]**	Show access-list-map information

3.96. match ip udp

[Introduction]
Use to define udp protocol match conditions.
[Command format]
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 }

no match ip udp { destination-port | source-port}

[Parameter]

destination-port——match ip udp destination port

source-port——match ip udp source 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 service protocol（53）

echo——echo protocol（7）

mobile-ip——mobile IP registration (434)

netbios-dgm——NetBios data message service（138）

netbios-ns——NetBios name service（137）

netbios-ss——NetBios session service（139）

ntp——Network Time Protocol (123)

pim-auto-rp——PIM Auto-RP (496)

rip——router information protocol(520)

snmp——Simple Network Management Protocol (161)

snmptrap——SNMP Traps (162)

sunrpc——Sun remote process control(111)

syslog——system log(514)

tacacs——TAC access control system (49)

talk——Talk (517)

tftp——Trivial File Transfer Protocol (69)

time——Time (37)

who——Who service (rwho, 513)

[Default]

N/A

[Command format]

Access-list configuration mode; privileged use exec.

[Usage Guide]

Under access-list-map configuration mode, **match** command is used to define UDP protocol match conditions.

[Explanation of command execution echo]

Conflict with previous matchs.

[Example]

Raisecom(config)# ***access-list-map*** *101 deny*
Raisecom(config-aclmap)# ***match ip udp destination-port tacacs***
Raisecom(config-aclmap)# ***match ip udp source-port 7306***

*Raisecom(config-aclmap)# **no match ip udp destination-port***

[Related command]

command	description
show access-list-map [acl-index **]**	Show access-list-map information
show access-list-map [acl-index **]**	Show access-list-map information

3.97. match ip icmp

[Introduction]

Define icmp protocol match conditions

[Command format]

match ip icmp <0-255> [<0-255>]

[Parameter]

<0-255> [<0-255>]——ICMP message type

[Default]

N/A

[Command format]

Access-list configuration mode; privileged user.

[Usage Guide]

Under access-list-map configuration mode, **match** command is used to define IP ICMP protocol match conditions.

[Explanation of command execution echo]

Conflict with previous matchs.

[Example]

*Raisecom(config)# **access-list-map** 101 deny*
*Raisecom(config-aclmap)# **match ip icmp** 2 2*
*Raisecom(config-aclmap)# **no match ip protocol***

[Related command]

command	description
show access-list-map [acl-index **]**	Show access-list-map inforamtion

3.98. match ip igmp

[Introduction]

Use to define the IP IGMP protocol match condition.

[Command format]

match ip igmp {<0-255> **| dvmrp | query | leave-v2 | report-v1 | report-v2 |report-v3 | pim-v1 }**

[Parameter]

<0-255>——IGMP message type

dvmrp——Distance Vector Multicast Routing Protocol

leave-v2——IGMPv2 leave group

pim-v1——protocol individual message version 1

query——IGMP member query

report-v1——IGMPv1 member report

report-v2——IGMPv2 member report

report-v3——IGMPv3 member report

[Default]

N/A

[Command Modes]

Access-list configuration mode;Privileged user.

[Usage Guide]

Under access-list-map configuration mode, **match** command is used to define IP IGMP protocol match conditions.

[Explanation of command execution echo]

conflict with previous matchs.

[Example]

*Raisecom(config)# **access-list-map** 101 deny*
*Raisecom(config-aclmap)# **match ip igmp query***
*Raisecom(config-aclmap)# **no match ip protocol***

[Related command]

command	description
show access-list-map [acl-index **]**	Show access-list-map information

3.99. match user-define

[Introduction]

Define the user defined match conditions.

[Command format]

match user-define RULE-STRING RULE-MASK <0-64>

no match user-define

[Parameter]

MATCH-STRING——match data, hex

RULE-MASK——mask of match data, used to filter match data from incoming packets.

<0-64>——Location of the matching data that offsets from header of L2 frame. For untag packets, please remember that switch will add 4 bytes (IEEE802.1Q tag) and set the offset of matching data carefully.

[Default]

N/A.

[Command format]

Access-list configuration mode;Privileged user.

[Usage Guide]

Access-list-map configuration mode, **match user-define** command is for users to define matching conditions by themselves. It is very flexible for user to define the ACL entries when the incoming packets are not in regular frame structure.

[Explanation of command execution echo]

Length of match data and mask is not equal!

The match data overrun the frame!

The match data is INVALID!

The mask data is INVALID!

[Example]

Raisecom(config)# ***access-list-map*** *101 deny*
Raisecom(config-aclmap)# ***match user-define a0 ff 24***
Raisecom(config-aclmap)# ***no match user-define***

[Related command]

Command	description
show access-list-map [acl-index **]**	Show access-list-map information

3.100. max-member

[Introduction]

Configure the maximum cluster member

max-member max-num

[Command format]

Cluster configuration mode; privileged user.

[Parameter]

max-num maximum cluster member.

[Default]

The amount of maximum supported cluster member is 128.

[Usage Guide]

User can use this command to configure the maximum cluster member.

[Explanation of command execution echo]

Set cluster max-member successfully
Set cluster max-member unsuccessfully

[Related command]

command	description
show cluster	Show cluster management information

3.101. member

[Introduction]

Add, active and delete cluster member.

[Command format]

member HHHH.HHHH.HHHH [**active** username password]

member HHHH.HHHH.HHHH **suspend**

no member {HHHH.HHHH.HHHH | **all**}

[Parameter]

active active this member

HHHH.HHHH.HHHH to active member which has this MAC address.

username username of the member to be active, the maximum length is 48 characters.

password password of active member to be active, the maximum length is 48 characters.

suspend to suspend this member.

all delete all the members.

[Default]

N/A

[Command Modes]

Cluster configuration mode; privileged user.

[Usage Guide]

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).

[Explanation of command execution echo]

This device is not a COMMANDER.
There is no this member.
Member add unsuccessfully.
Member add successfully.
This member has been acitved.
Add successfully, active successfully.
Add successfully, active unsuccessfully, this member is not operation up.
add successfully, active unsuccessfully, the switch be configed is a commander.
Add successfully, active unsuccessfully, the switch be configed is allready a member.
Add successfully, active unsuccessfully, usrname or password is wrong.
Add successfully, active unsuccessfully, timeout.
This member has not been actived.
Delete member unsuccessfully.
Delete successfully.

[Example]

Add the candidate 1111.1111.1111 to the cluster.

Raisecom(config-cluster)#member 1111.1111.1111

Add the candidate 1111.1111.1111 to the cluster and suspend the member.

Raisecom(config-cluster)#member 1111.1111.1111 active

Add and suspend the cluster member 1111.1111.1111

Raisecom(config-cluster)#member 1111.1111.1111 suspend

Delete cluster member 1111.1111.1111.

Raisecom(config-cluster)#no member 1111.1111.1111

Delete all the cluster member.

Raisecom(config-cluster)#no member all

[Related command]

command	description
show cluster member [HHHH.HHHH.HHHH]	Show cluster member information.

3.102. member auto-build

[Introduction]

Automatically active all the member switches.

Member auto-build [{**active** username password}| {**active** username password **all**}]

[Parameter]

active active cluster member

username username of the member that to be active, the maximum length is 48 characters.

password password of the member that to be active, the maximum length is 48 characters.

all automatically build and active all the candidates.

[Default]

N/A

[Command Modes]

Cluster configuration mode; privileged user.

[Usage Guide]

In order to make the operation of add and active conveniently, this command permit user using the same username and password for all the candidate adding and active, or to automatically active all the members which auto-acitve commander is pointed to current switch.

Using **member auto-build** command to automatically add and activate all the candidate members that auto-acitve commander is pointed to current switch.

Using **member auto-build active username password** command under the prompt command line, all the candidate members can be added and activated.

Using **member auto-build active username password all** command to automatically add and activate all the candidate members.

[Explanation of command execution echo]

this device is not a COMMANDER.
there is no such a candidate.
Apply the command **member auto-build active** username password or **member auto-build active** username password all on the commander switch, which does have candidate.
there is no candidate that can be auto-build
Apply the command **member auto-build** on the switch, which cannot be auto-build.
too many members have been added.
HHHH.HHHH.HHHH : add successfully, active successfully.
HHHH.HHHH.HHHH : add successfully, active unsuccessfully, this member is not operation up.
HHHH.HHHH.HHHH : add successfully, active unsuccessfully, the switch be configed is a commander.

HHHH.HHHH.HHHH : add successfully, active unsuccessfully, the switch be configed is allready a member.
HHHH.HHHH.HHHH : add successfully, active unsuccessfully, usrname or password is wrong.
HHHH.HHHH.HHHH : add successfully, active unsuccessfully, timeout.

[Example]

Add all the candidates into the cluster and active them.

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

Add all the candidates into the cluster seriatim and active them.

Raisecom(config-cluster)# member auto-build active raisecom raisecom

Automatically add the candidates which can be self-activated into the cluster and activate them.

Raisecom(config-cluster)# member auto-build

[Related command]

Command	description
show cluster member [HHHH.HHHH.HHHH]	Show cluster member information.

3.103. Mirror

[Introduction]

Enable/disable the mirror function

mirror {enable | disable} [**schedule-list** list-no]

[Parameter]

enable enable mirroring function
disable disable mirroring function
schedule-list set the starting time, ending time and time interval of dispatching task.
list-no schedule list number range from <0-99>;

[Default]

Disabled

[Command Modes]

Global configuration mode and privileged user (priority 15)

[Usage Guide]

Only users whose priority is 15 can perform the command.

[Explanation of command execution echo]

SUCCESS!
Command executed successfully.
This operation failed!
Command failed.

[Example]

Enable the mirroring function
*raisecom(config)# **mirror enable***
Disable the mirroring function
*raisecom(config)# **mirror disable***

[Related command]

Command	Description
show mirroring	Display the mirroring function status

3.104. mirror block-non-mirror

NOT AVAILABLE FOR: ISCOM2826/3026/2008/2026/2826E.

[Introduction]

Enable or disable block non-mirror flow control function.

mirror block-non-mirror {enable | disable}

[Parameter]

block-non-mirror block the traffic from non-mirror port to the monitor port.
enable active the function.
disable stop the function.

[Default]

Block-non-mirror port traffic function disable

[Command Modes]

Global configuration mode; privileged user (priority 15).

[Usage Guide]

Only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Success!
Set successfully
Failure!
Set unsuccessfully !

[Example]

Enable the mirror block-non-mirror function
Raisecom (config)# ***mirror block-non-mirror enable***
Disable the mirror block-non-mirror function
Raisecom (config)# ***mirror block-non-mirror disable***

[Related command]

Command	description
Show mirror	Show the settings of mirror function.

3.105. mirror divider

NOT AVAILABLE FOR: ISCOM2826/3026/2008/2026/2826E.

[Introduction]

Configure mirror divider; **no** command to delete the setting of mirror divider.

mirror { ingress | egress } divider <1-1023>

no mirror { ingress | egress } divider

[Parameter]

ingress ingress mirror divider;
egress egress mirror divider;
divider copy the reciprocal rate packet of the number of divider ,from source port to the monitor port
1—1023 number of mirror divider.

[Default]

The dividers for ingress mirror and egress divider are 1;

[Command Modes]

Global configuration mode; privileged user.（priority 15）.

[Usage Guide]

only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Success!
Set successfully
Failure!
Set unsuccessfully !

[Example]

Set the ingress divider to 30
Raisecom (config)# ***mirror ingress divider 30***

Set the egress divider to 50
Raisecom (config)# ***mirror egress divider 50***

Delete the mirror divider
(config)# ***no mirror ingress divider***
Raisecom (config)# ***no mirror egress divider***

[Related command]

command	description
show mirror	Show the setting of mirror function.

3.106. mirror filter

NOT AVAILABLE FOR: ISCOM2826/3026/2008/2026/2826E.

[Introduction]

Configure the rule of mirror filter. **no** command is used to recover to default setting.

mirror { ingress | egress } filter { destination | source } mac HHHH.HHHH.HHHH

no mirror { ingress | egress } filter

[Parameter]

ingress ingress mirror filtering rule;
egress egress mirror filtering rule;
destination target MAC address;
source source MAC address;
HHHH.HHHH.HHHH MAC address;

[Default]

All the packets on the mirror ports are mirrored

[Command Modes]

Global configuration mode; privileged user（priority 15）.

[Usage Guide]

Only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Success!
Set successfully
Failure!
Set unsuccessfully !

[Example]

Set the ingress mirror filter rule, only the packet with a MAC address equals to

0050.8D54.BE64 can be mirrored.

Raisecom (config)# ***mirror ingress filter source mac*** *0050.8D54.BE64*

Set the egress mirror filter rule, only the packet with a MAC address equals to 0050.8D54.BE64 can be mirrored.

Raisecom (config)# ***mirror egress filter destination mac*** *0050.8D54.BE64*

Recover the filter rule to the default setting.

Raisecom (config)# ***no mirror ingress filter***

Raisecom (config)# ***no mirror egress filter***

[Related command]

Command	Description
show mirror	Show the settings of mirror function.

3.107. mirror monitor-port

[[Introduction]

Set monitor port of mirror function, use “no” to delete.

mirror monitor-port port_number

no mirror monitor-port

[Parameter]

monitor_port monitor port

port_number the number of physical port, range from 1 to 26

[Default]

On default condition, not set monitor port.

[Command Modes]

Global configuration mode and privileged user

[Usage Guide]

Only privileged users whose priority is 15 can use the command.

[Explanation of command execution echo]

The port X has been set to be mirrored port , please reset!

This echo shows when setting a monitoring port that has been set to monitoring port before. Please set up after deletion of previous setup.

Set successfully !

[Example]

Set port 5 is monitor port of mirror function.

Raisecom(config)# ***mirror monitor_port*** *5*

Delete mirror port

Raisecom(config)# ***no mirror monitor***

[Related command]

Command	description
no mirror all	Delete all the mirror setting
show mirror	Show all the mirror setting

3.108. mirror source-port-list

[Introduction]

Set source port and mirror rule of mirror function, use “no” command to perform deletion.

mirror source-port-list both port-list

mirror source-port-list ingress port-list

mirror source-port-list egress port-list

mirror source-port-list ingress port-list **egress** port-list

no mirror source-port-list

no mirror all

[Parameter]

source-port-list source mirror port;
port_list the number of physical port, range from 1 to 26, use ",", "-" for multi port input;
ingress mirror ingress packets;
egress mirror egress packets;
both mirror both ingress and mirror egress packets;
all all the mirror configuration.

[Default]

Disabled.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

The port list is wrong!
Error occurred when enter multi ports using "-" and ",".
The port X has been set to be monitor port , please reset!
The port X is already a monitoring port.
Set successfully !

[[Example]

Set physical port of 1 to 5 is mirror port.
*Raisecom(config)# **mirror source_port** 1-5*
Delete mirror of port 2
*Raisecom(config)# **no mirror source_port** 2*
Delete all mirror setting
*Raisecom(config)# **no mirror all***

[Related command]

Command	description
show mirror	Show all the mirror information

3.109. mls qos

[Introduction]

Enable or disable QOS function.

[Command format]

[no] mls qos

[Parameter]

N/A

[Default]

QOS function is disabled.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to enable the QOS function globally. If some QOS settings have been enabled, then QOS can work immediately.

[Explanation of command execution echo]

Enable global QoS successfully.

Enable global QoS unsuccessfully.

[Example]

Raisecom(config)#mls qos
Raisecom(config)#no mls qos

[Related command]

command	description
show mls qos	Show QOS configuration information

3.110. mls qos {aggregate-policer |class-policer | single-policer }

NOT AVAILABLE FOR: RC2126/2016/2008/2026.

[Introduction]

Configure policer.

[Command format]

mls qos {aggregate-policer |class-policer | single-policer } policer-name rate burst **[exceed-action { drop | policed-dscp-transmit** dscp **}]**

no mls qos {aggregate-policer |class-policer | single-policer } policer-name

[Parameter]

aggregate-policer: all the class-map under this police-map will use the same policer (that is to say, all the class-maps share this policer).

class-policer: all the match conditions in the class-map share this policer.

single-policer: when there is more than one match conditions in one class-map, each match condition uses one policer.

policer-name——appoint the name for policer, the maximum length is 16 characters.

Rate: limited speed, unit is Kbps.

Burst: limited value of burst, unit is KB.

Drop: when the traffic exceeds the defined rate and burst, drop the packets.

policed-dscp-transmit: when the traffic exceed the defined rate and burst, change the dscp to a lower value.

dscp——when the traffic exceeds defined rate and burst, change dscp value to this value.

[Default]

N/A

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Create or delete policer. If do not specify **exceed-action**, the default operation is **drop**.

[Command execution]

Create the policer successfully.

Create the policer unsuccessfully.

Delete the policer successfully.

Delete the policer unsuccessfully.

The input name is too long.

The policer has not existed.

The policer has existed.

[Example]

Raisecom(config)# ***mls qos aggregate-policer*** *sss 400 60* ***exceed-action drop***
Raisecom(config)# ***mls qos aggregate-policer*** *sss 400 60* ***exceed-action policed-dscp-transmit*** *3*
Raisecom(config)# ***no mls qos aggregate-policer*** *aaa*

[Related command]

command	description
show mls qos { aggregate-policer |class-policer | single-policer } [policer-name]	Show policer information

3.111. mls qos default-cos

NOT AVAILABLE FOR: RC2016/2008/2826/2826E/3026.

[Introduction]

Configure default COS and QOVERRIDE of the port

[Command format]

mls qos default-cos { default-cos | **override }**

no mls qos default-cos [override]

[Parameter]

default-cos: specify default CoS value, if the port trust CoS value of ingress packets and packets are untag, use default CoS as the ingress packets' CoS value. The CoS value is from 0 to 7, default value is 0.

Override: the default-cos value of port will be effective no matter trust what conditions. Default-cos override function is disabled. For example, no matter the port trusts COS, DSCP or IP Precedence, all ingress port will use this default-cos; if the ingress packets are tagged, the default-cos will replace the original value.

[Default]

Default CoS value is 0, override is disabled.

[Command Modes]

Physical port/range configuration mode; privileged user.

[Usage Guide]

Set the default CoS value for the port and override function.

[Explanation of command execution echo]

Set the default cos value for the port successfully.

Set the default cos value for the port unsuccessfully.

Set cos override for the port successfully.

Set cos override for the port unsuccessfully.

[Example]

Raisecom(config)#interface port 1
Raisecom(config-port)#mls qos default-cos 3
Raisecom(config-port)#no mls qos default-cos
Raisecom(config-port)#mls qos default-cos override
Raisecom(config-port)#no mls qos default-cos override

[Related command]

Command	Description
show mls qos port portid	Show QOS config information.

3.112. mls qos default-dscp

NOT AVAILABLE FOR: RC2016/2008/2826E.

[Introduction]

Configure default DSCP and override.

[Command format]

mls qos default-dscp { default-dscp | **override }**

no mls qos default-dscp [override]

[Parameter]

default-dscp: specify the default dscp value for the port, if the port trusts DSCP value, and the ingress packets are untag, set the default dscp value for the data packet. Dscp value scales from 0 to 63; default value is 0.

Override: the default-dscp value of port will be effective no matter trust what conditions. Default- dscp override function is disabled. For example, no matter the port trusts COS, DSCP or IP Precedence, all ingress port will use this default-dscp; if the ingress packets are tagged, the default- dscp will replace the original DSCP value.

[Default]

Set the default dscp value to 0; override is disabled.

[Command format]

Physical port configuration mode; privileged user.

[Usage Guide]

Set the default DSCP value and override function for the ports.

[Explanation of command execution echo]

Set the default dscp value for the port successfully.
Set the default dscp value for the port unsuccessfully.
Set dscp override for the port successfully.
Set dscp override for the port unsuccessfully.

[Example]

Raisecom(config)#interface port 1
Raisecom(config-port)#mls qos default-dscp 3
Raisecom(config-port)#no mls qos default-dscp
Raisecom(config-port)#mls qos default-dscp override
Raisecom(config-port)#no mls qos default-dscp override

[Related command]

Command	description
show mls qos port portID	Show QOS config information.

3.113. mls qos dscp-mutation

NOT AVAILABLE FOR: RC2016/2008/2026/2126.

[Introduction]

Use DSCP MUTATION mapping table on the ports.

[Command format]

mls qos dscp-mutation dscp-name

no mls qos dscp-mutation dscp-name

[Parameter]

dscp-name——specify the name of dscp-mutation, maximum length of the name is 16 characters.

[Default]

Default dscp mutation name is default-dscp, mapping relationship is 0->0, 1->1,…, 63->63.

[Command Modes]

Use the port/range configuration mode; privileged user.

[Usage Guide]

If users need to realize QoS between two independent regions, you can set the edge port to trust DSCP, and the port will receive the packets and trust the DSCP value of ingress packets, and the classification will be avoided. If the DSCP value of two QOS regions indicate differently, DSCP-to-DCSP map is available for the mutation.

[Explanation of command execution echo]

Set the dscp mutation for the port successfully.

Set the dscp mutation for the port unsuccessfully.

The input name is too long.

[Example]

Raisecom(config-port)# ***mls qos dscp-mutation*** *aaa*
Raisecom(config-port)# ***no mls qos dscp-mutation*** *aaa*

[Related command]

Command	Description
show mls qos port portid	Show port dscp-mutation information

3.114. mls qos map cos-dscp

NOT AVAILABLE FOR: ISCOM2026/2126.

Configure CoS to dscp mapping table.

[Command format]

mls qos map cos-dscp dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8

no mls qos map cos-dscp

[Parameter]

dscpn——dscp value of CoSn mapping, range from 0 to 63.

[Default]

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

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

Configure the mapping from cos to dscp.

[Explanation of command execution echo]

Set the cos to dscp map successfully.

Set the cos to dscp map unsuccessfully.

[Example]

Raisecom(config)# ***mls qos map cos-dscp 10 15 20 25 30 35 40 45***
*Raisecom(config)#****no mls qos map cos-dscp***

[Related command]

Command	Description
show mls qos maps cos-dscp	Show cos-dscp mapping information.

3.115. mls qos map dscp-cos

NOT AVAILABLE FOR: ISCOM2026/2126.

[Introduction]

Configure the mapping from dscp to switch internal priority.

[Command format]

mls qos map dscp-cos dscp-list **to** cos

no mls qos map dscp-cos

[Parameter]

dscp-list——dscp value, range from 0 to 63, the format is:2,3,5-10

cos——switch internal priority, scales from 0 to 7.

[Default]

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

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

configure the mapping from dscp to switch internal priority.

[Explanation of command execution echo]

Set the cos to dscp map successfully.

Set the cos to dscp map unsuccessfully.

[Example]

Raisecom(config)# ***mls qos map dscp-cos 0,8,16,24,32,40,48,50 to 0***
*Raisecom(config)#****no mls qos map dscp-cos***

[Related command]

Command	Description
show mls qos maps	Show dscp-cos mapping information

dscp-cos	

3.116. mls qos map dscp-mutation

NOT AVAILABLE FOR: RC2008/2016/2026/2126.

[Introduction]

Configure DSCP MUTATION mapping table.

[Command format]

mls qos map dscp-mutation dscp-name dcp-list **to** dscp

no mls qos map dscp-mutation dscp-name

[Parameter description]

dscp-name: specify the name of dscp-mutation, the maximum length is 16 characters.

dscp-list: dscp list value, use',' or ' - ' to separate, Example 2,3,5-12. The maximum value is 63.

Dscp: dscp value, range from 0 to 63.

[Default]

The name of the default dscp mutation is default-dscp, mapping relationship is 0->0, 1->1, …, 63->63.

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

Create or delete dscp-mutation mapping. The default mapping can not be modified or erased.

[Explanation of command execution echo]

Set the dscp mutation successfully.

Set the dscp mutation unsuccessfully.

The input parameter is wrong.

The input name is too long.

[Example]

*Raisecom(config)# **mls qos map dscp-mutation** aaa 1-10 **to** 5*
*Raisecom(config)# **no mls qos map dscp-mutation** aaa*

[Related command]

Command	Description
show mls qos maps dscp-mutation	Show dscp-mutation information

3.117. mls qos map ip-prec-dscp

NOT AVAILABLE FOR: ISCOM2026/2126.

[Introduction]

Configure the mapping from TOS to dscp.

[Command format]

mls qos map ip-prec-dscp dscp1 dscp2 dscp3 dscp4 dscp5 dscp6 dscp7 dscp8

no mls qos map ip-prec-dscp

[Parameter]

dscpn——dscp value of TOS n mapping, range from 0 to 63.

[Default]

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

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Configure the mapping from IP priority to dscp.

[Explanation of command execution echo]

Set the ip precedence to dscp map unsuccessfully.

[Example]

Raisecom(config)# ***mls qos map ip-prec-dscp 10 15 20 25 30 35 40 45***
*Raisecom(config)#****no mls qos map ip-prec-dscp***

[Related command]

Command	Description
show mls qos maps ip-prec-dscp	Show mapping information for ip-prec-dscp

3.118. mls qos trust

Not available for: ISCOM2826/2826E/3026.

[Introduction]

Configure global trust state.

[Command format]

mls qos trust [**cos** | **dscp | ip-precedence**]

no mls qos trust [**cos** | **dscp | ip-precedence**]

[Parameter]

CoS: classify based on the CoS value of ingress packets. For UNTAG packets, use the default CoS value for the port, that is 0.

DSCP: classify based on the DSCP value of input packet. To non-IP packet, if the packet is tag, use the CoS value of the packet, if the packet is untag, use the default CoS value. Switch maps the CoS value to DSCP by CoS-to-CoS mapping table.

IP priority——classify based on the priority of incoming packet. To non-IP packet, if the packet is tag, use the CoS value of the packet, if the packet is untag, use the default CoS value for the packet. Switch maps the CoS value to DSCP through CoS-to-CoS mapping table.

[Default]

Default configuration is untrust; that is untrust state.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Used to set the CoS, IP priority or dscp of switch trust packets as the internal QoS priority.

[Explanation of command execution echo]

Set the trust state for the switch successfully.

Set the trust state for the switch unsuccessfully.

[Example]

Raisecom(config)#mls qos trust cos
Raisecom(config)#no mls qos cos

[Related command]

Command	description
show mls qos port	Show QOS configuration information.

3.119. mls qos trust

Not available for: ISCOM2008/2016/2026.

[Introduction]

Configure global trust state.

[Command format]

mls qos trust [**cos** | **dscp | ip-precedence**]

no mls qos trust [**cos** | **dscp | ip-precedence**]

[Parameter]

CoS: classify ingress packets based on the CoS value. For UNTAG packet, use the port default-CoS value, that is 0.

DSCP: classify ingress packets based on the DSCP value. For non-IP packet, if the packet is tag, use the CoS value of the packet, if the packet is untag, use the default CoS value. Switch maps the CoS value to DSCP by CoS-to-DSCP mapping table.

IP precedence——classify based on the priority of incoming packet. For non-IP packet, if the packet is tagged, use the CoS value of the packet, if the packet is untagged, use the default CoS value of the packet. Switch maps the CoS value to DSCP through CoS-to-CoS mapping table.

[Default]

Not trust

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to set the port to trust the CoS, IP precedence or DSCP.

[Explanation of command execution echo]

Set the trust state for the switch successfully.

Set the trust state for the switch unsuccessfully.

[Example]

Raisecom(config)#interface port 1
Raisecom(config-port)#mls qos trust cos
Raisecom(config-port)#no mls qos cos

[Related command]

Command	description
show mls qos port	Show QOS configuration information.

3.120. mvr { enable | disable }

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Use this global configuration command to enable/disable the multicast VLAN registration (MVR) feature on the switch.

.

[Command format]

mvr { **enable** | **disable** }

[Parameter]

N/A.

[Default]

MVR function disables.

[Command]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to start the MVR function of the switch globally. If there are some MVR relative configuration, then the functions become effective immediately after globally enable MVR.

[Explanation of command execution echo]

Enable MVR successfully

Enable MVR unsuccessfully

Disable MVR successfully

Disable MVR unsuccessfully

[Example]

Raisecom(config)#mvr enable
Raisecom(config)#mvr disable

[Related command]

command	Description
show mvr	Show MVR configuration information

3.121. mvr group

NOT AVAILABLE: ISCOM2026.

[Introduction]

(Optional) Statically configure an MVR group IP multicast address on the switch.

[Command format]

[no] mvr group ip -adress [count]

mvr group any

[Parameter]

ip-adress—— Statically configure an multicast group IP address, this address is used for switch to receive the multicast group data flow, should be class D IP address, format is A.B.C.D.

count——Configure multiple contiguous MVR group addresses.

range from1-256, default is 1.

Any——permit any multicast group.

[Default]

No IP multicast address is configured, that is to say, any multicast group is allowed.

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

The maximum multicast group number that switch permits is 256. All the multicast traffic with multicast address will be sent to receiver ports. Since the multicast

forwarding of ISCOM switch is based on MAC, so please do not configure IP address with the same name, Example, 244.1.1.1 and 255.1.1.1 is not allowed to be configured at the same time. In order to delete defined IP group address, use **no mvr group ip –adress [count]** command.

If the multicast group has been configured, only the group members within the multicast group can be added. If there is no multicast group IP address being been configured, any member can be added.

If the multicast group has been configured, after that the command **mvr group any** is applied, then the multicast group, which has been configured, will be deleted.

[Explanation of command execution echo]

Set MVR group address successfully
Set MVR group address unsuccessfully
MVR receive any group address successfully
MVR receive any group address unsuccessfully
Address aliases with the address configured
The MVR group address has existed
The MVR MAX groups has exceeded
Not an IP multicast group address
Delete MVR group address successfully
Delete MVR group address unsuccessfully

[Example]

configure 226.1.2.3 as the IP multicast address:
Raisecom(config)#mvr group 226.1.2.3
Configure consecutive IP multicast address, range from 226.1.2.3 to 226.1.2.12.
Raisecom(config)#mvr group 226.1.2.3 10
Delete previously configured address.
Raisecom(config)#no mvr group 226.1.2.3 10
Any group member can be added.
Raisecom(config)#mvr group any

[Related command]

Command	description
show mvr member [ip-address **]**	Show MVR multicast group address.

3.122. mvr vlan

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Configure multicast VLAN of MVR.

[Command format]

mvr vlan vlanid

no mvr vlan

[Parameter]

vlanid——specify the VLAN that needs to receive the multicast group data. Scale form 1 to 4094, default is VLAN 1.

[Default]

Default is VLAN 1.

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

Specify the VLAN that need receive multicast group data. All the source ports should belong to this VLAN. In order to recover default configuration, use **no mvr vlan command**. If both the multicast VLAN and the static multicast address have been configured on the ports, please delete the port configuration before modifying the multicast VLAN.

[Explanation of command execution echo]

Set the VLAN in which multicast data is received successfully

Set the VLAN in which multicast data is received unsuccessfully

Set the default VLAN in which multicast data is received successfully

Set the default VLAN in which multicast data is received unsuccessfully

[Example]

Set the multicast VLAN to 2:

Raisecom(config)#mvr vlan 2

Recover the default setting.

Raisecom(config)#no mvr vlan

[Related command]

Command	Description
show mvr	Show MVR configure information.

3.123. mvr mode

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Configure MVR operation mode.

[Command format]

mvr mode { dynamic | compatible }

[Parameter]

dynamic——the dynamic mode allows the source ports to be added to multicast group dynamically.

compatible——does not allow dynamic membership joins on source ports

[Default]

Default mode is **compatible**

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Under the **compatible** mode, group members can receive the multicast traffic only when there are some members adding to the group at the receiving port, and switch transfers the message of IGMP enrollment to the multicast router. When some member is leaving, the information for “leave” should also be transferred to the router. That is to say, source ports do not join the multicast group voluntarily.

Under the **dynamic** mode, source port join the multicast group voluntarily (that is using **mvr group** command to configure the multicast address), multicast traffic is

sent till the source ports. When there are some members adding to the group, multicast traffic is sent to the receiving port immediately. When some group member is leaving, switch will send the “leave” message at the receiving port. If there are no member messages received within the **querytime**, the multicast transferring entity will be deleted, multicast traffic will not be sent to the receiving port.

[Explanation of command execution echo]

Set MVR mode dynamic successfully

Set MVR mode compatible successfully

Set MVR mode dynamic unsuccessfully

Set MVR mode compatible unsuccessfully

[Example]

Set the MVR mode to dynamic mode.

Raisecom(config)#mvr mode dynamic

Set the MVR mode to compatible mode

Raisecom(config)#mvr mode compatible

[Related command]

Command	description
show mvr	Show MVR configuration information

3.124. mvr timeout

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Configure MVR time out

[Command format]

mvr timeout timeout

no mvr timeout

[Parameter]

timeout——maximum overtime for MVR multicast address, unit is second, range from 60 to 36000, default is 600 seconds.

[Default]

Default is 600 second.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

MVR timeout is the maximum waiting time for waiting the IGMP members report message on the receiving port. If doesn’t get the member report within this period, delete the multicast transfer entity of the port. In order to recover the default configuration, use **no mvr timeout** command.

[Explanation of command execution echo]

Set MVR timeout successfully

Set MVR timeout unsuccessfully

Set default MVR timeout successfully

Set default MVR timeout unsuccessfully

[Example]

Set the timeout to 180 seconds.

Raisecom(config)#mvr timeout 180

Recover to default setting.

Raisecom(config)#no mvr timeout

[Related command]

command	description
show mvr	Show MVR configure information.

3.125. mvr type

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Configure MVR port type.

[Command format]

mvr type { source | receiver }

no mvr type

[Parameter]

source——specify the port as the source port, which is the port connected to the multicast router.

receiver——specify the port as the receiving port.

[Default]

Default port type is non-MVR type, not the source port nor the receiving the port.

[Command Modes]

Physical port configuration mode; privileged user.

[Usage Guide]

The receiving port is subscriber, can only receive multicast data. The receiving port can belong to any VLAN but multicast VLAN.

The source port is the port connected to the multicast router, can send and receive multicast data. All the source port should belong to multicast VLAN.

If configure on the non-MVR port, operation will fail.

If want to recover the port type to non-MVR, use **no mvr type** command; Any previously defined MVR property will be erased.

[Explanation of command execution echo]

Set MVR port type as source port successfully

The source port is not in multicast VLAN, set unsuccessfully

Set MVR port type as source port unsuccessfully

Set MVR port type as receiver port successfully

The port has been in multicast VLAN, set unsuccessfully

Set MVR port type as receiver port unsuccessfully

[Example]

Set port 1 as receiving port:

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

*Raisecom(config-port)# **mvr type receiver***

Set port 1 as the source port:

*Raisecom(config-port)# **mvr type source***

Se the port 1 as the non-MVR port:

*Raisecom(config-port)# **no mvr type***

[Related command]

Command	Description
show mvr port [portid **]**	Show MVR port information

3.126. mvr immediate

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Start the immediate leave function on the port.

[Command format]

[no] mvr immediate

[Parameter]

N/A.

[Default]

All the immediate leave function is disabled.

[Command Modes]

Physical port configuration mode; privileged user.

[Usage Guide]

When the immediate leave function is configured, receiving port can leave the multicast group even faster, receiving port sends IGMP enquiry packet. If doesn't get member report after a while, the receiving port will be deleted from the multicast group.

If the immediate leave function is started, then the receiving port will be erased from multicast group as soon as the IGMP leave message is received. The immediate leave function is only fit for the situation that one receiving-equipment is connected.

[Explanation of command execution echo]

Enable the Immediate Leave feature of MVR on a port successfully

Enable the Immediate Leave feature of MVR on a port unsuccessfully

Disable the Immediate Leave feature of MVR on a port successfully

Disable the Immediate Leave feature of MVR on a port unsuccessfully

[Example]

Start the immediate leave function on port 1:

Raisecom(config)#interface port 1

Raisecom(config-port)# ***mvr type receiver***

Raisecom(config-port)# ***mvr immediate***

[Related command]

Command	Description
show mvr port [portid **]**	Show MVR port information

3.127. mvr vlan group

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Add some ports on designated VLAN as the static multicast member.

[Command format]

[no] mvr vlan vlanid **group** ip-address

no mvr vlan vlanid **group [**ip-address **]**

[Parameter]

vlanid——specify multicast VLAN ID, range from 1 to 4094.

ip-address——the type of class-map, apply AND operation between match. Default is match-all.

[Default]

N/A.

[Command Modes]

Physical port configuration mode; privileged user.

[Usage Guide]

Add ports on designated VLAN as the static multicast group member. This command can only be applied on the receiving port. Use can receive multicast data when the receiving port get this enroll information of the group. Multicast address should be the IP address configured by mvr group command. Use **no mvr vlan** vlandid **group** ip-address command, if want to delete all the static multicast member of the ports, use **no mvr vlan vlanid group** command.

[Explanation of command execution echo]

Specify MVR group IP multicast address for specified VLAN ID successfully

Specify MVR group IP multicast address for specified VLAN ID unsuccessfully

Delete MVR group IP multicast address for specified VLAN ID successfully

Delete MVR group IP multicast address for specified VLAN ID unsuccessfully

MVR group address isn't class D address.

Invalid multicast VLAN

The input name too long.

Non MVR group cannot be added

[Example]

Configure port 2, add it to multicast VLAN 3, multicast address is 234.5.6.7.

*Raisecom(config)#**mvr enable***
*Raisecom(config)#**mvr vlan 3***
*Raisecom(config)#**mvr group 234.5.6.1 10***
*Raisecom(config)#**interface port 2***
*Raisecom(config-port)#**mvr type reciver***
*Raisecom(config-port)#**mvr vlan 3 group 234.5.6.7***

Delete configuration:

*Raisecom(config-port)#**no mvr vlan 3 group 234.5.6.7***

[Related command]

Command	Description
show mvr port [portid **]**	Show MVR port information
show mvr port [portid **] member**	Show MVR port member information.

3.128. mvr

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Set the port as non-MVR port.

[Command format]

[no] mvr

[Parameter]

N/A.

[Default]

All the ports do not start MVR function.

[Command Modes]

Physical port configuration mode; privileged user.

[Usage Guide]

Use this command to start port MVR function, the static multicast of the port will be added to the group immediately. Use **no mvr** to stop port MVR function. the dynamically added multicast group of the port will be erased.

[Explanation of command execution echo]

Enable MVR on the port successfully

Disable MVR on the port successfully

Enable MVR on the port unsuccessfully

Disable MVR on the port unsuccessfully

[Example]

start MVR on port 2:

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

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

[Related command]

Command	Description
show mvr port [portid **]**	Show MVR port information
show mvr port [portid **] member**	Show the member information of MVR port.

3.129. name

[Introduction]

Configure the name of static VLAN.

name WORD

[Parameter]

The name shall be less than 15 characters

[Default]

On default condition, the name of system default VLAN(VLAN1) is “Default”, other name of static VLAN is character “VLAN” plus four bit VLAN ID, Example, the default name of VLAN1 is “VLAN0001”, VLAN 4094 default name is “VLAN4094”

[Command Modes]

Static VLAN configuration mode; privileged user.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Set the name of VLAN 3 to “HR”:

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

[Related command]

Command	description
name	Name static VLAN
state	State the active state of VLAN

show vlan	Show VLAN configuration information.

3.130. password

[Introduction]

Use password to change the login password for current user.

password

[Parameter]

N/A.

[Default]

The default user login password for Raisecom switch series equipments is "Raisecom"

[Command Modes]

Privileged EXEC, privileged user.

[Usage Guide]

Use this command can change login password of current login user.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully!

Password not same!

Radius user can't change password!

Password is too long (must less than 16 chars)

[Example]

*Raisecom#**password***
Please input password:xxxx
Please input again:xxxx

[Related command]

Command	description
user privilege	Set user popedom.

3.131. permit | deny

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Set action of IGMP profile as permit or deny.

[Command format]

{ permit | deny }

[Parameter]

Permit: allow the user to be added to the multicast group if IP address is within the profile

Deny: deny the user to be added to the multicast group if IP address is within the profile

[Default]

The default operation is deny.

[Command Modes]

Profile configuration mode; Privileged user.

[Usage Guide]

Set the operation of IGMP profile to permit or deny.

[Explanation of command execution echo]

Set the action to permit access to the IP multicast address successfully

Set the action to permit access to the IP multicast address unsuccessfully

Set the action to deny access to the IP multicast address successfully

Set the action to deny access to the IP multicast address unsuccessfully

Set the action to access to the IP multicast address unsuccessfully

[Example]

Set IGMP profile operation:

*Raisecom(config)#**ip igmp profile** 1*
*Raisecom(config-profile)#**permit***

[Related command]

Command	description
ip igmp profile profile-number	Create IGMP profile
show ip igmp profile	Show IGMP profile configuration information.

3.132. police

NOT AVAILABLE FOR :RC2008/2016/2026/2126.

[Introduction]

Configure action for traffic.

[Command format]

[no] police policer-name

[Parameter]

policer-name: specify the name of policer, maximum length is 16 characters.

[Default]

N/A.

[Command Modes]

PMAP-C configuration mode; privileged user.

[Usage Guide]

set the plastic action for the traffic.

[Explanation of command execution echo]

Apply the policer successfully.

Apply the policer unsuccessfully.

[Example]

*Raisecom(config-pmap-c)#**police** aaa*
*Raisecom(config-pmap-c)#**no police** aaa*

[Related command]

Command	Description
show policy-map [policy-map-name**]**	Show information policy-map

3.133. policy-map

NOT AVAILABLE FOR: RC2008/2016/2026/2126.

[Introduction]

Create or delete **policy-map**.

[Command format]

[no] policy-map policy-map-name

[Parameter]

Policy-map-name: specify the name of policy -map, maximum is 16 characters.

[Default]

N/A.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to create a policy-map and enter (config-pmap) configuration view. Use **set**, **trust** command to set the new priority for the traffic or set the new trust relationship under this view. One policy map can include several class map.

[Explanation of command execution echo]

Create the policy map successfully.

Create the policy map unsuccessfully.

Delete the policy map successfully.

Create the policy map unsuccessfully.

The input name is too long.

[Example]

*Raisecom(config)# **policy-map** aaa*
*Raisecom(config-pmap)#**exit***
*Raisecom(config)# **no policy-map** aaa*

[Related command]

Command	Description
show policy-map [policy-map-name]	Show policy-map information

3.134. queue bounded-delay

NOT AVAILABLE FOR: RC2008/2016/2026/2126/2826E.

[Introduction]

Set the queueing mode of the port as BOUNDDELAY mode, and set the bound and delay for the queue.

[Command format]

queue bounded-delay weight0 weight1 weight2 weight3 delaytime

[Parameter]

Weightn: bound for the queue n, range from 1-255.

Delaytime: delay time, unit is ms, range from 1-255.

[Default]

The default queueing mode is strict priority (SP).

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Set the queueing mode of port as BOUNDDELAY mode, and set the bound and delay for the queue.

[Explanation of command execution echo]

Set the scheduling mode of cos queue for bounded-delay successfully.

Set the scheduling mode of cos queue for bounded-delay unsuccessfully.

[Example]

Raisecom(config)# ***queue bounded-delay 1 2 3 5 60***

[Related command]

Command	Description
show mls qos queueing	show queue information

3.135. queue cos-map

NOT AVAILABLE FOR: RC2008/2016.

[Introduction]

Configure the mapping from switch internal priority to output queues.

[Command format]

queue cos-map queue-id cos-list

no queue cos-map

[Parameter]

queue-id——Switch queue ID, range from 1 to 4.

cos-list——cos value, range from 0 to 7, format is:2,3,5-7

[Default]

COS value	0-1	2-3	4-5	6-7
Queue ID	1	2	3	4

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Configure the mapping from switch internal priority to queue.

[Explanation of command execution echo]

Set cos priority to queue map successfully.

Set cos priority to queue map unsuccessfully.

[Example]

Raisecom(config)# ***queue cos-map 1 2-5***
*Raisecom(config)#****no queue cos-map***

[Related command]

Command	Description
show mls qos queueing	Show queue information

3.136. queue preemp-wrr

NOT AVAILABLE FOR: RC2008/2016/2026/2126.

[Introduction]

set the queueing mode of the port to PREEMP-WRR mode, that is SP+WRR mode, and also set the weight for each queue.

[Command format]

queue preemp-wrr weight1 weight2 weight3

[Parameter]

weightn——weight for the queue n, range from 1-255.

[Default]

Default queueing mode is strict priority（SP）.

[Command format]

Global configuration mode; privileged user.

[Usage Guide]

Set the queueing mode of the port to PREEMP-WRR mode that is SP+WRR MODE, and set the bound for the queue. At this time, queue 0 uses strict priority for queueing, and other queues are based on the WRR queueing mode.

[Explanation of command execution echo]

Set the weight of cos queue successfully.

Set the weight of cos queue unsuccessfully.

[Example]

Raisecom(config)# ***queue preemp-wrr 1 2 3***

[Related command]

Command	Description
show mls qos queueing	Show queue information.

3.137. queue strict-priority

NOT AVAILABLE FOR: RC2008/2016.

[Introduction]

Set the queueing mode of the port to strict priority mode.

[Command format]

queue strict-priority

[Parameter]

N/A.

[Default]

Default queueing mode is strict priority (SP).

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Set the queueing mode to strict priority.

[Explanation of command execution echo]

Set the strict priority mode successfully.

Set the strict priority mode unsuccessfully.

[Example]

Raisecom(config)# ***queue strict-priority***

[Related command]

Command	Description
show mls qos queueing	Show queue information

3.138. queue wrr-weight

NOT AVAILABLE FOR: RC2008/2016.

[Introduction]

Configure switch the queueing mode to WRR, and set the weight for the queue.

[Command format]

queue wrr-weight weight0 weight1 weight2 weight3

[Parameter]

weightn——bound for the queue n, range from 1-255.

[Default]

default dispatching mode is strict priority（SP）.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Configure switch queueing mode as WRR, and set the weight for each queue.

[Explanation of command execution echo]

Set the weight of cos queue successfully.

Set the weight of cos queue unsuccessfully.

[Example]

Raisecom(config)# ***queue wrr-weight 1 2 3 5***

[Related command]

Command	Description
show mls qos queueing	Show queue information

3.139. quit

[Introduction]

Use the command to exist from current mode to previous mode or logout.

quit

[Parameter]

N/A

[Command Modes]

User EXEC, Privileged EXEC, Global configuration mode, vlan configuration mode, physical port configuration mode, router protocol configuration mode; normal user, privileged user.

[Usage Guide]

Use the command to quit login state on priviledged EXEC and user EXEC.

Use the command to exist from current mode to previous mode.

[Explanation of command execution echo]

N/A

[Example]

*Raisecom>****quit***

[Related command]

Command	Description
exit	Quit from current mode to previous mode or quit login state.

3.140. radius

[Introduction]

Set the IP address of authentication server, no command to delete.

radius ipaddress

no radius

[Parameter]

ipaddress – host computer of RADIUS server, point separate decimal format.

[Default]

default situation: RADIUS UDP port is 1813.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A

[Explanation of command execution echo]

Invalid parameters.
Set radius server IP address unsuccessfully.
Set radius server IP address successfully.

[Example]

Set the IP address of RADIUS account server to 10.0.0.1
Raisecom(config)# radius 10.0.0.1

[Related command]

Command	Description
radius-key	Set the radius-key for RADIUS server.

3.141. radius-key

[Introduction]

The radius-key between RADIUS account servers. **no** command to delete.

radius-key string

no radius-key

[Parameter]

String a string within 16 characters.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

Set radius server key unsuccessfully.
Set radius server key successfully.

[Example]

Set the radius-key of the RADIUS server to “123”:
Raisecom# ***radius-key*** *123*

[Related command]

Command	Description
radius	Set the IP address of the certification server.

3.142. range

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Set the address range for IGMP profile.

[Command format]

[no] range start-ip [end-ip]

[Parameter]

start-ip——the starting address of the address range for IGMP profile.

end-ip——the ending address of the address range for IGMP profile.

[Default]

Default scale is all the multicast address.

[Command Modes]

profile configuration mode; privileged user.

[Usage Guide]

Set the address range for IGMP profile, if do not specify the ending address, it stands for an IP address. Use **no range start-ip [end-ip]** to delete the range.

[Explanation of command execution echo]

Set the range of IP multicast addresses successfully

Set the range of IP multicast addresses unsuccessfully

Delete the range of IP multicast address successfully

Delete the range of IP multicast address unsuccessfully

Not an IP multicast group address

Invalid group address

[Example]

Set the range of IGMP profile from 234.5.6.7 to 234.5.7.7:

*Raisecom(config)#**ip igmp profile** 1*
*Raisecom(config-profile)#**permit***
*Raisecom(config-profile)#**range 234.5.6.7 234.5.7.7***
Delete the range of IGMP profile from 234.5.7.0 to 234.5.7.7
*Raisecom(config-profile)#**no range 234.5.7.0 234.5.7.7***

[Related command]

Command	Description
ip igmp profile profile-number	Create IGMP profile
{ permit | deny}	Set IGMP profile action
show ip igmp profile	Show IGMP profile configuration information.

3.143. rate-limit port-list

[Introduction]

Set the rate limiting for physical port, **no** command used to delete.

rate-limit port-list port-list **ingress** rate **[**ingress-burst **]** [**schedule-list** list-no]

rate-limit port-list port-list **egress** rate **[**egress-burst **]** [**schedule-list** list-no]

no rate-limit port-list port-list **{**ingress | egress | both**}** [**schedule-list** list-no]

[Parameter]

port-list physical port number, range from 1-26, can use "," and "-" to set multiple ports;
ingress the "in" direction for physical port;
egress the "out" direction for physical port;
rate set the speed, unit is kbps, range from 1 to 1048576;
burst peak value speed, unit is KBps, range from1 to 512.
schedule-list set the starting time, ending time and time interval;

list-no range of the dispatching list table is <0-99>;

[Default]

No rate limiting for the physical port.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

The rate value with a power (integer) up near to 2

[Explanation of command execution echo]

Set successfully
Set unsuccessfully!

[Example]

Set the uplink speed for port 5 to 5Mbps, peak value is 32KBps; downlink speed is 10Mbps, peak value is 64Kbps.
Raisecom(config)# **rate-limit port-list** 5 **ingress** 5120 32
*Raisecom(config)# **rate-limit port-list** 5 **egress** 10240 64*
Delete the bandwidth limitation for port 5.
*Raisecom(config)# **no rate-limit port-list** 5 **both***

[Related command]

Command	Description
show rate-limit port-list [port_number]	Show bandwidth limitation information for particular or all the ports

3.144. rcommand

[Introduction]

Under cluster mode, enter cluster member remotely from commander switch.

rcommand { [hostname] [HHHH.HHHH.HHHH] }

[Parameter]

hostname the cluster member's name
HHHH.HHHH.HHHH the MAC address for cluster member who want to login.

[Command Modes]

Cluster configuration mode; privileged user (priority 15).

[Usage Guide]

Only the privileged user with priority 15 can use this command.

This command can only be applied on the switch which enable cluster function.

[Explanation of command execution echo]

Connect unsuccessfully!
Connection to host lost
Failed! This device is NOT a commander!
Failed! This hostname is NOT in the cluster!
Failed! This mac address is NOT in the cluster!

AAAA.BBBB.CCCC
DDDD.EEEE.FFFF
If several device use the same name, please input the MAC address of the device!
MAC address which match this hostname in the cluster::

AAAA.BBBB.CCCC
DDDD.EEEE.FFFF
If a name used by several cluster member, system shows following information.

Duplicate hostname in the cluster, please input the mac address of the device

[Example]

Login the cluster member with a MAC address AAAA.BBBB.CCCC

*raisecom(config-cluster)# **rcommand** AAAA.BBBB.CCCC*

login the cluster member “swA”

*raisecom(config-cluster)# **rcommand** swA*

3.145. reboot

[Introduction]

Use “reboot” to restore switch.

reboot

[Parameter]

N/A

[Command Modes]

Privileged EXEC; privileged user

[Usage Guide]

’Yes’ should be entered to identify the operation when the command is used to reboot switch.

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#**reboot***
Please input 'yes' to confirm:yes
Rebooting ...

[Related command]

N/A

3.146. relay

[Introduction]

Start the function for forwarding layer-2 message transparently. Use **no** command to deny the function.

relay {bpdu | dot1x | lacp | garp | gmrp | gvrp | all} **port-list** port-list [**schedule-list** list-no]

no relay {bpdu | dot1x | lacp | garp | gmrp | gvrp | all} **port-list** [{1-26}] [**schedule-list** list-no]

[Parameter]

message type bpdu | dot1x | lacp | garp | gmrp | gvrp;
port-list physical port;
port-list physical list, range is 1-26, use “,” and “-“ for multiple port input;
all all the two layer message;
schedule-list set the starting time, ending time and time interval for dispatching;
list-no dispatching list range is <0-99>;

[Default]

Disable.

[Command Modes]

Global configuration mode, privileged user (priority 15).

[Usage Guide]

Only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Failed to set forwarding ports

Set forwarding ports successfully.

[Example]

Start the transparent transmission for EAPOL message at port 3:

Raisecom (config)# ***relay dot1x port-list*** *3*

Deny transparent transmission for EAPOL message;

Raisecom (config)# ***no relay dot1x port-list*** *3*

[Related command]

command	Description
show relay port-list	Show current configuration information.

3.147. rmon alarm

[Introduction]

Use and add rmon alarm entries, use **no** format to delete.

rmon alarm <1-512> MIBVAR [**interval** <1-3600>] {**delta | absolute**} **rising-threshold** <1-65535>$_1$ [<1-65535>$_2$] **falling-threshold** <1-65535>$_3$ [<1-65535>$_4$] [**owner** STRING]

no rmon alarm <1-512>

[Parameter]

<1-512> Index number

MIBVAR the MIB variable which should be remotely monitored

Interval check the MIB variable time period

<1-3600> the time period for checking MIB variable (unit is second).

delta check between the change for MIB variables.

absolute check the absolute value for MIB

rising-threshold upper bound value for MIB variable

<1-65535>1 upper bound value for MIB variable

<1-65535>2 rising-threshold associated index.

falling-threshold lower bound value for MIB variable.

<1-65535>3 lower bound value for MIB variable.

<1-65535>4 falling-threshold associated MIB variable.

owner Alarm table associated owner.

STRING owner characters.

[Default]

Default polling time period is 2s.

Default owner is config.

[Command Modes]

Global configuration mode.

[Usage Guide]

MIBVAR should be decimal dotted; this command should be efficient MIB variable and can be monitored, otherwise the MIB variable can not be monitored. Use **no rmon alarm <1-512>** command to delete associated Alarm.

[Explanation of command execution echo]

Wrong Mib variable format!

Wrong MIB variable !

Owner name is too long!

Set successfully.

Set unsuccessfully.

[Example]

Set warning 10, use it to monitor MIB variable 1.3.6.1.2.1.2.2.1.20.1, every 20 seconds, check the value whether it is rising or falling. If rise 15, Example 10000 to 10015, spring alarm.

*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** 1 **owner** jjohnson*

[Related command]

Command	Description
show rmon alarm	Show rmon alarm table.

3.148. rmon event

[Introduction]

rmon event <1-65535> **[log] [trap** COMMUNITY **] [description** STRING **] [owner** STRING]

no rmon event <1-65535>

[Parameter]

<1-65535> index of RMON Event table

log	whether to log when it is triggered.
trap	send the community name of trap.
COMMUNITY	community name.
description	description string.
STRING	character string.
owner	owner
STRING	string of owner

[Default]

The default community name is public.

The default description string is null.

The default owner is config.

[Command Modes]

Global configuration mode; privileged user

[Usage Guide]

Use the command to add and set the attribute of event

[Explanation of command execution echo]

Community name is too long!

The community property string is too long.

Description is too long!

The description property string is too long

Owner name is too long!

The owner's name string is too long.

set successfully.

Command successful

set fail.

Command fails

[Example]

*Raisecom(config)#**rmon event** 1 **trap** private*

[Related command]

Command	Description
Show rmon event	show RMON EVENT table.

3.149. rmon history

[Introduction]

Start the history statistical group function for some port; no format command is used to stop the function.

rmon history (**ip** {0-14} | **port** {1-26}) [**shortinterval** <1-600>] [**longinterval** <600-3600>] [**buckets** <10-1000>] [**owner** STRING]

no rmon history (**ip** {0-14} | **port** {**1-26**})

[Parameter]

ip layer 3 port

0-14 layer 3 port from 0-14

port physical port

1-26 physical port, range is 1-26.

shortinterval short polling interval time.

1-600 the short polling interval, range is 1-600, unit is second.

longinterval long polling interval time.

600-3600 long time polling interval, range is 600-3600, unit is second.

buckets history group data storage queue.

10-1000 the range for history group data storage queue is 10-1000.

owner owner

STRING string of owner.

[Default]

Default short sampling time period is 30s.

Default long sampling time period is 1800s

Default value for history group data storage queue is 10.

Default owner value is monitorHistory.

[Command Modes]

Global configuration mode.

[Usage Guide]

N/A

[Explanation of command execution echo]

Owner name is too long!

Set successfully.

Set unsuccessfully.

[Example]

*Raisecom(config)#**rmon history ip** 1-9 **shortinterval** 60 **buckets** 50 **owner** raisecom*

*Raisecom(config)#**rmon history port** 1-5,10-18,25 **shortinterval** 60 **longinterval** 500 **buckets** 50 **owner** test*

[Related command]

Command	Description
show rmon history	Show the configuration result and information of history statistical group.

3.150. rmon statistic

[Introduction]

Start the statistical group function for particular port, **no** format command is used to stop the function.

rmon statistics (**ip** {0-14} | **port** {1-26}) [**owner** STRING]

no rmon statistics (**ip** {0-14} | **port** {1-26})

【Parameters】

ip layer 3 port

0-14 layer 3 port from 0-14

port physical port

1-26 physical port, range is 1-26.

owner owner

STRING string of owner.

[Default]

Owner default value is monitorStatitistics.

[Command Modes]

Global configuration mode.

[Usage Guide]

N/A

[Expla*nation of command execution echo]*

Owner name is too long !

Set successfully.

Set unsuccessfully.

[Example]

*Raisecom(config)#**rmon statistics ip** 1-9 **owner** raisecom*

*Raisecom(config)#**rmon statistics port** 1-5,10-18,25 **owner** test*

[Related command]

Command	description
show rmon statistics	Show configuration result and information of statistical group.

3.151. rndp

[Introduction]

Enable and disable RNDP（Raisecom Neighbor Discovery Protocol）.

rndp {**enable** | **disable**}

[Parameter]

enable RNDP;

disable RNDP;

[Default]

Enabled on all the ports.

[Command Modes]

Global configuration mode or physical configuration mode; privileged user.

[Usage Guide]

RNDP is used to discover the directly connected switch within a LAN, obtain and record device information. RNDP is the foundation for RTDP (Raisecom Topology Discovery Protocol). Generally speaking, they are used together. Only if the device is discovered by RNDP, the device can be discovered and its parameters can be collected by RTDP. User can disable RNDP to deny other devices within the LAN to discover it; RNDP also can be disabled on particular port.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Deny RNDP globally.

Raisecom(config)#rndp disable

Enable RNDP globally

Raisecom(config)#rndp enable

Deny RNDP under physical Physical port configuration mode.

Raisecom(config-port)#rndp disable

[Related command]

Command	Description
show rndp	Show RNDP configuration information
show rndp neighbor	Show RNDP neighboring information.

3.152. rtdp

[Introduction]

Enable and disable RTDP（Raisecom Topology Discovery Protocol）function.

rtdp {**enable** | **disable**}

[Parameter]

enable enable RTDP collection function.

disable disable RTDP collection function.

[Default]

switch RTDP function disable.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

RTDP is used to collect all switches' information, which support the RTDP and RNDP function is started. When **rtdp enable** command is applied to start RTDP collection function, RTDP will collect information of all the switches within specified collection scale (use **rtdp max-hop command** to set). Generally speaking, RTDP and RCMP (Raisecom Cluster Management Protocol) are used together. In cluster management, when the user wants to enable the cluster management function of cluster member device within the protocol, user should start RTDP to find out this device and get basic information for the device.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Deny RTDP collection globally.
Raisecom(config)#rtdp disable
Enable RTDP collection globally
Raisecom(config)#rtdp enable

[Related command]

Command	Description
rtdp max-hop	Set RTDP the maximum collection scale
show rtdp	Show RTDP config information
show rtdp device-list [HHHH.HHHH.HHH | hostname] [**detailed**]	Show RTDP device list information.

3.153. rtdp max-hop

[Introduction]

The maximum hop of RTDP（Raisecom Topology Discovery Protocol）

rtdp max-hop <1-16>

no rtdp max-hop

[Introduction]

<1-16> the maximum collection scale parameter (hop); first hop starts from directly connected device.
no command used to recover default setting.

[Default]

The maximum hop of RTDP is 16 hops

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to limit the range of RTDP collection.

[Explanation of command execution echo]

Set successfully.
Set unsuccessfully.

[Example]

set the max-hop of FTDP to 2 hops.
Raisecom(config)# ***rtdp max-hop*** *2*
Recovery the max-hop of RTDP to 16 hops.
Raisecom(config)# ***no rtdp max-hop***

[Related command]

Command	description
rtdp max-hop	Set the max-hop of RTDP
show rtdp	Show RTDP config information
show rtdp device-list [HHHH.HHHH.HHH | hostname] [**detailed**]	Show RTDP found device list information.

3.154. schedule-list

[Introduction]

Add or modify schedule-list, this command used to set the starting time, ending time and periodical execution interval.

no command to delete a queue.

schedule-list list-no **start** { **up-time** days time [**every** days time [**stop** days time]] | **date-time** date time [**every** { **day** | **week** | days time } [**stop** date time]]}

no schedule-list list-no

[Parameter]

list-no dispatching list range is <0-99>;

up-time Relative time after startup.

date-time Absolute time after startup.

days time a time period, the format is: days: <0-65535>, time: HH:MM:SS Example 3 3:2:1

date time a time point, input format is: MMM-DD-YYYY HH:MM:SS Example jan-1-2003 or 1-1-2003, the range of YYYY is 1970 to 2199.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

N/A

[Explanation of command execution echo]

Set successfully.

input Date & Time should be MMM-DD-YYYY(1900-2199), HH:MM:SS format

[Example]

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

[Related command]

Command	description
Show schedule-list	Show schedule-list information
Comd-str schedule-list list-no	Execute the command base on the way of dispatching.

3.155. search mac-address

[Introduction]

Search the state of mac-address in the switch.

search mac-address *HHHH.HHHH.HHHH*

[Parameter]

mac-address MAC address

HHHH.HHHH.HHHH MAC address, the format of input is dotted heximal notation string, dotted every four characters.

[Default]

Don’t search in default.

[Command Modes]

Global configuration mode.

[Usage Guide]

N/A

[Explanation of command execution echo]

if the mac address is finded out, show following information:

MAC address Port number VLAN identifier Layer 2 flags

[Example]

Search mac address 1234.1234.1234

*Raisecom#**search mac-address** 1234.1234.1234*

[Related command]

Command	Description
show mac-address-table l2-address	Show the MAC address which matching particular condition or all the MAC address information.

3.156. service-policy

[Introduction]

Apply policy on the port.

[Command format]

service-policy policy-map-name **ingress** portid **[egress** portlist]

no service-policy policy-map-name **ingress** portid

[Parameter]

policy-map-name——specify the name of policy, the maximum length is 16 characters.

Portid——ingress port ID

Portlist——egress port ID

[Default]

N/A.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Apply the policy on the port. The setting is mutually exclusive with the trust on the port. If QoS still not been started, setting doesn't work.

[Explanation of command execution echo]

Apply the policy successfully.

Apply the policy unsuccessfully.

The policy has attached on the port.

[Example]

*Raisecom(config)# **service-policy aaa ingress 1 egress 2-4***

*Raisecom(config)#**no service-policy aaa ingress 1***

[Related command]

Command	description
show mls qos port [portid]	Show port information.

3.157. set

[Introduction]

Configure the action of the traffic.

[Command format]

set {**ip dscp** new-dscp | **ip precedence** new-precedence | **cos** new-cos }

no set {**ip dscp** | **ip precedence** | **cos** }

[Parameter]

cos——modify the ingress packet cos value to a new value, and then classify the packets based on the new cos value.

dscp——first, change the ingress packet dscp value to a new value, then classify the packets based on the new dscp value.

precedence——first change the ingress packet precedence value to a new value, and then classify the packets based on the new value.

[Default]

N/A

[Command Modes]

PMAP-C configuration mode; privileged user.

[Usage Guide]

Users can set the action for the traffic and specify the new QOS value. Set command and the trust (port mode and policy-map mode) command are mutually exclusive; it depends on which command is executed later.

[Explanation of command execution echo]

Set the dscp for the class map successfully.

Set the dscp for the class map unsuccessfully.

[Example]

*Raisecom(config-pmap-c)#**set cos 3***

Raisecom(config-pmap-c)#**no set cos**

[Related command]

Command	Description
show policy-map [policy-map-name**]**	Show policy-map information

3.158. show access-list

[Introduction]

This command is used to show the ACL information.

[Command format]

show (ip-access-list|mac-access-list) [{0-399}]

[Parameter]

ip-access-list|mac-access-list:The ACL type used by filtering rule.

{0-399}:Serial number of ACL, if the parameter is ignored, then that is the all the defined ACL.

[Default]

N/A.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

This command is used to show the ACL information.

[Explanation of command execution echo]

Show the type of ACL, time for which is cited by the filtering rule, actual number of matching rule and other parameters.

[Example]

Show ip-access-list

Show mac-access-list 0-5

[Related command]

Command	Description
access-list	Relevant ACL
no access-list	Delete relevant ACL table.

3.159. show access-list-map

[Introduction]

This command is used to show ACL map table configured content for relevant type.

[Command format]

Show access-list-map [0-399]

[Parameter]

access-list-map:ACL map table

{0-399}:Serial number of ACL, if the parameter is ignored, then that is the all the defined ACL.

[Default]

N/A

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

This command is used to show the configured content of ACL.

[Explanation of command execution echo]

Show the actual matching rule of ACL map.

[Usage Guide]

show access-list-map 10

[Related command]

Command	Description

access-list-map	Define related ACL map table.
no access-list-map	Delete related ACL map table.

3.160. show arp

[Introduction]

Show the item of ARP mapping table

[Command Format]

show arp

[Parameter]

N/A

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user

[Usage Guide]

Use show arp to search all the item in arp address list, every item includes IP address, MAC address and the type information.

[Explanation of command execution echo]

current arp table aging-time is 6000 seconds(default:1200s)

show ARP table:

IP Address	*MAC Address*	*Type*
10.0.0.5	*0050.8d4b.fd1e*	*static*
10.0.0.6	*0050.0a3c.ac2e*	*dynamic*
10.0.0.7	*0050.1c4e.15a7*	*dynamic*

[Example]

show ARP table:

*Raisecom#show **arp***

[Related command]

Command	Description
arp	Add a static MAC address table
clear arp	Clean up all the items in ARP address mapping table

3.161. show buffer

[Introduction]

show the buffer information of the port.

show buffer [port <1-26>**]**

[Parameter]

port <1-26> specify the port number (optical);

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

If the port number is not specified, show all the port driver pool information.

[Explanation of command execution echo]

N/A

[Example]

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

Port 2

Total mBlks: 500 Free mBlks: 500 DATA: 0

HEADER: 0 SOCKET: 0 PCB: 0

RTABLE: 0 HTABLE: 0 ATABLE: 0

SONAME: 0 ZOMBIE: 0 SOOPTS: 0

FTABLE: 0 RIGHTS: 0 IFADDR: 0

CONTROL: 0 OOBDATA: 0 IPMOPTS: 0

IPMADDR: 0 IFMADDR: 0 MRTABLE: 0

[Related command]

N/A.

3.162. show class-map

NOT AVAILABLE FOR: RC2008/2016/2026/2126.

[Introduction]

Show class-map information.

[Command format]

show class-map [class-map-name]

[Parameter]

class-map-name——specify the name of class-map, the maximum length is 16 characters.

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

show class-map information.

[Explanation of command execution echo]

Raisecom#show class-map

Class Map match-any aaa (id 0)

Description:aaaaaaaaaaaaaaaaaa

Match N/A

[Example]

Raisecom# **show class-map**

[Related command]

Command		Description
class-map	class-map-name	Create class map

[**match-all** | **match-any**]	
description WORD	Set class map description information
match	Set match announcement

3.163. show clock

[Introduction]

Use show clock to show current system time.

show clock

[Command format]

show clock [summer-time-recurring]

[Parameter]

summer-time-recurring show summer time

[Command Modes]

Privileged EXEC, privileged user

[Usage Guide]

Use the command to show current system time.

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#**show clock***
Current system time: Sep-30-2003 00:28:07
Timezone offset: +08:00:00

*Raisecom#**show clock summer-time-recurring***
Current system time: Jan-01-2004 08:39:13
Timezone offset: +08:00:00
Summer time recuuring: Disable

*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

[Related command]

Command	Description
clock summer-time recurring	Set the starting time and ending time of summer time.
clock summer-time	Summer time enable.
clock timezone	Set the time zone of current time.
clock set	Set the current system time of system

3.164. show cluster

[Introduction]

Show cluster related information

show cluster

[Command format]

Privileged EXEC; privileged user.

[Usage Guide]

user can use this command to check cluster related information.

[Explanation of command execution echo]

The execution echo on the switch.

Raisecom#show cluster
cluster information:
identity:COMMANDER
current member num:4
max member num:128

The execution echo on the candidate.

Raisecom#show cluster
cluster information:
identity: CANDIDATE
autoactive: OFF
autoactive commander's mac: 0000.0000.0000

The execution echo on the member.

Raisecom#show cluster
cluster information:
identity:MEMBER
autoactive:ON
autoactive commander's mac:000e.5e23.34e2
commander's mac:000e.5e23.34e2

[Related command]

Command	Description
[**no**] **cluster**	Enable or disable the cluster function
member HHH.HHHH.HHHH [**active** username password] **member** HHH.HHHH.HHHH **suspend** **no member** {HHHH.HHHH.HHHH | **all**}	The "add", "active" and "delete" operation of the cluster members.
auto-build [{**active** username password}| {**active** username password **all**}]	The automatically add, active for all the candidates.
max-member	Configure the maximum member of supported cluster member.

3.165. show cluster candidate

[Introduction]

Show all the information about cluster candidate

show cluster candidate

[Command Modes]

Privileged user; privileged user.

[Usage Guide]

User can use this command to check all the information about cluster candidate.

[Explanation of command execution echo]

```
Raisecom#show cluster c
Cluster candidate list:
MAC Address       RcvdPort   Hop     HostName
-----------------------------------------
000e.5e00.c2c2    2          2       swD
```

[Related command]

Command	Description
[**no**] **cluster**	Enable or disable the cluster management function.
member HHH.HHHH.HHHH [**active** username password] **member** HHH.HHHH.HHHH **suspend** **no member** {HHHH.HHHH.HHHH | **all**}	The “add”, “active” and “delete” operation for cluster member.
auto-build [{**active** username password}| {**active** username password **all**}]	The automatically add, active and delete for all the cluster candidates.

3.166. show cluster member

[Introduction]

Show particular or all the information about cluster member.

show cluster member [HHHH.HHHH.HHHH]

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

User can use this command to check particular or all the information of cluster member.

[Explanation of command execution echo]

```
Raisecom#show cluster m
cluster member list:
Mac Address       OperationState   ActiveState   HostName
-----------------------------------------------------
000e.5e00.c2c5    UP               SUSPEND       swE
000e.5e00.c2c2    UP               SUSPEND       swD
000e.5e00.c2c8    UP               ACTIVE        swC
```

[Related command]

Command	Description

[**no**] **cluster**	Enable or disable the cluster management function.
member HHH.HHHH.HHHH [**active** username password] **member** HHH.HHHH.HHHH **suspend** **no member** {HHHH.HHHH.HHHH | **all**}	The “add”, “active” and “delete” operation for cluster members.
auto-build [{**active** username password}| {**active** username password **all**}]	Automatically add, active and delete operation for all the candidates.

3.167. show dhcp-relay

NOT AVAILABLE FOR: ISCOM2826/2126/2016/2008/2026/2826E

[Introduction]

Show the configuration and statistical information of DHCP Relay.

show dhcp-relay

[Parameter]

N/A

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

This command is used to show the content of VLAN that starts DHCP Relay and statistical information of DHCP Relay

[Explanation of command execution echo]

N/A.

[Example]

Show DHCP Relay information:

*Raisecom# **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

[Related command]

Command	Description
dhcp-relay enable	Start global DHCP Relay
dhcp-relay listen	Enable or disable the DHCP Relay function on the VLAN

3.168. show dhcp-relay listen

NOT AVAILABLE FOR: ISCOM2826/2126/2016/2008/2026/2826E

[Introduction]

Show the configuration information about particular or all the VLAN of DHCP Relay.

show dhcp-relay listen [**vlan** vlanid]

[Parameter]

vlanid specify VLAN, range is 1～4094.

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

show dhcp-relay listen show all the configuration information about DHCP Relay on the VLAN

show dhcp-relay listen vlan vlanid this command show particular configuration information about DHCP RELAY on the VLAN.

If the VLAN is not specified, then all the information for the VLAN are shown. The main content is that the VLAN of DHCP Relay is not started.

[Explanation of command execution echo]

N/A

[Explanation of command execution echo]

Show the configuration information for all the VLAN:

*Raisecom# **show dhcp-relay listen***
The VLAN that enabled the DHCP Relay include:
VLAN ID = 1, 2
The total enabled VLAN num is 2

Show the configuration information for designated VALN 2:

*Raisecom# **show dhcp-relay listen vlan** 2*
VLAN 2 disabled DHCP Relay

[Related command]

Command	Description
dhcp-relay enable	Start global DHCP Relay
dhcp-relay listen	Enable or disable the DHCP Relay function on the VLAN.

3.169. show dhcp-relay server-ip

NOT AVAILABLE FOR: ISCOM2826/2126/2016/2008/2026/2826E

[Introduction]

Show the IP address information for DHCP server.

show dhcp-relay server-ip

[Parameter]

N/A

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

This command is used to show the IP address information for DHCP Server.

[Explanation of command execution echo]

N/A.

[Example]

show DHCP server address information:

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

index IP address Status

----

1 10.0.0.1 active

2 10.0.0.12 active

3 10.0.0.13 active

[Related command]

Command	Description
dhcp-relay server-ip	Set or delete DHCP server IP address.

3.170. show dhcp-server

[Introduction]

Show the configuration information and statistic information of DHCP server.

show dhcp-server

[parameter]

N/A

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

The command is used to show the configuration information and statistic information of DHCP server.

[Explanation of command execution echo]

N/A.

[Example]

Show the information of adjacent DHCP server.

*Raisecom#**show dhcp-server***
DHCP server: Enable
Active VLAN:
1
The total enabled VLAN: 1

Max lease time: 4334 m
Min lease time: 232 m
Default lease time: 339 m

Statistics infomation:
Running time: 6 hours 36 munites 20 seconds
Bootps: 0
Discover: 0
Request: 0
Release: 0
Offer: 0
Ack: 0
Nack: 0
Decline: 0
Information: 0
Unknows: 0
Total: 0

[Related command]

Command	Description
dhcp-server enable	Start DHCP server
dhcp-server active	Start DHCP server on the VLAN.

3.171. show dhcp-server ip-pool

[Introduction]

Show the configuration information for the IP pool of DHCP server.

show dhcp-server ip-pool

[Parameter]

N/A.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

This command is used to show the configuration information for the IP pool of DHCP server.

[Explanation of command execution echo]

N/A.

[Example]

Show adjacent information for DHCP Server.

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

Name of IP pool table: aa

Status of IP pool table: active

IP address range: 1.2.0.1 - 1.2.0.5

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: 5

Alloted IP address count: 0

[Related command]

Command	Description
dhcp-server enable	Start DHCP server.
dhcp-server ip-pool name	Configure IP pool

3.172. show dhcp-server relay-ip

[Introduction]

Show the configuration information of adjacent DHCP-server relay-ip address

show dhcp-server relay-ip

[Parameter]

N/A

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

The command is used to show the configuration information of adjacent DHCP-server relay-ip.address.

[Explanation of command execution echo]

N/A

[Example]

Show the information of adjacent DHCP-server relay-ip address.

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

index IP address IP Mask Status

----

1 2.0.0.2 255.0.0.0 active

[Related command]

Command	Description
dhcp-server relay-ip	Set of delete the adjacent DHCP-server relay-ip address.

3.173. show diags

[Introduction]

Show port diagnose information

show diags link-flap

[Parameter]

link-flap show UP/DOWN times and their speed(number of UP/DOWN at the last minute);

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

N/A.

[Example]

Raisecom#show diags l

Port Total Last Min

---

19 2 0

21 2 2

[Related command]

N/A.

3.174. show dlf-forwarding

[Introduction]

Show whether to forward DLF message.

show dlf-forwarding

[Parameter]

N/A

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

DLF-forwarding: Enable

[Example]

*Raisecom# **show dlf-forwarding***

[Related command]

Command	Description

dlf-forwarding {enable | disable}	Forward or terminate DLF packet locally.

3.175. show filter

NOT AVAILABLE FOR: 2126/2016/2008/2026.

[Introduction]

This command is used to show the related information of filter

[Command format]

show filter

[Parameter]

N/A

[Default]

N/A.

[Command Modes]

Privileged EXEC

[Example]

This command is used to show the related information of the filter. The content is shown based on the order of arrival, the earlier the ACL is added, the more frontal it is.

[Explanation of command execution echo]

Rule filter: Disable

Filter list(Larger order number, Higher priority):

Order ACL-Index IPort EPort VLAN Hardware

---

1 MAP 0 1 - - No

2 IP 0 - 3 - No

[Example]

Raisecom#show filter

[Related command]

Command	Description
filter	Put the filter rule into the rule filter table

filter enable | disable	Start or cancel filter function.

3.176. show ip igmp filter

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Show IGMP filter configuration information.

[Command format]

show ip igmp filter

[Parameter]

N/A.

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

use this command to show global configuration information which is IGMP filtered.

[Explanation of command execution echo]

.

*Raisecom# **show ip igmp filter***

IGMP filter: Enable

[Example]

Raisecom# show ip igmp filter

[Related command]

Command	Description
ip igmp filter	Enable or disable IGMP filter function.

3.177. show ip igmp filter port

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Show the port configuration information of IGMP filter.

[Command format]

Show ip igmp filter port [portid **]**

[Parameter]

portid——(optical), port number.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Use this command to show port config information, which is IGMP filtered, if the parameter is not specified, show information for all the ports.

Filter represents that which IGMP profile is applied by the port. If it is 0, the port

doesn't apply any IGMP profile.

[Explanation of command execution echo]

Show all the ports.

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*

Specify particular port

Raisecom#show ip igmp filter port 1

IGMP Filter: 1

Max Groups: 20

Current groups: 0

Action: Deny

[Example]

Raisecom# ***show ip igmp filter port 1***

[Related command]

Command	Description
ip igmp profile profile-number	Create IGMP profile information
ip igmp max-groups	The maximum number which is allowed to be added into group.
ip igmp max-groups action	The action is taken when the number of group added exceeds the allowed maximum number.

3.178. show ip igmp snooping

NOT AVAILABLE FOR: ISCOM2026.

[Introduction]

Show the dynamic-studying or manual configuration information of multi-router port or IGMP Snooping configuration information.

[Command Format]

show ip igmp-snooping [mrouter] [vlan *vlanid* **]**

[Parameter]

mrouter Show the dynamic-studying or manual configuration information of multi-router port.

vlanid VLAN ID range form 1 to 4094.

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user

[Usage Guide]

show ip igmp snooping show IGMP snooping state and particular VLAN state.

show ip igmp snooping mrouter show dynamic studying or manual configuration information of multi-cast router port.

show ip igmp snooping vlan vlanid show the state of particular VLAN.

show ip igmp snooping mrouter vlan vlanid show multicast router port information of designated VLAN.

If do not specify VLAN, show all the VLAN information.

[Explanation of command execution echo]

N/A.

[Example]

Show IGMP snooping configuration information:

*Raisecom# **show ip igmp snooping***

IGMP snooping: Enable

IGMP snooping aging time: 50s

IGMP snooping active vlan: 1

IGMP snooping immediate-leave active vlan: --

Show all the multicast router information of all the VLAN:

*Raisecom# **show ip igmp snooping mrouter***

Ip Address Port VLAN Age Type

Show IGMP snooping configuration information of VLAN 1:

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

IGMP snooping: Enable

IGMP snooping aging time: 50s

IGMP snooping on Vlan 1: Enable.

IGMP snooping immediate-leave on Vlan 1: Disable.

Show IGMP snooping multicast router information of VLAN 1:

*Raisecom#**show ip igmp snooping mrouter vlan 1***

IGMP snooping: Enable

IGMP snooping aging time: 50s

IGMP snooping on Vlan 1: Enable.

IGMP snooping immediate-leave on Vlan 1: Disable.

VLAN 1 immediate leave: Disable.

[Related command]

N/A.

3.179. show ip igmp profile

NOT AVAILABLE FOR:ISCOM2026.

[Introduction]

Show the configuration information of IGMP profile.

[Command format]

show ip igmp profile [profile-number**]**

[Parameter]

profile-number——optical, already defined IGMP profile number.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Use this command to show IGMP profile configuration information. When the parameter has not been specified, show all the already defined IGMP profile information.

[Explanation of command execution echo]

show all the 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

·show designated ip igmp 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

[Example]

Raisecom# ***show ip igmp profile***

[Related command]

Command	Description
ip igmp profile profile-number	Create IGMP profile information
permit | deny	Set IGMP profile action
range start-ip [end-ip]	Set IGMP profile range.

3.180. show ip route

[Introduction]

use **show ip route** to show the route of system route table.

show ip route [A.B.C.D_1 **[** A.B.C.D_2 **\| longer-prefixes]]**

[Parameter]

A.B.C.D_1 IP network prefix;

A.B.C.D_2 network mask;

longer-prefixes long network prefix matching

[Default]

Show all the routes.

[Command Modes]

Privileged EXEC; privileged user.

[Example]

Use this command to show IP router information, can show different route information based on their types, also can route information for particular network prefix. Also can use this command to show the route information in hardware transmit table.

[Explanation of command execution echo]

N/A.

[Example]

*Raisecom#**show ip route 10.0.0.0 longer-prefixes***

Codes: C - connected, H-HardWare S - static, R - RIP, O - OSPF

C 8.1.0.0[255.255.0.0],is directly connected , Interface 0

C 8.2.0.0[255.255.0.0],is directly connected , Interface 1

*Raisecom#**show ip route***

Codes: C - connected, H-HardWare S - static, R - RIP, O - OSPF

C 8.1.0.0[255.255.0.0],is directly connected , Interface 0

C 8.2.0.0[255.255.0.0],is directly connected , Interface 1

O 10.0.0.0[255.0.0.0],via 8.1.0.2

O 9.0.0.0[255.0.0.0], via 8.1.0.2

[Related command]

Command	Description
ip route	Configure static IP route

3.181. show interface ip ip-access-list

[Introduction]

This command is used to show access control related information for layer-3 interface.

[Command format]

show interface ip ip-access-list

[Parameter]

N/A.

[Default]

N/A.

[Command Modes]

Privileged user.

[Usage Guide]

This command is used to show related information of layer-3 ACL. The information shown is based on the order of arrival, the later the information is added, the more frontal it is.

[Explanation of command execution echo]

Filter list(Larger order number, Higher priority):

Index ACL-Index

---

0 IP 3

3.182. show interface mac-address-table threshold

NOT AVAILABLE FOR: ISCOM3026/2826/2126/2026/2826E

[Introduction]

Show the number limitation of port studying MAC address.

show interface mac-address-table threshold

[Parameter]

N/A.

[Default]

N/A.

[Command Modes]

Privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

Show “port….. MAC valve value” information.

[Example]

Show the limitation of port MAC address studying

*Raisecom#**show interface mac-address-table threshold***

[Related command]

command	Description
mac-address-table threshold	Configure the upper bound value of port studying MAC address

3.183. show interface port

NOT AVAILABLE FOR: ISCOM2026

[Introduction]

show state of particular or all the ports.

show interface port [{ statistic |[port-list **statistic] }]**

[Parameter]

interface interface

port physical port;

statistic statistical information;

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user. (Priority 15)

[Usage Guide]

Only the privileged user with priority not less than 5 can use this command.

[Explanation of command execution echo]

R: Receive Direction
S: Send Direction
Port Admin Operate Speed/Duplex Flowcontrol(R/S) Mac-learning
---
show port state:

port No: X

InOctets: 0
InUcastPkts: 0
InMulticastPkts: 0
InBroadcastPkts: 0
OutOctets: 0
OutUcastPkts: 0
OutMulticastPkts: 0
OutBroadcastPkts: 0
DropEvents: 0
CRCAlignErrors: 0
UndersizePkts: 0
OversizePkts: 0
Fragments: 0
Jabbers: 0
Collisions: 0
Tx: 0 pps, 0 bps during 30 seconds.
Rx: 0 pps, 0 bps during 30 seconds.
Tx: 0 pps, 0 bps during 1800 seconds.
Rx: 0 pps, 0 bps during 1800 seconds.
Show statistical information for port X

[Usage Guide]

Show the state for port 5.

*Raisecom# **show interface port** 5*

Show statistical information for port 2:

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

[Related command]

Command	Description
speed	Set the speed and duplex mode.
duplex	Set the duplex mode of the port.
speed auto-negotiate	Set the port speed to auto-negotiate.
flowcontrol	Set the start and shutdown for flow control function of the port.
mac-address-table learning	Set the start and shutdown of physical port MAC address studying function.

3.184. show interface port statistics

ONLY AVAILABLE FOR: ISCOM2026

[Introduction]

show the packet statistical information for particular or all the ports.

show interface port [<1-26>] statistics

[Parameter]

interface port:

port physical port;
statistic statistical information;

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user (priority 5).

[Usage Guide]

Only the privileged user with priority not less than 5 can use this command.

[Explanation of command execution echo]

[Example]

Show the statistical information for port 2.

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

Port 2

InOctets: 0
InUcastPkts: 0
InMulticastPkts: 0
InBroadcastPkts: 0
OutOctets: 0
OutUcastPkts: 0
OutMulticastPkts: 0
OutBroadcastPkts: 0
DropEvents: 0
CRCAlignErrors: 0
UndersizePkts: 0
OversizePkts: 0
Fragments: 0
Jabbers: 0
Collisions: 0
Tx: 0 bps during 2 seconds.
Rx: 0 bps during 2 seconds.
Tx: 0 bps during 300 seconds.
Rx: 0 bps during 300 seconds.

[Related command]

Command	Description
statistic packet ingress {good |bad |local} egress {good |bad |abort}	Set the type for port statistical packet.

3.185. show interface port protected

NOT AVAILABLE FOR: ISCOM3026/2826/2126/2026/2826E

[Introduction]

show port protected property of physical port.

show interface port protected

[Parameter]

N/A.

[Default]

N/A.

[Command Modes]

Privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

show “port….protected state” information.

[Usage Guide]

Show port protected property.

Raisecom# ***show interface port protected***

[Related command]

command	description
switchport protect	Configure the protected property of theport.

3.186. show interface port switchport

[Introduction]

Show the configuration information of the VLAN.

show interface port [{1-26}] **switchport**

[Parameter]

{1-26} port list.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Show VLAN configuration information of the port.

[Explanation of command execution echo]

X stands for port number.

Port X:
Administrative Mode: extend-access
Operational Mode: extend-access
Access Mode VLAN: 1(default)
Administrative Hybrid Allowed VLANs: 1,2
Operational Hybrid Allowed VLANs: N/A
Administrative Hybrid Untagged VLANs: N/A
Operational Hybrid Untagged VLANs: N/A
Administrative Trunk Allowed VLANs: all
Operational Trunk Allowed VLANs: N/A
Native Mode Vlan: 1(default)

[Related command]

Command	Description
switchport access vlan	Show the ACCESS VLAN ID of the port
switchport hybrid allowed vlan	Set the port to allowable VLAN, when it is set to HYBRID mode.
switchport hybrid untagged vlan	Set the port to allowable UNTAG VLAN, when it is set to HYBRID mode.
switchport mode	Set the VLAN mode of the port.
switchport native vlan	Set the NATIVE VLAN for the port, when it is set to HYBRID or TRUNK mode.
switchport trunk allowed vlan	Set the port to allowable VLAN, when the port is set to TRUNK mode.
show interface port portlist **switchport**	Show the port related VLAN configuration.

3.187. show logging

[Introduction]

Show log information.

show logging [file]

[Parameter]

file show the logging information which is stored in the file.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Use this command to show the logging configuration information or logging information in the logging information saved in the logging file.

[Explanation of command execution echo]

Show logging information.

*Raisecom#**show logging***
Syslog logging: enable, 0 messages dropped, messages rate-limited 0 per second
Console logging: enable, level=debug ,22 Messages logged
Monitor logging: disable, level=info ,0 Messages logged
Time-stamp logging messages: enable

Log host Information:
Target Address Level Facility Sent Drop

192.168. 1. 9 debug local7 11 11
192.168. 1.185 debug local7 11 11

show the information saved in the logging file.

*Raisecom#**show logging file***
Logging information in file
DEC-31-1999 00:04:45 SYS-1-START-A:System startup

DEC-31-1999 00:16:40 SYS-1-START-A:System startup
DEC-31-1999 03:54:37 SYS-1-START-A:System startup
DEC-31-1999 05:24:22 SYS-1-WRITE-A:Write system configuration
DEC-31-1999 04:02:35 SYS-1-START-A:System startup
DEC-31-1999 05:34:36 SYS-1-WRITE-A:Write system configuration
DEC-31-1999 05:37:41 SYS-1-WRITE-A:Write system configuration

[Example]

Show the log information saved in the file.

*Raisecom#**show logging file***

[Related command]

Command	Description
Logging console	Start the console output direction of the logging file.
logging monitor	Start the monitor output direction of the logging file.
logging file	Start the output direction of logging file.
logging time-stamp	Set the countermark of logging information.

3.188. show loopback-detection

[Introduction]

Show the loopback-detection state for the port.

show loopback-detection

[Parameter]

N/A.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A

[Explanation of command execution echo]

Show the time period of loopback-detection and target address. Show port loopback-detection state including the port loopback-detection function state (enable or disable); whether the there is a loopback setting for the port:: yes-loopback, no- no loopback; port state and closing time; the source port which has loopback with this port.

[Example]

Set the time period for loopback-detection to 3 second.

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

Close the loopback detection function for port 1.

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

Show port loopback state.

*Raisecom# **show loopback-detection***

Show the content as following, port 2 and port 6 form external loopback, port 9 self-loop.

Period of loopback-detection: 3 s
VLAN: 1
Destination address: FFFF.FFFF.FFFF
Port Detection State Loop Flag State/Time Source Port
----
1 disable no --/infin --
2 enable no --/infin --
3 enable no --/infin --

4 enable no --/infin --
5 enable no --/infin --
6 enable yes down/infin 2
7 enable no --/infin --
8 enable no --/infin --
9 enable yes down/infin 9

[Related command]

Command	Description
loopback-detection { enable **|** disable **} port-list {**all **|** port-list**}**	Start/close the loopback-detection function of designated port
loopback-detection hello-time <1-65535**>**	Configure the time period of loopback-detection.
loopback-detection destination-address [mac-addr **vlan** vid**]**	Configure the loopback-detection address.
loopback-detection down-time {infinite | <0-65534>}	Shutdown loop port time.

3.189. show mac aging-time

[Introduction]

Show MAC address aging time.

show mac aging-time

[Parameter]

aging-time MAC address aging time.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Only the privileged user with priority not less than 5 can use this command.

[Explanation of command execution echo]

Aging time: X seconds
Set unsuccessfully !

[Example]

Show current aging time:
Raisecom# **show mac aging-time**

[Related command]

command	Description
mac-address-table aging-time	Set MAC address aging time.
no mac-address-table aging-time	Recover the default value of MAC address aging time.

3.190. show mac-address-table l2-address

[Introduction]

Show all the addresses list in the current MAC address table, including static setting and dynamic MAC address which have been aged.

show mac-address-table l2-address

show mac-address-table l2-address port port-number

show mac-address-table l2-address vlan vlan_id

[Parameter]

vlan VLAN;
vlan_id VLAN ID, range from 1-4094;
port physical port.
port-number physical port number, range is from 1-26.

[Default]

N/A.

[Command Modes]

Privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

show “MAC address, port, VLAN, symbol” and other address item information.

[Example]

Show all the MAC address.

*Raisecom#**show mac-address-table l2-address***

Show all the MAC address of physical port 5.

*Raisecom#**show mac-address-table l2-address port** 5*

Show all the MAC address of vlan 2.

*Raisecom#**show mac-address-table l2-address vlan** 2*

[Related command]

Command	Description
search mac-address HHHH.HHHH.HHHH	Search the state of MAC address in the switch.

3.191. show mac-address-table l2-address count

[Introduction]

Count MAC address table.

show mac-address-table l2-address count

show mac-address-table l2-address count port port-number

show mac-address-table l2-address count vlan vlan_id

[Parameter]

count count the number.;
vlan VLAN;
vlan_id VLAN ID, range from 1-4094;
port physical port;
port-number physical port number, range from 1-26;

[Default]

N/A.

[Command Modes]

Privileged user.

[Example]

N/A.

[Explanation of command execution echo]

Show the number of related MAC address.

[Example]

Count the number of all the MAC address.

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

Count the number of MAC address for physical port 5.

*Raisecom#**show mac-address-table l2-address count port** 5*

Count the number for all MAC address of VLAN 2

*Raisecom#**show mac-address-table l2-address count vlan** 2*

[Related command]

Command	Description
Search mac-address HHHH.HHHH.HHHH	Search the state of MAC address in the switch.

3.192. show mac-address-table multicast

[Introduction]

Use the command to show layer 2 multicast entity of switch or referred VLAN.

show mac-address-table multicast [vlan vlan-id**] [count]**

[Command Format]

show mac-address-table multicast [vlan *vlan-id***] [count]**

[Parameter]

count show all count.

vlan *vlanid* VLAN ID(optional),range from 1 to 4094

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user

[Usage Guide]

show mac-address-table multicast show all VLAN layer 2 multicast router information of switch

show mac-address-table multicast vlan *vlan-id* show referred VLAN layer 2 multicast router information of switch.

show mac-address-table multicast count show all VLAN layer 2 multicast count information of switch

show mac-address-table multicast vlan *vlan-id* **count** show referred VLAN layer 2 multicast count information of switch.

if VLAN is not referred ,show all VLAN layer 2 multicast router information.

[Explanation of command execution echo]

N/A.

[Example]

Show all VLAN layer 2 multicast router information

*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)

Show layer 2 multicast router information of VLAN 2.

*Raisecom#**show mac-address-table multicast vlan** 2*

Multicast filter mode: Forward-all

Vlan Group Address Ports[Static](Hardware)

----

2 0100.5E08.0808 1-6[1-6](1-6)

Show all VLAN layer 2 multicast router count information.

*Raisecom#**show mac-address-table multicast count***

Multicast filter mode: Forward-all

Multicast address entries for all Vlans: 1

Show layer 2 multicast router counter information of VLAN 2.

*Raisecom#**show mac-address-table multicast vlan** 2 **count***

Multicast filter mode: Forward-all

Multicast address entries for all Vlans: 1

[Related command]

command	description
ip igmp snooping static	Add a layer 2 port as multicast member.

3.193. show mac-address-table static

[Introduction]

Show statid MAC address information.

show mac-address-table static

show mac-address-table static port port-number

show mac-address-table static vlan vlan_id

[parameter]

vlan VLAN;
vlan_id VLAN ID, range is 1-4094;
port physical port;
port-number physical port number ,range from 1 to 26.

[Default]

N/A

[Command Modes]

privileged user

[Usage Guide]

N/A.

[Explanation of command execution echo]

Information of static mac address in switch:
port No. VLAN ID static MAC Addr

[Example]

show static MAC address.
*Raisecom# **show mac-address-table static***
show the static MAC address table of physical port 5
*Raisecom#**show mac-address-table static port** 5*
Show the static MAC address information of vlan 2.
Raisecom#show mac-address-table static vlan 2

[Related command]

Command	Description
mac-address-table static	Set static MAC address.use no to delete.

3.194. show memory

[Introduction]

Show memory information.

show memory

[Parameter]

N/A.

[Default]

N/A.

[Command format]

Privileged EXEC; privileged user.

[Usage Guide]

N/A.

[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*	-

[Related command]

N/A.

3.195. show mirror

[Introduction]

Show the mirror situation for all the settings.

show mirror

[Parameter]

mirror mirror function;

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A

[Explanation of command execution echo]

Mirror: Disable
Monitor port: 1
----------the ingress mirror rule----------
Mirrored ports: 3,4
----------the egress mirror rule----------
Mirrored ports: 3,4

[Example]

show the mirror rule:

*Raisecom# **show mirror***

[Related command]

Command	Description
mirror {enable | disable}	Mirror function enable/disable.
mirror monitor-port	Set the mirror monitor port.
mirror source-port-list	Set the source mirror port.

3.196. show mls qos

[Introduction]

show QoS configuration information.

[Command format]

show mls qos

[Parameter]

N/A.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

show QoS configuration information.

[Explanation of command execution echo]

Set the strict priority mode unsuccessfully.
Raisecom#show mls qos

[Example]

*Raisecom# **show mls qos***

[Related command]

Command	Description
mls qos	Show the queue information.

3.197. show mls qos maps

NOT AVAILABLE FOR:ISCOM2026/2126.

[Introduction]

show the mapping configuration information in the QoS.

[Command format]

show mls qos maps [**cos-dscp** | **dscp-cos** | **dscp-mutation** | **ip-prec-dscp**]

[Parameter]

N/A.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Show QoS mapping configuration information.

[Explanation of command execution echo]

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
```

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
```

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
```

Raisecom#show mls qos maps ip-prec-dscp

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 :      10   11   12   13   14   15   16   17   18   19
 2 :      5    5    5    5    5    5    5    5    5    5
 3 :      5    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
```

[Example]

Raisecom# ***show mls qos maps***

[Related command]

Command	Description
mls qos map [cos-dscp | dscp-cos | ip-prec-dscp | dscp-mutation]	Show queue information.

3.198. show mls qos policer

NOT AVAILABLE FOR:RC2008/2016/2026/2126.

[Introduction]

Show policer configuration information in QOS.

[Command format]

show mls qos policer [police-name **| aggregate-policer |class-policer | single-policer]**

[Parameter]

police-name——policer name.

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Show policer configuration information in QoS

[Explanation of command execution echo]

Raisecom#show mls qos policer
aggregate-policer bbb 50 500 exceed-action drop
Not used by any policy map

Raisecom#show mls qos police aggregate-policer
aggregate-policer bbb 50 500 exceed-action drop
Not used by any policy map

[Example]

Raisecom# **show mls qos policer**

[Related command]

command	description
mls qos {aggregate-policer |class-policer | single-policer } policername **rate burst [exceed-action { drop | policed-dscp-transmit dscp }]**	Configure policer

3.199. show mls qos port

[Introduction]

Show port configuration information.

[Command format]

show mls qos port [portid]

[Parameter]

portid—port ID.

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user.

[Example]

Show port configuration information.

[Explanation of command execution echo]

Raisecom#show mls qos port 1

port 1:

Attached policy-map for Ingress: aaa

trust state: not trusted

default COS: 0

COS override: disable

default DSCP: 0

DSCP override: disable

DSCP Mutation Map: default-dscp

[Example]

Raisecom# ***show mls qos port 1***

[Related command]

Command	Description
mls qos trust [**cos** | **dscp** | **ip-precedence**]	Set the trust state for the port.
mls qos default-cos { default-cos | **override }**	Set the default cos for the port.
mls qos default-dscp { default-dscp | **override }**	Set the default dscp for the port.
mls qos dscp-mutation dscp-name	Apply dscp-mutaion on the port.
Service-policy policy-name **ingress** portid	Apply policy on the port.

3.200. show mls qos port policers

NOT AVAILABLE FOR: RC2008/2016/2026/2126.

[Introduction]

Show policer configuration information on the port.

[Command format]

show mls qos port [portid] **policers**

[Parameter]

portid——port ID.

[Default]

N/A

[Command Modes]

Privileged user, privilege configuration mode.

[Usage Guide]

Show the policer configuration information on the port.

[Explanation of command execution echo]

Raisecom#show mls qos port 1 policer

Port id 1

policymap name: hh

policer type: Aggregate, name: aa

rate: 433 kbps, burst: 43 kbyte, exceed action: drop

[Example]

Raisecom# ***show mls qos port 1 policer***

[Related command]

Command	Description
mls qos {aggregate-policer |class-policer | single-policer } policername **rate burst [exceed-action { drop | policed-dscp-transmit dscp }]**	Configure policer
police policer-name	Apply policer

3.201. show mls qos queueing

[Introduction]

Show queue configure information.

[Command format]

show mls qos [**port** portid] **queueing**

[Parameter]

portid——port ID.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Show queue configuration information.

[Explanation of command execution echo]

Raisecom#show mls qos queueing

the queue schedule mode: strict priority(SP)

wrr queue weights:

queueid-weights-delay

1 - 0 - 0

2 - 0 - 0

3 - 0 - 0

4 - 0 - 0

Cos-queue map:

cos-queueid

0 - 1

1 - 1

2 - 2

3 - 2

4 - 3

5 - 3

6 - 4

7 - 4

[Example]

Raisecom# ***show mls qos port 1 queueing***

[Related command]

Command	Description
Queue wrr-weight	Configure queue mode.
Queue preemp-wrr	Configure queue mode.
Queue strict-priority	Configure queue mode.
Queue bounded-delay	Configure queue mode.
Queue cos-map	Set the mapping form internal priority to queue.

3.202. show mvr

NOT AVAILABLE FOR:ISCOM2026.

[Introduction]

Show MVR configuration information.

[Command format]

show mvr

[Parameter]

N/A.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Use this command to show MVR global configuration information.

[Explanation of command execution echo]

.

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

[Example]

Raisecom# ***show mvr***

[Related command]

Command	Description
mvr { enable | disable }	Start/stop MVR
mvr vlan vlanid	Set multicast VLAN
mvr mode { dynamic | compatible }	Set MVR mode.
mvr group	Set MVR multicast group

3.203. show mvr member

NOT AVAILABLE FOR:ISCOM2026.

[Introduction]

show MVR configuration multicast group information.

[Command format]

show mvr member [ip-address **]**

[Parameter]

ip-address——show designated IP group information, the IP address should be IP address of D type, format is A.B.C.D.

[Default]

N/A.

[Command Modes]

Privileged user; Privileged EXEC.

[Example]

Show MVR configured multicast group information.

MVR group state: active stands for there are ports added into this group(statically or dynamically), inactive stands for no ports added into this group.

Members explain which port is added into this group; if N/A, the state is N/A.

[Explanation of command execution echo]

.

Raisecom#show mvr members

MVR Group IP	*Status*	*Members*
234.5.6.7	*Active*	*1*
234.5.6.8	*Active*	*1*
234.5.6.9	*Inactive*	*N/A*
234.5.6.10	*Inactive*	*N/A*
234.5.6.11	*Inactive*	*N/A*

[Example]

*Raisecom# **show mvr members***

[Related command]

Command	Description
mvr { enable | disable }	Start /stop MVR
mvr group	Set MVR multicast group.

3.204. show mvr port

NOT AVAILABLE FOR:ISCOM2026.

[Introduction]

Show MVR port configuration information.

[Command format]

show mvr port [portid**]**

[Parameter]

portid——port ID.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

show MVR port configuration information.

“running” stand for whether the port has started the MVR.

“type” stands for port MVR type, there are three types: non-MVR, source, receiver;

up/down stands for the connection status for the ports, active stands for the port belongs to a VLAN; inactive stands for the port is not belongs to a VLAN.

Immediate leave stand for whether the port is started or not.

[Explanation of command execution echo]

show all the port 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
```

show individual port information.

```
Raisecom#show mvr port 1
Running: Enable
Type: Receiver
Status: Inactive/down
Immediate Leave: Enable
```

[Example]

show all the port information.

Raisecom# ***show mvr port***

Show designated port information.

Raisecom# ***show mvr port 1***

[Related command]

Command	Description
mvr { enable | disable }	start/stop MVR
mvr vlan vlanid	Set multicast VLAN
mvr group	Set MVR multicast group.
mvr type { source | receiver}	Configure port MVR type.
mvr immediate	Configure immediate leave.
mvr vlan vlanid **group** ip-address	Configure port to static multicast group

	member.

3.205. show mvr port member

NOT AVAILABLE FOR:ISCOM2026.

[Introduction]

Show MVR port static multicast group member configuration information.

[Command format]

show mvr port portid **members**

[Parameter]

portid——PortID.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Show static multicast group member configuration information of the MVR port.

"type" stands for whether the port is statically configured by mvr vlan vlanid group command, or by igmp dynamically study and add the packet.

"status" stands for the MVR state of the port, active stand for the port belongs to the same VLAN, inactive stands for the port is not in the same VLAN.

[Explanation of command execution echo]

Raisecom#show mvr port 1 members

MVR Group IP Type Status

234.5.6.7 static Inactive

234.5.6.8 static Inactive

[Example]

show port 1 information:

*Raisecom# **show mvr port 1 members***

[Related command]

Command	Description
mvr { enable | disable }	Start / stop MVR
mvr vlan vlanid	Set multicast VLAN
mvr group	Set MVR multicast group
mvr type { source | receiver}	Configure port MVR type.
mvr immediate	Configure immediate leave.
mvr vlan vlanid **group** ip-address	Configure port to be a static multicast group member.

3.206. show policy-map

NOT AVAILABLE FOR:RC2008/2016/2026/2126.

[Introduction]

show class-map information.

[Command format]

show policy-map [policy-map-name] [**class** class-name]

show policy-map port [portId]

[Parameter]

policy-map-name——specify the name of policy-map, the maximum length is 16 characters.

class-name——specify the name of class-map, the maximum length is 16 characters.

Portid——port id

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

show policy-map information.

[Explanation of command execution echo]

Raisecom#show policy-map port 1
port 1:
Policy Map aaa:
Egerss:n/a
Class Map :aaa (match-any)

Raisecom#show policy-map
Policy Map aaa
Class aaa
police bbb
trust dscp

Raisecom#show policy-map aaa class aaa
Policy Map aaa
Class aaa
police bbb
trust dscp

[Example]

Raisecom# ***show policy-map***
Raisecom# ***show policy-map*** *aaa*
Raisecom# ***show policy-map class-map*** *aaa*
Raisecom# ***show policy-map*** *aaa* ***class-map*** *aaa*
Raisecom# ***show policy-map port*** *1*

[Related command]

Command	Description
Policy-map policy-map-name	Create policy map
description WORD	Set policy map description information.
[no] class class-map-name	Apply class map on the policy
set {**ip dscp** new-dscp | **ip precedence** new-precedence | **cos** new-cos }	Set the action.

[no] police policer-name	Apply policer
trust [**cos** | **dscp | ip-precedence**]	Set the trust state for the traffic.

3.207. Show processes

[Introduction]

Show the status and stack information of the process.

show processes

[Parameter]

N/A.

[Default]

N/A.

[Command Modes]

Privileged user; Privileged EXEC.

[Usage Guide]

N/A.

[Explanation of command execution echo]

[Example]

*Raisecom#**show processes***

Task Information :

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

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

TSD- task delay;DTS-dead task

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2907680 tCcomTm 840 55 TSD 0 (2 / 0.0%)
348df68 tSntpS 4344 56 POS 0 (0 / 0.0%)
2a7c008 tDhcpS 19464 56 0 (0 / 0.0%)
2a6f480 tLoopD 3944 60 TSD 0 (10 / 0.0%)
2906408 tCcom 3848 60 POS 0 (2 / 0.0%)
2a1e7f0 tRmon 32632 75 TSD 81000c (15 / 0.0%)
2a11358 tPortStats 3632 75 TSD 0 (6 / 0.0%)
2a0aeb8 tLinkTrap 8040 75 TSD 0 (2 / 0.0%)
2a06868 tColdTrap 3944 75 TSD 0 (1 / 0.0%)
2a23a38 tIgmpTm 2848 100 TSD 0 (0 / 0.0%)
2a22c20 tIgmpSnoop 3816 100 POS 0 (0 / 0.0%)
2a21a08 tSnmp 11816 100 POS 0 (0 / 0.0%)
2a16590 tIpBind 3904 100 TSD 81000c (1 / 0.0%)
2a08b78 tEndStat 7832 100 3d0004 (0 / 0.0%)
29e2558 tRmonAlrm 7976 100 POS 0 (2 / 0.0%)
27aea90 tTelnetdOut0 3336 100 POS 0 (0 / 0.0%)
27ad878 tTelnetdIn0 3384 100 POS 0 (0 / 0.0%)
27ac610 tTelnetdOut1 3336 100 POS 0 (0 / 0.0%)
27ab3f8 tTelnetdIn1 3384 100 POS 0 (0 / 0.0%)
27aa190 tTelnetdOut2 3336 100 POS 0 (0 / 0.0%)
27a8f78 tTelnetdIn2 3384 100 POS 0 (0 / 0.0%)
27a7d10 tTelnetdOut3 3336 100 POS 0 (0 / 0.0%)
27a6af8 tTelnetdIn3 3384 100 POS 0 (0 / 0.0%)
27a5890 tTelnetdOut4 3336 100 POS 0 (0 / 0.0%)
27a4678 tTelnetdIn4 3384 100 POS 0 (0 / 0.0%)
27a3460 tTelnetd 3640 100 POS 0 (0 / 0.0%)
3489320 tSyslog 7968 105 POS 0 (0 / 0.0%)
2daaac8 tx_cb 15912 110 POS 0 (0 / 0.0%)
348f558 tSntpCLsn 4760 150 TSD 0 (1 / 0.0%)
2a52d20 tRelay 3880 151 POS 0 (0 / 0.0%)
2da0958 rx0 15888 200 3d0004 (29 / 0.0%)
2cc1c98 tArlAging 1896 200 TSD 0 (0 / 0.0%)
2b38248 tSnmpTm 3856 200 POS 0 (0 / 0.0%)
2c25d60 tRosInit 5912 250 POS 81000e (0 / 0.0%)
2a730d0 tStpTm 3808 250 TSD 0 (6 / 0.0%)
27af260 tIdle 568 251 RDY 0 (281 / 0.0%)

[Related command]

N/A.

3.208. show rate-limit port-list

[Introduction]

Show the setting of bandwidth limitation.

show rate-limit port-list [{port-list}]

[Parameter]

rate-limit bandwidth limitation;
port-list physical port;

port-list physical port number, range is 1-26, can use “,” and “;” to set multiple port inputs;

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

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)

[Example]

Show bandwidth control information.

Raisecom# ***show rate-limit port-list***

[Related command]

Command	Description
rate-limit port-list	Set the bandwidth limitation.
no rate-limit port-list	Delete the bandwidth limitation for the port.

3.209. show relay port-list

[Introduction]

Show the setting of transparent transmission port.

show relay port-list

[Parameter]

relay port transparent transmission for two layer packets.

port-list physical ports.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

Type Ports

BPDU --

Dot1x --

LACP --

GARP --

GMRP --

GVRP --

[Example]

show transparent transmission port:

Raisecom# ***show relay port-list***

[Related command]

Command	Description
realy protocol-type **port-list**	Set transparent transmission port

3.210. show rmon alarms

[Introduction]

Use **show rmon alarms** to show rmon alarm information.

show rmon alarms

[Parameter]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

[Explanation of command execution echo]

refer RFC 1757 for detail information of **rmon alarms** table

[Example]

*Raisecom#****show rmon alarms***

Alarm 10 is Active, Owned by jjhshen

Monitors 1.3.6.1.2.1.2.2.1.20 every 20 seconds

Taking delta samples, last value was 0

Rising threshold is 15, assigned to event 1

Falling threshold is 1, assigned to event 0

On startup enable rising or falling alarm

[Related command]

Command	Description
show rmon event	Show rmon **events** table information
show rmon history	Show rmon **history** table information.
show rmon statistics	Show rmon **statistics** table information.

3.211. show rmon events

[Introduction]

Use show rmon event to show information of rmon events table.

show rmon event

[Parameter]

N/A

[Command Modes]

Privileged EXEC, privileged user

[Usage Guide]

rmon alarm the detailed information of rmon alarm is in RRFC 1757.

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#****show rmon event***

Event 2 is active, owned by this

Description is eee.

Event firing causes log and trap ,last send 0:0:0.

[Related command]

command	Description
show rmon history	Show rmon **history** table information.
show rmon statistics	Show rmon **statistics** table information.
show rmon alarm	Show rmon alarm table information.

3.212. show rmon statistics

[Introduction]

Use show rmon statistics of rmon statistics table.

show rmon statistics

[Parameter]

N/A

[Command Modes]

Privileged EXEC, privileged user

[Usage Guide]

rmon statistics The detailed information of rmon statistics is shown in RFC 1757

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#**show rmon statistics***

Interface 2 is active, and owned by monitorEtherStats

Monitors 1.3.6.1.2.1.2.2.1.1.17825795(ifEntry.1.17825795),which has

Received 0 octets, 0 packets,

0 broadcast and 0 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions.

# of dropped packet events (due to lack of resources): 0

# of packets received of length (in octets):

64: 0, 65-127: 0, 128-255: 0,

256-511: 0, 512-1023: 0, 1024-1518:0

[Related command]

Command	Description
show rmon history	Show the information of rmon history table.
show rmon events	Show the information of rmon events.
show rmon alarms	Show the information of rmon alarm table.

3.213. show rndp

[Introduction]

show RNDP configuration information.

show rndp

[Command format]

Privileged EXEC; privileged user.

[Usage Guide]

user can use this command to check the RDNP global enable state and port enable state.

[Explanation of command execution echo]

Global RNDP Configuration:
RNDP feature is currently enabled on the switch
Participant ports: 1-26

The second and third line show the RNDP enable and port enable state respectively.

[Related command]

Command	Description
rndp	Set RNDP enable status
show rndp neighbor	Show RNDP adjacent information

3.214. show rndp neighbor

[Introduction]

show RNDP neighbor information.

show rndp neighbor

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

User can use this command to check RNDP found neighbor information.

[Explanation of command execution echo]

```
Mac Address       LocalPort   RemotePort   SysID       Hostname
--------------------------------------------------------------------------------
000e.5e00.c2c4        1           9          60003       swB
000e.5e11.4d0b        17          18         60003       Raisecom
000e.5e23.34e2        17          24         60003       Raisecom
```

The first line shows the MAC address of neighbor device

The second line shows the port numbers that is used to connect current device and neighbor device.

The third line shows the port numbers that is used to connect neighbor device and current device

The fourth line shows the device systemID, each device has exclusive systemID, i.e. ISCOM2826 system ID is 60003, but ISCOM2126 is 60005.

The fifth line shows the device hostname.

[Related command]

Command	Description
rndp	Set the enable status of RNDP
show rndp	Show RNDP configuration information.

3.215. show rtdp

[Introduction]

Show RTDP configuration information.

show rtdp

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

user can use this command to check RTDP configuration information.

[Explanation of command execution echo]

RTDP max-hop: 16
RTDP collecting feature: Disabled
RTDP reporting feature: Enabled

[Related command]

Command	Description
rtdp	Set RTDP enable status
rtdp max-hop	Set maximum collection scope of RTDP
show rtdp device-list [HHHH.HHHH.HHH | hostname] [**detailed**]	Show RTDP found device-list information

3.216. show rtdp device-list

[Introduction]

Show FTDP collection information.

show rtdp device-list [HHHH.HHHH.HHHH | hostname] [**detailed**]

[Parameter]

HHHH.HHHH.HHHH the MAC address of need shown device
hostname the hostname of the device.
detailed show detail device information.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

User can use this command to check RTDP collected device information.

[Explanation of command execution echo]

RTDP discovery device-list:

MAC Address	*RcvdPort*	*Hop*	*SysID*	*HostName*
000e.5e00.c2c2	*1*	*2*	*60003*	*swD*
000e.5e00.c2c8	*1*	*2*	*60003*	*swC*
000e.5e00.c2c4	*1*	*1*	*60003*	*swB*

The first line shows the MAC address of the device.
The second line showing: the device is found from which port.
The third line showing the device is found from which hop.
The fourth line showing the device system ID, each device has exclusive system ID, i.e. ISCOM 2826 system ID is 60003, but ISCOM 2126 system ID is 60005

The fifth line showing the device hostname.
Execution echo Detail information

RTDP search by mac 000e.5e00.c2c4 result:
MAC Address RcvdPort Hop SysID HostName

000e.5e00.c2c4 1 1 60003 swB
-Device cluster information:
Idendity: member
Commander MAC: 000e.5e00.c366
AutoActive: on
AutoActive MAC: 000e.5e00.c366
-Device adjacency information:
MAC Address Native Port Remote Port

000e.5e00.c2c2 24 9
000e.5e00.c2c8 1 9

Detail information not only showing all the concise information, but also adding two other following information.

Device cluster information, including:

DeviceID(identity): can be member/candidate/commander;
Commander MAC: it is the MAC address of Commander that can be automatically active by device, and if the device is not the member, do not show the information.
AutoActive on-off(AutoActive): represent whether this device can be automatically active , can be on/off.
AutoActive MAC: the MAC address of Commander that can be automatically active, if the device is not allowed to be automatically active, do not show the information.

Device adjacent information:

The first line represents the downlink MAC address.
The second line represents the port number of the device that is used to connect the adjacent device.
The third line represents the port number of the adjacent device used to connect device.

[Related command]

Command	Description
rtdp	Set RTDP enable status.
rtdp max-hop	Set the maximum range of RTDP.
show rtdp	Show configuration information of RTDP.

3.217. show schedule-list

[Introduction]

Show schedule list information.

show schedule-list [list-no]

[Parameter]

list-no schedule-list range is <0-99>;

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

[Example]

Raisecom# ***show schedule-list 1***

[Related command]

Command	Description
schedule-list list-no	Add or modify schedule list
Comd-str **schedule-list** list-no	Apply the command based on the way of schedule list.

3.218. show running-config

[Introduction]

Use **show running-config** to show the configuration information of current system.

show running-config

[Parameter]

N/A

[Command Modes]

Privileged EXEC, privileged user

[Usage Guide]

Show the configuration information of current system.'!' stands for explanation. Use command write to write to flash memory.

[Explanation of command execution echo]

N/A

[Example]

Raisecom# ***show running-config***
System current configuration:
!command in view_mode
terminal time-out 65535
!
!command in enable_mode
!
!command in vlan configuration mode
!
!command in port_mode
!
!command in aggregator mode
!
!command in ip interface mode
!
!command in rip_mode
!
!command in ospf_mode
!
!command in config_mode
!

[Related command]

Command	Description
show startup-config	Show system startup information
download	Download system configuration file or startup file.
upload	Upload system configuration file or startup file.
write	Save current system configuration.

3.219. show snmp access

[Introduction]

Use **show snmp access** to show snmp access group information.

show snmp access

[Parameter]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

show snmp access group information.

[Explanation of command execution echo]

N/A.

[Example]

*Raisecom#**show snmp access***

Index: 0
Group: initial
Security Model: usm
Security Level: authnopriv
Context Prefix: --
Context Match: exact
Read View: internet
Write View: internet
Notify View: internet

Index: 2
Group: initialN/A
Security Model: usm
Security Level: noauthnopriv
Context Prefix: --
Context Match: exact
Read View: system
Write View: --
Notify View: internet

[Related command]

Command	Description
snmp-server access	Add or modify access control group.
no snmp-server access	Delete access control group.

3.220. show snmp community

[Introduction]

Use **show snmp community** to show the community information of snmp protocol.

show snmp community

[Parameter]

N/A

[Command Modes]

Privileged EXEC, privileged user

[Usage Guide]

Use show snmp community to show the community information of snmp protocol.

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#**show snmp community***

Index Community Name View Name Permission

---

1 public internet ro

[Related command]

Command	Description
snmp community	Set snmp group information.
show snmp view	Show snmp view information

3.221. show snmp config

[Introduction]

use show snmp **config** command to show the basic config information of snmp.

show snmp config

[Parameter]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Use this command to show the different quantity statistics that is received or sent by SNMP.

[Explanation of command execution echo]

N/A.

[Example]

*Raisecom#**show snmp config***

Contact Information: support@Raisecom.com

Device location : world china raisecom

SNMP trap status: Enable

SNMP EngineID: 800022b603000e5e1a2b3c

[Related command]

Command	Description
snmp-server location	Set location information of snmp
snmp-server contact	Set snmp contact information
snmp-server enable traps	Enable snmp traps

3.222. show snmp group

[Introduction]

Use **show snmp group** to show the map relationship between snmp user and access group.

show snmp group

[Parameter]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Show the map relationship between snmp user and access control group.

[Explanation of command execution echo]

N/A.

[Example]

*Raisecom#**show snmp group***

Index: 0
Group: group1
User Name: guestuser1
Security Model: usm

Index: 1
Group: initialN/A
User Name: raisecomN/A
Security Model: usm

Index: 2
Group: initial
User Name: raisecommd5nopriv
Security Model: usm

Index: 3
Group: initial
User Name: raisecomshanopriv
Security Model: usm

[Related command]

Command	Description
snmp-server group	Add or modify the map relationship from one user to access control group.
no snmp-server group	Delete the map relationship from one user to access control group.

3.223. show snmp host

[Introduction]

Use show snmp host to show the information of target host server.

show snmp host

[Parameter]

N/A

[Command Modes]

Privileged EXEC, privileged user

[Usage Guide]

Use the command to show the ip address of target host server

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#**show snmp host***

Index: 0

IP address: 10.168. 0. 16

Port: 162

User Name: testuser2

SNMP Version: v3

Security Level: authnopriv

TagList: bridge config interface rmon snmp ospf

[Related command]

Command	Description
snmp-server host	Add or modify target host address.
no snmp-server host	Delete target address.

3.224. show snmp statistics

[Introduction]

use **show snmp statistics** to show snmp statistical information.

show snmp statistics

[Parameter]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Use this command to show the quantity statistics that are received and sent by SNMP agent.

[Explanation of command execution echo]

N/A.

[Example]

*Raisecom#**show snmp statistics***

SNMP packets input:162

Unsupported SNMP version SNMP PDUs: 0

Unknown SNMP community name SNMP PDUs: 0

SNMP community not allowed operation SNMP PDUs: 0

ASN.1 or BER errors SNMP PDUs: 0

Too big SNMP PDUs: 0

Name error SNMP PDUs: 0

Bad value SNMP PDUs: 0

ReadOnly SNMP PDUs: 0

GenErrs SNMP PDUs: 0

Get-Request and Get-Next PDUs MIB objects SNMP PDUs: 0

Set-Request MIB objects SNMP PDUs: 0
Get-Request MIB objects SNMP PDUs: 0
Getnext-Request MIB objects SNMP PDUs: 0
Set-Request MIB objects SNMP PDUs: 0
Get-Response PDUs SNMP PDUs: 0
Received Traps SNMP PDUs: 0
SNMP packets output:0
Error name SNMP PDUs: 0
Too big SNMP PDUs: 0
Bad value SNMP PDUs: 0
Gen Errs SNMP PDUs: 0
Get request SNMP PDUs: 0
Get-next SNMP PDUs: 0
Set Request SNMP PDUs: 0
Get Responses SNMP PDUs: 0
Trap SNMP PDUs: 0
Unsupported security level SNMP PDUs: 0
Not in time window SNMP PDUs: 0
Unknown user name SNMP PDUs: 0
Unknown EngineID SNMP PDUs: 0
Wrong Digests SNMP PDUs: 0
Decryption Errors SNMP PDUs: 0

[Related command]

N/A.

3.225. show snmp user

[Introduction]

use **show snmp user** to show snmp user information.

show snmp user

[Parameter]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Show snmp user information.

[Explanation of command execution echo]

N/A.

[Example]

*Raisecom#**show snmp user***
Index: 0
User Name: guestuser1
Security Name: guestuser1
EngineID: 800022b603000e5e1a2b3c
Authentication: MD5
Privacy: NoPriv

Index: 1
User Name: raisecomN/A
Security Name: raisecomN/A
EngineID: 800022b603000e5e1a2b3c
Authentication: NoAuth
Privacy: NoPriv

Index: 2
User Name: raisecommd5nopriv
Security Name: raisecommd5nopriv
EngineID: 800022b603000e5e1a2b3c
Authentication: MD5
Privacy: NoPriv

Index: 3
User Name: raisecomshanopriv
Security Name: raisecomshanopriv
EngineID: 800022b603000e5e1a2b3c
Authentication: SHA
Privacy: NoPriv

[Related command]

Command	Description
snmp-server user	Add or modify user list.
no snmp-server user	Delete a snmp user

3.226. show snmp view

[Introduction]

Use **show snmp view** to show snmp view information.

show snmp view

[Parameter]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Show snmp view information.

[Explanation of command execution echo]

N/A.

[Example]

*Raisecom#**show snmp view***
Index: 0
View Name: system
OID Tree: 1.3.6.1.2.1.1
Mask: --
Type: included

Index: 1

View Name: internet

OID Tree: 1.3.6

Mask: --

Type: included

[Related command]

Command	Description
snmp-server view	Add or modify view
no snmp-server view	Delete view.

3.227. show sntp

[Introduction]

Show the “sntp” information

show sntp

[Parameter]

N/A

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user

[Usage Guide]

Use the history studying information of sntp.

[Explanation of command execution echo]

Show log information

Raisecom#show sntp

SNTP configuration information

SNTP server address:192.168.1.169

SNTP server Stratum Version Last Receive

[Example]

N/A

[Related command]

Command	Description
sntp server	Learn the system time form sntp server.
sntp broadcast client	set the device as detector of sntp broadcast

3.228. show spanning-tree

[Introduction]

Show the global activity status and configuration of spanning-tree.

show spanning-tree

[Command Modes]

Privilege configuration mode; privileged user.

[Usage Guide]

show the activity status and configuration of spanning tree.

[Explanation of command execution echo]

Raisecom#show spanning-tree
RSTP admin state:enabled
Protocol mode: RSTP
bridge ID: 32768-000e5e9c5bf3(proirity-MAC)
Root ID: 32768-000e5e9c5bf3(proirity-MAC)
Root Port: N/A
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
The first line: RSTP protocol status, show whether the RSTP is enabled or not.
The second line: Current running mode of RSTP.
The third line: current bridge ID.
The fourth line: root bridge ID of spanning tree.
The fifth line: root port of current bridge.
The sixth line: the maximum information living time for spanning tree and current bridge.
The seventh line: the hello time and current bridge hello time of the spanning tree.
The eighth line: the time delay for spanning tree status conversion and the time delay for current bridge status conversion.
The ninth line: the maximum BPDU transmission limit per second of current bridge.

[Related command]

Command	Description
spanning-tree	Enable/disable spanning tree protocol
spanning-tree priority	Set the system priority of spanning tree or port priority
spanning-tree forward-delay	Set the forward-delay of spanning-tree protocol.
spanning-tree hello-time	Set the hello-time
spanning-tree transit-limit	Set the maximum transit-limit for each hello time.
spanning-tree mode	Set the RSTP mode of the switch.

3.229. show spanning-tree port

[Introduction]

Show the port activity status and configuration of spanning tree.

show spanning-tree port [portlist]

[Parameter]

portlist port list.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

show the port activity status and configuration of spanning tree.

[Explanation of command execution echo]

Raisecom#show spanning-tree port 1

RSTP Admin State: Enable
Protocol Mode: RSTP
Bridge ID: 32768-000E5E1A2B3C(priority-MAC)
Root ID: 32768-000E5E1A2B3C(priority-MAC)
Root Port: N/A
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:1

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

[Related command]

Command	Description
spanning-tree	Enable/disable port spanning-tree.
spanning-tree priority	Set the system priority and port priority of spanning tree.
spanning-tree path-cost	Set the port expense of spanning tree
spanning-tree link-type	Set the link type for the port of the switch.
spanning-tree edged-port	Configure current Ethernet port to be marginal port.

3.230. show startup-config

[Introduction]

Use **show startup-config** command to show startup configuration information that is saved in the system.

[Parameter]

N/A.

[Command mode]

Privileged EXEC; privileged user.

[Usage Guide]

Use this command to show startup configuration information that is saved in flash system file; use **write** command to save information for the device or to refresh

information by download, or use **erase** command to delete information. Also can save information by uploading.

[Explanation of command execution echo]

N/A.

[Example]

*Raisecom#**show startup-config***

!command in view_mode

!

!command in enable_mode

!

!command in vlan configuration mode

!

!command in port_mode

!

!command in aggregator mode

!

!command in ip interface mode

!

!command in rip_mode

!

!command in ospf_mode

!

!command in config_mode

snmp-server host 20.0.0.1 v2 public udp-port 163snmp

snmp-server host 20.0.0.2 v1 public

!

!NEVER change the NOTATION

!end

[Related command]

Command	Description
show startup-config	Show system startup config information.
download	Download system configuration file or startup file.
upload	Upload system config file or start file.
write	Save current system configuration.
erase	Delete designated file in the system.

3.231. show storm-control

Show the setting for storm-control.

show storm-control

[Parameter]

storm-control storm-control function;

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user exe.

[Usage Guide]

N/A.

[Explanation of command execution echo]

Broadcast: Enable

Multicast: Enable

Unicast destination lookup unsuccessfully (DLF): Enable

Threshold: 1024 pps

[Example]

show the storm-control rule.

Raisecom# ***show storm-control***

[Related command]

Command	Description
storm-control	Set the rule of storm-control
no storm-control	Delete the rule of storm-control

3.232. show svl

[Introduction]

Show the function of shared VLAN.

show svl

[Parameter]

svl Share vlan function(share vlan);

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

SVL: Enable

show above information when set SVL mode.

[Example]

Show current SVL situation.

Raisecom# ***show svl***

[Related command]

command	Description
svl { **enable** | **disable** }	Set start or shut up of shared VLAN mode

3.233. show svl default vlan

[Introduction]

Show default shared vlan.

show svl default vlan

[Parameter]

svl set SVL
default SVL default VLAN
vlan SVL default VLAN

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

SVL default vlan: 1

[Example]

show mirror rule:

Raisecom# ***show svl default vlan***

[Related command]

Command	Description
svl default vlan <1-4094>	Set SVL default shared VLAN
no svl default vlan	Recover default shared VLAN to 1

3.234. show switchport svl vlanlist

[Introduction]

show default share VLAN.

show switchport [<1-26>] svl vlanlist

[Parameter]

switchport port
<1-26> port number
svl set share VLAN
vlanlist share VLAN list.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

port svlVlan
----
1 1-4

[Example]

show mirror rule:

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

[Related command]

Command	Description
switchport svl vlanlist {1-4094}	Set share VLAN list
no switchport svl vlanlist	Delete share VLAN list.

3.235. show tech-support

[Introduction]

Show technical support information, all the information about trouble shooting.

show tech-support

[Parameter]

N/A.

[Default]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

N/A.

[Explanation of command execution echo]

N/A.

[Example]

*Raisecom#**show tech-support***

[Related command]

N/A.

3.236. show terminal

[Introduction]

Use **show terminal** to show system terminal running situation.

show terminal

[Parameter]

N/A.

[Command Modes]

Privileged EXEC; privileged user.

[Usage Guide]

Use this command to check system terminal equipment usage status, including a console and five telnet.

[Explanation of command execution echo]

N/A.

[Example]

*Raisecom#**show terminal***

terminal	*state*	*time-out*	*user*
console	*active*	*600sec*	*Raisecom*
telnet-1	*inactive*	-	-
telnet-2	*inactive*	-	-
telnet-3	*inactive*	-	-
telnet-4	*inactive*	-	-
telnet-5	*inactive*	-	-

[Related command]

N/A.

3.237. show trunk

[Introduction]

Show trunk information, trunk mode and member port of current trunk group and current enabled member port.

Show trunk

[Parameter]

N/A

[Default]

N/A

[Command Modes]

Privileged EXEC; privileged user

[Usage Guide]

This command is used to display the load-sharing mode of all aggregated links, ticket algorithm using mac address, all current aggregation group, group members and current effective member port. The current effective member port is the group member that has “UP” status.

[Explanation of command execution echo]

Trunk: Enable

Loading sharing mode: SXORDMAC

Loading sharing ticket algorithm: --

Trunk Group *Member Ports* *Efficient Ports*

[Example]

Display current trunk related information.

raisecom# ***show trunk***

[Related command]

Command	Description
trunk-group	Create an aggregation group
trunk-loading-sharing mode	Set the load-sharing mode of all aggregated ports
trunk-loading-sharing ticket-generation-algorithm	Set the ticket algorithm by using MAC address

3.238. show user

[Introduction]

Use show user to show the user information stored in system.

show user

[Parameter]

N/A

[Command Modes]

Privileged EXEC; privileged user

[Usage Guide]

Use the command to inspect how many users can login the system. The information of users is stored in usertable.conf. Users can use erase to delete the file to restore default user status.

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#****show user***

User name *priority*

Raisecom *15*

factory *15*

[Related command]

Command	Description
user	Set up the user information
user privilege	Set the privilege of user

3.239. show version

[Introduction]

Use show version to show system version.

[parameter]

N/A

[Command Modes]

privileged configuration mode, privileged user.

[Usage Guide]

Use the command to show the software and system hardware version.

[Explanation of command execution echo]

N/A

[Example]

*Raisecom#**show version***
RaiseCom Operating System Software
Copyright(c) 2001-2003 by Raisecom Science & Technology CO., LTD.

Product name: ISCOM2826
RaiseComOS Software Version 2.1.237.20050117.(Compiled Feb 18 2005, 14:54:07)
Hardware ISCOM2826. Version Rev.A
System MacAddress is :000e.5e11.c34f
ISCOM2826 with
64M bytes DRAM
8 M bytes Flash Memory

Switch uptime is 0 days, 0 hours, 36 minutes

[Related command]

3.240. show vlan

[Introduction]

Show static VLAN configuration information.

show vlan [{1-4094}]

[Parameter]

{1-4094} VLAN list

[Command Modes]

Privileged user; Privileged EXEC.

[Usage Guide]

Show all the static VLAN configuration information, including active and sustained.

[Explanation of command execution echo]

VLAN Name State Ports

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

1 Default active 1-26

2 Cluster-Vlan active 1-26

3 VLAN0003 suspend 1,2,10,20-25

[Related command]

Command	Description
name	Name static VLAN
state	Set active status of static VLAN
show vlan	Show VLAN configuration information.

3.241. shutdown

[Introduction]

Shutdown the physical port, use **no** command to open the port.

shutdown [**schedule-list** list-no]

no shutdown [schedule-list **list-no]**

[Parameter]

Schedule-list: set the starting time, ending time and time period of schedule list.

List-no: schedule list <0-99>.

[Default]

The port is open in default.

[Command Modes]

Ethernet physical interface configuration mode; privileged user

[Usage Guide]

Only users whose priority is 15 can use the command.

[Explanation of command execution echo]

SUCCESS!

Set up successfully

This operation failed!

Set up failed

[Example]

Shut down the physical port

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

Open the physical port

*Raisecom(config-port)# **no-shutdown***

[Related command]

Command	Description
show interface port	show the state of some or all interface port

3.242. snmp-server access

[Introduction]

Add a SNMP access group. **no** command to delete.

Add a SNMP access group

snmp-server access groupname **[read** readview**] [write** writeview**] [notify** notifyview**]** { **v1sm | v2csm** }

snmp-server access groupname **[read** readview**] [write** writeview**] [notify** notifyview**] [**contextname {**exact | prefix**}**] usm** { **noauthnopriv | authnopriv**}

delete a SNMP access group.

no snmp-server access groupname **[context** contextname**] usm** { **noauthnopriv | authnopriv**}

no snmp-server access groupname { **v1sm | v2csm** }

[Parameter]

groupname group name, length should be less 32 characters.
read specify read view.
readview the name of readview, the length should be less than 32 characters.
write specify write view;
writeview the name of writview, length should be less than 32 character.
notify specify general view.
notifyview notify the name of the view, the length should be less than32 characters;
context specify Specify the name of context.
contextname the name of context or prefix, length should be less than 32 characters.
exact contextname fully match context.
prefix contextname match frontal characters of the context.
v1sm (Security Model)SNMPv1
v2csm (Community based Security Model)SNMPv2c
usm (User based Security Model)SNMPv3
noauthnopriv Security level; do not encrypt and distinguish.
authnopriv Security level, distinguish but do not encrypt.

[Default]

Default readview is Internet scope including all the MIB variables in 1.3.6 tree. Default write is empty;default notifyview is Internet. Default context match option is **exact.**

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Set the priority of access group, the relationship between access group and view including the name of access group, security model, security level, write and read notifyview and name matching of context. The general read and write view is the view which is set by **snmp-server view**. When the last option is **exact**, the content name of incoming message should fully match the contextname of access group; when the last option is **prefix,** the contextname of incoming message only need to match the prefix of the context.

When the security is **v1sm** or **v2csm**, security level is **noauthnopriv**.

[Explanation of command execution echo]

Set successfully.
Group name too long!
Read view name too long!
Write view name too long!
Notify view name too long!
Context prefix too long!
Unsupported security model !
Unsupported security level !
Set unsuccessfully !

[Example]

Creat a guestgroup access group, the security mode is usm, the security level is distinguished but not encrypted, readview is mib2, writeview and notifyview are default view.

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

Delete guestgroup

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

[Related command]

Command	Description
show snmp access	Show all the items in the access table.

3.243. snmp-server community

[Introduction]

SNMP community strings authenticate access to MIB objects and function as embedded passwords.

snmp-server community community-name [view view-name] { **ro** | **rw** }

no snmp-server community community-name

[Command Format]

[no] snmp-server community *community-name* [view *view-name*] { **ro** | **rw** }

[Parameter]

community-name	community name, string, less than 32
view *view-name*	view name, less than 32
ro	Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
rw	Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings

[Default]

Community name is public; view name is internet.

[Command Modes]

Global configuration mode; privileged user mode

[Usage Guide]

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the network management system to access the switch, the community string definitions on the NMS must match at least one of the three community string definitions on the switch.

[Explanation of command execution echo]

Set successfully!

Set community name successfully

Community name is too long(less than 32)

The entered community name is longer than 32

View name is too long(less than 32)

The entered view name is longer than 32

No so many space for create community (less equal 8)

There are already 8 communities

Set fail!

Set community name failed

[Example]

Define community raisecom,the relative default view is internet,priority is read and write.

Raisecom(config)# snmp-server community raisecom rw

Define community guest,the default view is mib2,read-olny priority.

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

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

[Related command]

Command	Description
snmp-server view	Set a view.
show snmp community	show SNMP community information
show snmp view	Show SNMP view information

3.244. snmp-server contact

[Introduction]

Configure the network administrator contact information.

[no] snmp-server contact sysContact

[Command Format]

[no] snmp-server contact *sysContact*

[Parameter]

sysContact the contact information of network administrator, character string type.

[Default]

The default contact information is mailto:support@Raisecom.com

[Command Modes]

Global configuration mode; privileged user mode

[Usage Guide]

The information includes the contact information of network administrator, so when help is needed, please refer this information for help.

[Explanation of command execution echo]

Set successfully!

Set up successfully

Set fail!

Set up failed

[Example]

Set up the contact information to service@raisecom.com

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

[Related command]

Command	Description
show snmp contact	Show the contact information of network administrator.

3.245. snmp-server enable traps

[Introduction]

Enable the trap function of SNMP

[Command Format]

[no] snmp-server enable traps [**snmp** | **if** | **ospf** |**lacp** |**stp**]

[Parameter]

N/A

[Default]

Enabled.

[Command Modes]

Global configuration mode; privileged user mode

[Usage Guide]

The switch will send notifications to SNMP managers when particular events occur if SNMP-server enables trap function.

[Explanation of command execution echo]

Set successfully!

Set up successfully

Set fail!

Set up failed

[Example]

Enable trap of ospf

Raisecom(config)# ***snmp-server enable traps ospf***

[Related command]

Command	Description
snmp-server host	set server of trap

3.246. snmp-server group

[Introduction]

Add or delete the mapping relationship of a user and access group. no command is used to delete.

[no] snmp-server group groupname **user** username { **v1sm | v2csm | usm**}

[Parameter]

groupname group name, the length is less than 32 characters.

user specify user name.

username username, the length should be less than 32 characters.

v1sm （Community based Security Model）SNMPv1

v2csm （Community based Security Model）SNMPv2c

usm （User based Security Model）SNMPv3

[Default]

N/A.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

A user will belong to an access group according to safety model, and different access group users have different access priviledge

[Explanation of command execution echo]

Set sucessfully

Group name too long!

User name too long!

Unsupported security model!

Set unsuccessfully !

[Example]

map guestuser1 with the security usm level to guestgroup.

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

Delete the maping from guestuser1 to guestgroup.

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

[Related command]

Command	Description
show snmp group	Display all the items in the mapping table

3.247. snmp-server host

[Introduction]

Add or delete an IP address of trap target.

Add a SNMP target host server address:

snmp-server host A.B.C.D version {1|2c} NAME [**udpport** <1-65535>] [bridge] [config] [interface] [rmon] [snmp] [ospf]

snmp-server host A.B.C.D version 3 { noauthnopriv | authnopriv } NAME [**udpport** <1-65535>] [bridge] [config] [interface] [rmon] [snmp] [ospf]

delete a SNMP target host server address.

no snmp-server host A.B.C.D

[Command Format]

[no] snmp-server host *ip-address* [*host-name*] [udp-port *port-id*]

[Parameter]

addrname host server address name, length should be less than 32 characters.

paramsname the parameter name of host server, used to select parameter, length should be less than 32 characters.

A.B.C.D trap target host IP address, point decimal.

Version the SNMP version which is used by target host.

1 use SNMPv1

2c use SNMPv2c

3 use SNMPv3\n

authnopriv authentic but not privacy

n. individual but can not be interrupted, privacy.

noauthnopriv neither authentic nor privacy.

NAME SNMPv1/v2c group name or SNMPv3 use name.

udpport specify UDP port.

<1-65535> host address receive the udp port number of trap, range is 1-65525.

bridge bridge trap;

config config trap;

interface interface trap;

rmon rmon trap;

snmp snmp trap;

ospf ospf trap.

[Default]

The default UDP port is set to 162; taglist is all the trap.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Add or delete a target host address.

[Explanation of command execution echo]

Set successfully

User name is too long !

If the user name is longer than 32 characters, display above information.

The input IP address is wrong!

Set unsuccessfully !

[Example]

Add a host address of host_1, ip address is 172.20.21.1, username is Raisecom, SNMP version is v3, authentic but not privacy, all the traps.

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

Delete host address-host_1

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

[Related command]

Command	Description
show snmp host	Show all the information in the host address table.

3.248. snmp-server location

[Introduction]

Set the description of switch physical location.

[Command Format]

[no] snmp-server location *sysLocation*

[Parameter]

sysLocation define the physical location of switch

[Default]

No location description

[Command Modes]

Global configuration mode; privileged user mode

[Usage Guide]

Provide

The physical location of the Switch can be viewed for the convenience of network administrators the locate it.

[Explanation of command execution echo]

Set successfully!

Set fail!

[Example]

Set the position of switch as HaiTaiEdifice8th

*Raisecom(config)# **snmp-server location** HaiTaiEdifice8th*

[Related command]

Command	Description
show snmp location	Show the physical position information of switch

3.249. snmp-server user

[Introduction]

Add a new user. No command to delete the operation.

Add a SNMP user.

snmp-server user username [**remote** engineid] **authentication**{**md5** | **sha**} authpassword

snmp-server user username [**remote** engineid]

delete a SNMP user.

no snmp-server user username [**remote** engineid]

[Parameter]

username username, length should less than 32 characters.
remote remote SNMP engine ID;
engineid remote SNMP engine ID. The SNMP engine ID by which username can contact it.
authentication Specify authentication algorithm.
md5 Use authentication algorithm md5;
sha Use authentication algorithm sha;
authpassword authentication password.

[Default]

Default situation is that there are no authentication and no privacy; the authentication password and authentication algorithm have to be selected beforehand;default SNMP engine ID is local engine ID.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Add or delete a user.

[Explanation of command execution echo]

Set sucessfully
Engine ID is too long!
Input engine ID is wrong!
Failed to get local engine ID!
Authentication key is wrong!

Set unsuccessfully !

[Example]

add a user guestuser1, local engine ID; md5 authentication algorithm, authentication password is Raisecom; no privacy.
*Raisecom(config)#**snmp-server user** guestuser1 **authentication md5** raisecom*
Add a user guestuser3, local engine ID; no authentication and no privacy.
*Raisecom(config)#**snmp-server user** guestuser2*
Delete user guestuser3, local engine is ID:
*Raisecom(config)#**no snmp-server user** guestuser2*

[Related command]

Command	Description
show snmp user	Show all the items in the user table.

3.250. snmp-server view

[Introduction]

add a SNMP view, no command to delete the operation.

Add a snmp view.

snmp-server view view-name oid-tree [mask] {**included | excluded**}

delete a SNMP view.

no snmp-server view view-name oid-tree

[Command Format]

[no] snmp-server view *view-name oid-tree* {**included | excluded**}

[Parameter]

view-name View name, length is below 32.
oid-tree OID number, length is below 128
mask- OID tree mask, length is below 128, format is OID format, OID option can only be 0 or 1.
included MIB variable in OID tree.
excluded MIB variable out of OID tree.

[Default]

All the numbers of mask are 1.

[Command Modes]

Global configuration mode; privileged user mode

[Usage Guide]

SNMPv3 defines access mode based on view. Users can use the command to define a view. Mask is the mask of OID subtree, each of its digit corresponding to each option of its tree. If particular digit of the mask is 1, view should according to subtree corresponding option; if particular digit of the mask is 0, then it is not needed to match the subtree corresponding option. The mask length is 16 characters, that is too say it support the subtree with length 128.

[Explanation of command execution echo]

Set successfully
Name too long !
Oid tree Name NOT correct !
mask too long!
Mask NOT correct !
View internet:1.3.6 should NOT be deleted!
Set unsuccessfully!

[Example]

The following example display how to configure SNMP view:
Create view mib 2, view includes all the MIB variables under 1.3.6.1.2.1
*Raisecom(config)#**snmp-server view** mib2 1.3.6.1.2.1 1.1.1.1.0.1 **included***
Delete view mib2, subtree is 1.3.6.1.2.1.
*Raisecom(config)# **no snmp-server view** mib2 1.3.6.1.2.1*

[Related command]

Command	Description
show snmp view	Show all the information SNMP view table.

3.251. sntp master

NOT AVAILABLE FOR: RC2016/2008/2126/2026.

[Introduction]

Start SNTP server function in the switch. **no** command is used to stop.

[no] sntp master

[Parameter]

N/A.

[Default]

Disable.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Add its system time to client after getting the request from client.

[Explanation of command execution echo]

Start SNTP server successfully!

[Example]

configure itself to sntp server.

*Raisecom(config)#**sntp master***

[Related command]

N/A.

3.252. sntp server

[Introduction]

Configure the IP address of SNTP server and switch will set system according to the server.

sntp server A.B.C.D [**schedule-list** list-no]

[Parameter]

A.B.C.D IP address of sntp server.

schedule-list Set the starting time, ending time and periodical operation task.

list-no schedule list range is<0-99>;

[Default]

Disabled.

[Command Modes]

Global configuration mode; privileged user

[Usage Guide]

Configure the IP address of SNTP server and switch will set system according to the server

[Explanation of command execution echo]

set successfully!

set fail!

[Example]

Raisecom(config)#sntp server 10.0.0.1

[Related command]

3.253. spanning-tree

[Introduction]

Enable or disable spanning tree（802.1W Rapid Spanning Tree Protocol）

spanning-tree {**enable** | **disable**} [**schedule-list** list-no]

[Parameter]

enable Enable spanning tree;

disable Disable spanning tree.

schedule-list Set the starting time, ending time and time interval of periodical operation task.

list-no schedule list range is <0-99>;

[Default]

Enable.

[Command mode]

Global configuration mode or Physical port configuration mode; privileged user.

[Usage Guide]

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations.

Raisecom series switch supports both STP and RSTP, please choose the mode you need and configure the relative parameters such as forward-delay, hello-time, path cost, edged port (RSTP) and etc.

This command can be used in both global configuration mode and physical port configuration mode.

[Explanation of command execution echo]

Set successfully.
Set unsuccessfully.

[Example]

Globally disable spanning tree protocol.
Raisecom(config)# spanning-tree disable
Globally enable spanning tree protocol.
Raisecom(config)# spanning-tree enable
Under physical interface configuration mode, enable spanning tree protocol on the port.
Raisecom(config-port)# spanning-tree disable

[Related command]

Command	Description
show spanning-tree	Show global active state and configuration information of spanning tree.

3.254. spanning-tree clear statistics

[Introduction]

Clear RSTP statistical information.

spanning-tree clear statistics

[Parameter]

N/A.

[Command Modes]

Physical interface/port range configuration mode; privileged user.

[Usage Guide]

Use this command to clear statistical information on designated port.

[Explanation of command execution echo]

Set successfully.
Set unsuccessfully.

[Related command]

Command	Description
show spanning-tree port	Show the port active status and configuration information of spanning tree.

3.255. spanning-tree edged-port

[Introduction]

Configure current Ethernet port as edged-port.

[no] spanning-tree edged-port

[Parameter]

N/A.

[Default]

No Ethernet port is configured as edged-port.

[Command Modes]

Physical port/ port range configuration mode; privileged user.

[Usage Guide]

spanning-tree edged-port command is used to configure current Ethernet port to be edged-port.

no spanning-tree edged-port is used to recover the current Ethernet port to default status, that is non edged-port.

If current Ethernet port is connected to other switch, please use **no spanning-tree edged-port** command to specify it to non edged-port.

Use **spanning-tree edged-port** to specify the Ethernet port which directly connected to PC to be edged-port.

If you configure a port as edge port on an RSTP switch, the edge port immediately transitions to the forwarding state. So please enable it only on ports that connects to a single end station.

[Explanation of command execution echo]

Set successfully.
Set unsuccessfully.

[Related command]

Command	Description
show spanning-tree port	Show the port active status and configuration information of spanning tree.

3.256. spanning-tree forward-delay

[Introduction]

set the forward-delay of spanning tree,

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:

spanning-tree forward-delay <4-30>

no spanning-tree forward-delay

[Parameter]

<4-30> The time delay of spanning tree protocol bridge port status conversion, unit is second.

[Default]

15 seconds.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

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.

[Explanation of command execution echo]

Set successfully.
Set unsuccessfully.

[Example]

set the value of forward-delay to 10 seconds:
Raisecom(config)# ***spanning-tree forward-delay*** *10*

[Related command]

Command	Description
show spanning-tree	Show the active status and configuration information of spanning tree
spanning-tree	Enable/disable spanning tree protocol
spanning-tree priority	Set the system priority or port priority of spanning tree.
spanning-tree forward-delay	Set the forward-delay of spanning tree.
spanning-tree hello-time	Set the hello-time of spanning tree.
spanning-tree path-cost	Set the port expense of spanning tree.

3.257. spanning-tree hello-time

[Introduction]

You can configure the interval between the generation of configuration messages by the root switch by changing the hello time.

spanning-tree hello-time <1-10>

no spanning-tree hello-time

[Parameter]

<1-10> The time interval of time-lapse sending bridge configuration information. Unit is second.

[Default]

2 seconds.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

You can configure the interval between the generation of configuration messages

[Explanation of command execution echo]

Set successfully.
Set unsuccessfully.

[Example]

Set the hello-time of spanning tree to 3 seconds.
Raisecom(config)# ***spanning-tree hello-time*** *3*
Set the hello-time of spanning to the default value, that is 2 seconds.
Raisecom(config)# ***no spanning-tree hello-time***

[Related command]

Command	Description

show spanning-tree	Show the active status and configuration information of spanning tree
spanning-tree	Enable/disable spanning tree protocol
spanning-tree priority	Set the system priority or port priority of spanning tree.
spanning-tree forward-delay	Set the forward-delay of spanning tree.
spanning-tree max-age	Set the max-age of spanning tree.
spanning-tree path-cost	Set the port expense of spanning tree.

3.258. spanning-tree link-type

[Introduction]

Set the RSTP link type of switch port.

spanning-tree link-type {**point-to-point** | **shared**}

no spanning-tree link-type

[Parameter]

point-to-point set the RSTP link type as point-to-point.

shared set the type of link to shared.

[Default]

By default, switch set link type as point-to-point in full-duplex mode, as shared link in half-duplex mode.

[Command Modes]

Physical port/port range configuration mode; privileged user.

[Usage Guide]

User can use this command to change the default setting of RSTP link type. Example: half-duplex port use point-to-point mode to connect the RSTP switch, if the port is set to point-to-point, then this port can change its state quickly.

[Explanation of command execution echo]

Set successfully.
Set unsuccessfully.

[Related command]

Command	Description
show spanning-tree port	Show port active status and configuration information of spanning tree.

3.259. spanning-tree max-age

[Introduction]

Set maximum aging time of spanning tree.

spanning-tree max-age <6-40>

no spanning-tree max-age

[Parameter]

<6-40> The maximum aging time of spanning tree configuration information, unit is second.

[Default]

The maximum age is 20 seconds.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

The maximum aging time is the number of seconds a switch waits without receiving spanning-tree configuration messages before attempting a reconfiguration.

[Explanation of command execution echo]

Set successfully.
Set unsuccessfully.

[Example]

set the max-age of spanning tree to 30 seconds.
Raisecom(config)# ***spanning-tree max-age*** *30*
set the max-age of spanning tree to 20 seconds.
Raisecom(config)# ***no spanning-tree max-age***

[Related command]

Command	Description
show spanning-tree	Show the active status and configuration information of spanning tree
spanning-tree	Enable/disable spanning tree protocol
spanning-tree priority	Set the system priority or port priority of spanning tree.
spanning-tree forward-delay	Set the forward-delay of spanning tree.
spanning-tree hello-time	Set the hello-time of spanning tree.
spanning-tree path-cost	Set the port expense of spanning tree.

3.260. spanning-tree mcheck

[Introduction]

Force the port as RSTP mode.

spanning-tree mcheck

[Parameter]

N/A

[Default]

N/A.

[Command Modes]

Physical port/range configuration mode; privileged user.

[Usage Guide]

When the network is stable, though the bridge which runs STP is disconnected, the port of running switch which runs RSTP still runs under the STP mode, under this situation, user can use **spanning-tree mcheck** command to set mCheck variable to force the port moving to RSTP mode. If the port is moved to RSTP mode, when the port get the new STP packet, port will back to STP mode again.

Only when the RSTP switch is working under global RSTP mode, user can use this command. If the RSTP switch is working under global STP mode, the command is not available.

批注 [l1]: 不知所云

[Explanation of command execution echo]

Set successfully.
Set unsuccessfully.

[Related command]

Command	Description
show spanning-tree port	Show the port activity status of spanning tree and configuration information.

3.261. spanning-tree mode

[Introduction]

Set the switch in STP or RSTP mode.

spanning-tree mode {stp|rstp}

[Parameter]

stp STP mode.

rstp RSTP mode.

[Default]

RSTP running mode is rstp.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

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.

Under RSTP mode switch sends RST BPDU. If the connected switch port is running STP protocol, port will change to STP compatible mode.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Related command]

Command	Description
show spanning-tree	Show the activity status and configuration information of spanning tree.

3.262. spanning-tree path-cost

[Introduction]

set the path cost of spanning tree.

spanning-tree path-cost <0-200000000>

no spanning-tree path-cost

[Parameter]

Path-cost is used to identify the path-cost, range form 0-200000000. Under the default situation, the bridge gets the path-cost is derived from the media speed of an interface.

[Default]

Generally speaking, the port path-cost should based on their physical characteristic, default situation as following:

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

[Command Modes]

Physical port/ port range configuration mode; privileged user.

[Usage Guide]

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.

[Explanation of command execution echo]

Set successfully.
Set unsuccessfully.

[Example]

Raisecom(config-port)# spanning-tree path-cost 100000

[Related command]

Command	Description
show spanning-tree port	Show the port activities status and configuration information of spanning tree.

3.263. Spanning-tree priority

[Introduction]

If a loop occurs, spanning tree uses the system/port priority when selecting a switch/interface to put into the forwarding state.

spanning-tree priority <0-61440>

no spanning-tree priority

[Parameter]

<0-61440> is used to identify bridge priority, this value is not continuous, range is 0~61440, step is 4096.

[Default]

The system priority is 32768.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

If a loop occurs, spanning tree uses the port priority when selecting an interface to put into the orwarding 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.

[Explanation of command execution echo]

Set successfully.
Set unsuccessfully.

[Example]

Set the spanning tree protocol system priority or port priority to 10.

*Raisecom(config)# **spanning-tree priority** 10*

[Related command]

Command	Description

show spanning-tree	Show the activities status and configuration information of spanning tree.

3.264. spanning-tree priority

[Introduction]

Set the port priority of spanning tree.

spanning-tree priority priority

no spanning-tree priority

[Parameter]

priority port priority of spanning tree, this value is discontinuous, range is 0-240, step is 16.

[Default]

Spanning tree port default priority is 128.

[Command Modes]

Physical port/port range configuration mode; privileged user.

[Usage Guide]

If a loop occurs, spanning tree uses the port priority when selecting an interface to put into the orwarding 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.

[Explanation of command execution echo]

Set successfully.
Set unsuccessfully.

[Example]

set the spanning tree port priority to 100:
*Raisecom(config-port)# **spanning-tree priority** 100*

[Related command]

command	description
show spanning-tree port	Show port activities status and configuration information.

3.265. spanning-tree transit-limit

[Introduction]

Set the maximum limitation for transiting packet within hello time, range is 1~10. Under default situation, the maximum sending speed is 3.

spanning-tree transit-limit packet-number

no spanning-tree transit-limit

[Parameter]

Packet-number used to set the maximum number of packets that can send BDPU within Hello Time. Under default situation, each hello time can sent 3 BPDU.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

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.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Related command]

Command	description
show spanning-tree	Show the activities status and configuration information.

3.266. Speed

[Introduction]

Use this command to set rate and mode of physical port.

speed { **10** | **100 | 1000** } **duplex** { **full-duplex** | **half-duplex** }

[Parameter]

10	speed is 10Mbps
100	speed is 100Mbps
1000	the speed the 1000Mbps
duplex	duplex mode
full-duplex	full duplex
half-duplex	half duplex

[Default]

The port speed is auto-negotiate in default.

The duplex mode is auto-negotiate in default.

带格式的：项目符号和编号

[Command Modes]

Ethernet interface configuration mode; privileged user

[Usage Guide]

Only users whose priority is 15 can use the command.

[Explanation of command execution echo]

SUCCESS!

This operation failed!

[Example]

Set up the physical port 4 to 1000Mbps half duplex

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

Command	description
show interface port	Show particular or all the port status.

3.267. State

[Introduction]

Set the active state of static VLAN

state {**active** | **suspend**}

[Parameter]

active	Set static VLAN active
suspend	Set static VLAN suspend

[Default]

Suspended by default.

[Command Modes]

The configuration exec of static VLAN; privileged user

[Usage Guide]

All the configuration of static VLAN is enabled when VLAN is active. When static VLAN is suspend, users can configure it, such as delete/add port, set the VLAN name, system will remain the configuration. Once the VLAN is active, the configuration will work in system

[Explanation of command execution echo]

Set successfully.
Set fail.
Default vlan is always active.

[Example]

Set VLAN 2 active,exit VLAN configuration mode;
Raisecom(config-vlan)# ***state active***
Raisecom(config-vlan)# ***exit***
Raisecom(config)#

[Related command]

Command	Description
vlan	enter the configuration mode of static VLAN
name	Set the name of static VLAN
shutdown	enable/disable the configuration of static VLAN
pvid	Set the priority of port VLAN ID
vlan-access	set the access priority of VLAN
show vlan static	show the configuration information of static VLAN
show vlan current	show the configuration information of current active VLAN

3.268. statistic packet

ONLY AVAILABLE FOR:ISCOM2026

[Introduction]

Set the type of statistical packet.

statistic packet ingress {good |bad |local} egress {good |bad |abort}

[Parameter]

good received good packet.
bad received bad packet.
local received local packet.
good sent good packet.
bad sent bad packet. (Example:resending the packet due to confliction);
abort aborted packet（Example: to much confliction leading to aborted packets）.

[Default]

Calculate received good packet and sent good packet.

[Command Modes]

Physical Physical port configuration mode; privileged user.

[Usage Guide]

Only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Set successfully
Set unsuccessfully!

[Example]

Let the port calculate received bad packet and sent good packet.
Raisecom(config-port)# statistic packet ingress bad egress good

[Related command]

Command	Description
show interface port [<1-26>] statistics	Show port statistical information.

3.269. storm-control

Multicast, DLF NOT AVAILABLE FOR: RC2126/2026

[Introduction]

Enable or disable port storm control function.

storm-control {**broadcast | multicast | dlf | all** } {**enable** | **disable**} [**schedule-list** list-no]

[Parameter]

broadcast broadcast packet.
multicast multicast packet.
dlf target searching failure packet;
all broadcast packet, multicast packet and dlf;
enable enable storm control function.
disable disable storm control function.
schedule-list Set the starting time, ending time and time interval of the schedule.
list-no schedule list range is <0-99>;

[Default]

Default situation: storm control function enable.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Set successfully
Set unsuccessfully !

[Example]

enable broadcast storm-control function.
*Raisecom(config)# **storm-control broadcast enable***
disable all the storm-control function
*Raisecom(config)# **storm-control all disable***

[Related command]

Command	Description
show storm-control	Show storm control function setting of all or particular packet

3.270. storm-control bps

NOT AVAILABLE FOR:ISCOM3026/2826/2126/2016/2008/2026/2826E

[Introduction]

Set the valve value for broadcast packet, multicast packet, and dlf, unit is bit/second.

storm-control bps bit-number [**schedule-list** list-no]

[Parameter]

bps Broadcast control function valve.
bit-number the number of bit limitation which storm packet allow to pass each second.
schedule-list set the starting time, ending time, and time interval of schedule.
list-no schedule list number range is <0-99>;

[Default]

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Set successfully
Set unsuccessfully !

[Example]

every second 200 bit can pass.
Raisecom(config)# ***storm-control bps*** *5000*

[Related command]

Command	Description
show storm-control	Show storm control setting for all or particular packet.

3.271. storm-control pps

NOT AVAILABLE FOR:RC2126/2016/2008/2026

[Introduction]

Set the storm control valve value for broadcast packet, multicast packet and dlf packet, unit is packet/second.

storm-control pps packets-number [**schedule-list** list-no]

[Parameter]

pps storm control valve value;
packets-number range is 0-262143;
schedule-list set the starting time, ending time and time interval of schedule.
list-no schedule list number range is <0-99>;

[Default]

The default pps limitation is 1024

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Set successfully
Set unsuccessfully !

[Example]

Set the broadcast quantity is 5000.
Raisecom(config)# ***storm-control pps*** *5000*

[Related command]

Command	Description
show storm-control	Show broadcast storm control setting for all or

	particular packet.

3.272. storm-control ratio

NOT AVAILABLE FOR:ISCOM3026/2826/2826E;RC2126/2026 do not support burst.

[Introduction]

Set the storm control pps for broadcast packet, multicast packet and dlf packet, unit is %.

storm-control ratio <1-100> **[** <0-512> **]** [**schedule-list** list-no]

[Parameter]

ratio storm-control ratio;
1-100 ratio of broadcast packet over bandwidth, the real setting is 3,5,10,20 near to the lower bound.
0-512 burst out value, unit is KBps.
schedule-list set the starting time, ending time and time interval of schedule.
list-no schedule list range is <0-99>;

[Default]

Default value is 3; burst value is 0.

[Command Modes]

Global configuration mode; privileged user.

[Example]

Only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Set successfully
Set unsuccessfully !

[Example]

Set storm-control ration to 10, burst out value to 64.
*Raisecom(config)# **storm-control ratio** 10 64*

[Related command]

Command	Description
show storm-control	Show the storm-control function settings of particular or all the ports.

3.273. svl

[Introduction]

Enable/disable shared VLAN mode.

svl { **enable** | **disable** } [**schedule-list** list-no]

[Parameter]

enable enable SVL function
disable disable SVL function
schedule-list set the starting time, ending time and time interval of schedule.
list-no schedule list range is <0-99>;

[Default]

SVL function is “disabled” in default.

[Command Modes]

Physical interface configuration mode of Ethernet; privileged user (priority 15)

[Usage Guide]

Only users whose priority is 15 can use the command.

[Explanation of command execution echo]

SUCCESS!
This operation failed!
This port has been in svl mode!
The echo shows when set the port that is already SVL mode
This port has not been in svl mode!
The echo shows when try to shutdown SVL at non-SVL port

[Example]

Enable the SVL at Port 5

rc2126(config-port)# ***svl enable***

Disable the SVL at Port 5

rc2126(config-port)# ***svl disable***

[Related command]

Command	Description
show svl	show the configuration information of shared VLAN function.

3.274. svl default vlan

[Introduction]

Set default shared VLAN, no command used to recover default setting.

svl default vlan <1-4094>

no svl default vlan

[Parameter]

default SVL default VLAN
vlan SVL default VLAN
<1-4094> SVL default VLAN number;

[Default]

Shared VLAN is 1.

[Command Modes]

Global configuration mode; privileged user. (Priority 15)

[Usage Guide]

Only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Set successfully
Set unsuccessfully !

[Example]

set default shared VLAN to 2.

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

recover default shared VLAN to 1.

Raisecom(config)# ***no svl default vlan***

[Related command]

Command	Description
show svl default vlan	Show default VLAN

3.275. switchport access vlan

[Introduction]

Set the ACCESS VLAN ID for the port.

switchport access vlan <1-4094>

no switchport access vlan

[Parameter]

<1-4094> Specify the ACCESS VLAN ID when port is set to ACCESS、EXTEND-ACCESS、DOT1Q-TUNNELmode. To UNTAG packet, use this value to mark TAG, port will give up TAG when transmit VLAN.

[Default]

Default value is 1.

[Command Modes]

Ethernet physical port interface/ port range configuration mode; privileged user.

[Explanation of command execution echo]

Set unsuccessfully on port PORTID!
Set successfully.

[Usage Guide]

Specify the ACCESS VLAN ID when port is set to ACCESS、EXTEND-ACCESS、DOT1Q-TUNNELmode. To UNTAG packet, use this value to mark TAG, port will give up TAG when transmit VLAN.

User can use no switchport access vlan command to recover default setting.

[Example]

Set ACCESS VLAN ID of the port to 3.

*Raisecom(config-port)# **switchport access vlan** 3*

Recover ACCESS VLAN.

*Raisecom(config-port)#**no switchport access vlan***

[Related command]

Command	Description
switchport hybrid allowed vlan	Set allowable VLAN when port is set to HYBRID mode.
switchport hybrid untagged vlan	Set allowable UNTAG VLAN when port is set to HYBRID mode.
switchport mode	Set the VLAN mode of the port.
switchport native vlan	Set the NATIVE VLAN when port is set to HYBRID or TRUNK mode.
switchport trunk allowed vlan	Set the allowable VLAN when port is set to TRUNK mode.
show interface port portlist **switchport**	Set port relevant VLAN setting.

3.276. switchport hybrid allowed vlan

[Introduction]

set the allowed vlan when port is HYBRID mode.

switchport hybrid allowed vlan {all | {1-4094}**}**

no switchport hybrid allowed vlan

[Parameter]

all all VLAN;
{1-4094} VLAN list;

[Default]

Only allow default VLAN 1 and cluster VLAN 2 pass.

[Command Modes]

Ethernet physical Physical port configuration mode; privileged user.

[Explanation of command execution echo]

Set unsuccessfully on port PORTID!

Set successfully.

[Usage Guide]

Set the allowed VLAN when port is set to HYBRID mode.

User can user **no switchport hybrid allowed vlan** command to recover default setting.

[Example]

set the allowed VLAN 2,3,100 when port is set to HYBRID mode.

*Raisecom(config-port)# **switchport hybrid allowed vlan** 2-3,100*

recover default setting.

*Raisecom(config-port)#**no switchport hybrid allowed vlan***

[Related command]

Command	description
switchport access vlan	Set the ACCESS VLAN ID of the port
switchport hybrid untagged vlan	Set the UNTAG VLAN when port is set to HYBRID mode.
switchport mode	Set port VLAN mode.
switchport native vlan	Set the NATIVE VLAN when port is set to HYBRID or TRUNK mode.
switchport trunk allowed vlan	Set the allowed VLAN when port is set to TRUNK mode.
show interface port portlist **switchport**	Set port relevant VLAN configuration.

3.277. switchport hybrid untagged vlan

[Introduction]

Set the allowed vlan when port is HYBRID mode.

switchport hybrid untagged vlan {all | {1-4094}**}**

no switchport hybrid untagged vlan

[Parameter]

all all VLAN;

{1-4094} VLAN list;

[Default]

N/A.

[Command Modes]

Ethernet physical port / port range configuration mode; privileged user.

[Explanation of command execution echo]

Set unsuccessfully on port PORTID!

Set successfully.

[Usage Guide]

Set the allowed UNTAGGED VLAN when port at HYBRID mode.

User can use **no switchport hybrid untagged vlan** command to recover default setting.

[Example]

set the allowed UNTAG VLAN 2,3,100 when port is HYBRID mode.

*Raisecom(config-port)# **switchport hybrid untagged vlan** 2-3,100*

recover to default setting.

*Raisecom(config-port)#**no switchport hybrid untagged vlan***

[Related command]

Command	Description
switchport access vlan	Set ACCESS VLAN ID of the port
switchport hybrid allowed vlan	Set the allowed VLAN when port is HYBRID mode.
switchport mode	Set the VLAN mode of the port
switchport native vlan	Set the NATIVE VLAN when port is HYBRID or TRUNK mode.
switchport trunk allowed vlan	Set the allowed VLAN when port is TRUNK mode.
show interface port portlist **switchport**	Set VLAN setting for the port.

3.278. switchport mode

dot1q-tunnel mode NOT AVAILABLE FOR: ISCOM2826/2126/2016/2008/2026

[Introduction]

Set the VLAN mode for the port.

switchport mode {access|hybrid|trunk}

no switchport mode

[Parameter]

access ACCESS mode, set port as UNTAG mode to sole VLAN.
hybrid HYBRID mode, set the port as UNTAG or TAG mode to several VLAN.
trunk TRUNK mode, set the port as TAG mode to several VLAN, as UNTAG mode in several Native vlan.

[Default]

all the port default as EXTEND-ACCESS mode in VLAN 1.

[Command Modes]

Ethernet physical Physical port configuration mode; privileged user.

[Explanation of command execution echo]

Set unsuccessfully on port PORTID!
Set successfully.

[Usage Guide]

When the port of the switch is connected to the end users, port can be set to ACCESS mode; port can be set to EXTEND-ACCESS mode when port is cascade mode but it isolated from other VLAN, and it can transmit default vlan and cluster vlan packet, port can be set to DOT1Q-TUNNELmode when switch port is the ingress port of Q-in-Q network; port can be set to HYBRID mode when user want to set the VLAN hybrid mode of the port; when the port of switch is set to uplink TAG port, set it to TRUNK mode.

User can use no switchport mode to recover default setting.

[Example]

When the port VLAN mode is set to ACCESS mode;
*Raisecom(config-port)# **switchport mode access***
Recover port VLAN mode;
*Raisecom(config-port)#**no switchport mode***

[Related command]

Command	description
switchport access vlan	Set the ACCESS VLAN ID of the port
switchport hybrid untagged vlan	Set the UNTAG VLAN when port is set to HYBRID mode.
switchport hybrid allowed valn	Set the allowed vlan when port is HYBRID mode.
switchport native vlan	Set the NATIVE VLAN when port is set to HYBRID or TRUNK mode.
switchport trunk allowed vlan	Set the allowed VLAN when port is set to TRUNK mode.
show interface port portlist **switchport**	Set port relevant VLAN configuration.

3.279. switchport native vlan

[Introduction]

Set allowed VLAN when port is HYBRID mode.

switchport native vlan <1-4094>

no switchport native vlan

[Parameter]

<1-4094> local VLAN;

[Default]

default situation.

[Command Modes]

Ethernet physical Physical port configuration mode; privileged user.

[Explanation of command execution echo]

Set unsuccessfully on port PORTID!
Set successfully.

[Usage Guide]

set the NATIVE VLAN when port is set to HYBRID or TRUNK mode, use NATIVE VLAN mark to enter port UNTAG packet, delete the mark for the packet for port egress NATIVE VLAN.

Use **no switchport native vlan** command to recover default setting.

[Example]

Set the NATIVE VLAN to 3 when port is set to HYBRID or TRUNK mode.
*Raisecom(config-port)# **switchport native vlan** 3*
Recover default setting.
*Raisecom(config-port)#**no switchport native vlan***

[Related command]

Command	description
switchport access vlan	Set the ACCESS VLAN ID of the port
switchport hybrid untagged vlan	Set the UNTAG VLAN when port is set to HYBRID mode.
switchport hybrid allowed valn	Set the allowed vlan when port is HYBRID mode.
switchport native vlan	Set the NATIVE VLAN when port is set to HYBRID or TRUNK mode.
switchport trunk	Set the allowed VLAN when port is set to TRUNK mode.

allowed vlan	
show interface port portlist **switchport**	Set port relevant VLAN configuration.

3.280. switchport protect

NOT AVAILABLE FOR:ISCOM3026/2826/2126/2026/2826E

[Introduction]

Set the port to protect port, no command to delete port protection.

switchport protect [**schedule-list** list-no]

no switchport protect [schedule-list **list-no]**

[Parameter]

protect protect port;
schedule-list set the starting time, ending time, and time interval of the schedule.
list-no schedule list range is <0-99>;

[Default]

Port is not the protect port.

[Command Modes]

Ethernet physical interface configuration mode and physical port range configuration mode; privileged user.

[Usage Guide]

only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

port X unsuccessfully !
Set successfully

[Example]

set port 5 to protect port
Raisecom(config-port)# ***switchport protect***
Delete port protection for port 5.
Raisecom(config-port)# ***no switchport protect***

[Related command]

Command	Description
show interface port protected	Show port protection setting of physical port

3.281. switchport svl vlanlist

[Introduction]

Set shared VLAN list. No command to delete shared VLAN list.

switchport svl vlanlist {1-4094}

no switchport svl vlanlist

[Parameter]

svl set shared VLAN
vlanlist shared VLAN list

[Default]

Shared vlan list is empty.

[Command Modes]

Ethernet physical Physical port configuration mode and physical port range configuration mode; privileged user (priority 15).

[Usage Guide]

Only the privileged user with priority 15 can use this command.

[Explanation of command execution echo]

Set unsuccessfully

Fail in setting svl vlan list to port n

[Example]

Set the shared VLAN of port 1 to 1-4.

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

Delete port 1 shared VLAN list.

Raisecom(config-port)# ***no switchport svl vlanlist***

[Related command]

Command	Description
show switchport [<1-26>] svl vlanlist	Show shared VLAN list.

3.282. switchport trunk allowed vlan

[Introduction]

Set port allowed VLAN when port is TRUNK mode.

switchport trunk allowed vlan {all | {1-4094}**}**

no switchport trunk allowed vlan

[Parameter]

all **all** VLAN;

{1-4094} VLAN list;

[Default]

Default value is all.

[Command Modes]

Ethernet physical interface range configuration mode; privileged user.

[Explanation of command execution echo]

Set unsuccessfully on port PORTID!

Set successfully.

[Usage Guide]

Set this value, and set the allowed VLAN when port is TRUNK mode.

User can use **no switchport trunk allowed vlan** command to recover default setting.

[Example]

Set the allowed VLAN 2,3,100 when port is in TRUNK mode.

Raisecom(config-port)# ***switchport trunk allowed vlan*** *2-3,100*

Recover default setting.

*Raisecom(config-port)#****no switchport trunk allowed vlan***

[Related command]

Command	Description
switchport access vlan	Set ACCESS VLAN ID of the port
switchport hybrid allowed vlan	Set the allowed VLAN when port is HYBRID mode.
switchport mode	Set the VLAN mode of the port
switchport native vlan	Set the NATIVE VLAN when port is HYBRID or TRUNK mode.
show interface port portlist **switchport**	Set VLAN setting for the port.

3.283. terminal history

[Introduction]

Change the history command number in memory input by console.

terminal history <*1-20*>

[Parameter]

history configuration information of terminate history command

<*1-20*> the history command number input by terminal

[Default]

The history command number input by terminal is 20

[Command Modes]

User EXEC; common user, privileged user

[Usage Guide]

Use the command to change the history command number input by console, making it clearer to show history command.

[Explanation of command execution echo]

Set successfully.

[Example]

*Raisecom>**terminal history** 10*

[Related command]

Command	Description
history	show the history command of the console

3.284. terminal time-out

[Introduction]

Use the command to change the configuration when the console logout because of time-out.

terminal time-out <*0-65535*>

[Parameter]

time-out the configuration information when terminal logout because of time-out.

<*0-65535*> the overtime when terminal is free.(point: second)

[Default]

The overtime of the console is 600 seconds and it will logout.

[Command Modes]

User EXEC; common user, privileged user

[Usage Guide]

Use the command to change the configuration information when the console logout bocause of time-out.

[Explanation of command execution echo]

Set successfully.

[Example]

*Raisecom> **terminal time-out** 1000*

[Related command]

Command	Description

show terminal	Show the information of terminal.

3.285. trunk

[Introduction]

Enable or disable trunk function.

trunk {enable|disable}

[Parameter]

enable enable trunk function.
disable disable trunk function.

[Default]

Start trunk function.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to enable or disable trunk function.

[Explanation of command execution echo]

Set success
Set unsuccessfully !

[Example]

Enable trunk function for the link.
Raisecom(config)# trunk enable
Disable trunk function for the link.
Raisecom(config)# trunk disable

[Related command]

Command	Description
show trunk	Show trunk status, link trunk load balance mode, all the trunk members of the trunk group and all the currently enabled port member.

3.286. trunk group

[Introduction]

Add a trunk group. no command is used to delete the operation.

trunk group trunk-group-id portlist

no trunk group trunk -group-id

[Parameter]

trunk-group-id trunk group ID, range is 1—6.
portlist port number for the group, format can be 1-3,5 etc. 8 ports as the maximum.

[Default]

N/A.

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Use this command to create a link trunk. Combine appointed port aggregation to a single aggregation port. Each aggregation port includes 8 ports with the same speed as the maximum.

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

[Explanation of command execution echo]

Set successfully
Set unsuccessfully !
Permit 8 members at most!
Some member ports are overlapped with those of other trunk group!
Trunk group 3 is not exist!

[Example]

Create aggregation group 3, including prt 1,4,5,6,8.
Raisecom(config)#trunk group 3 1,4-6,8
Delete aggregation group 3.
Raisecom(config)#no trunk group 3

[Related command]

Command	Description
show trunk	Show trunk status, link trunk load balance mode, all the trunk members of the trunk group and all the currently enabled port member.

3.287. trunk loading-sharing mode

[Introduction]

Set loading-sharing mode of aggregation ports.

trunk loading-sharing mode {smac | dmac | sxordmac | sip | dip | sxordip}

no trunk loading-sharing mode

[Parameter]

smac select the forward port based on source MAC address.
dmac select the forward port based on destination MAC address.
sxordmac select the forward port based on the result of logical operation “or” of source MAC address, destination MAC address.
sip select the forward port based on source IP address.
dip select the forward port based on target IP address.
sxordip select the forward port based on the result of logical operation “or” of source MAC address, destination MAC address.

[Default]

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

[Command Modes]

Global configuration mode; privileged user.

[Usage Guide]

Users can select different loading shared mode based on the usage of the aggregation links.

Example, if the link is used to connect layer-3 switch in order to provide router support for access layer, users should select loading shared mode based on source MAC address.

[Explanation of command execution echo]

Set successfully
Set unsuccessfully !

[Example]

Select the forward port based on source MAC address.
Raisecom(config)#trunk loading-sharing mode sip

Recover trunk loading shared mode to default setting.
Raisecom(config)#no trunk loading-sharing mode

[Related command]

Command	Description
show trunk	Show trunk status, link trunk load balance mode, all the trunk members of the trunk group and all the currently enabled port member.

3.288. trust

[Introduction]

Configure the trust status for the traffic (Not available in this version)

[Command format]

trust [**cos** | **dscp | ip-precedence**]

no trust [**cos** | **dscp | ip-precedence**]

[Parameter]

CoS—classify based on the CoS value of the ingress packet. To UNTAG packet, use port default CoS value, that is 0.

DSCP—classify based on the DSCP value of the ingress packet. To non-IP packet, if the packet is tagged, use the CoS value of the packet; if the packet is untagged, use the default CoS value. The switch use CoS-to-DSCP mapping table map the CoS value to DSCP value.

IP priority—classify based on the IP priority of ingress packet. To non-IP packet, if the packet is tagged, use the CoS value of the packet; and if the packet is untagged,use the default CoS value of the packet. The switch use CoS-to-DSCP mapping table map the CoS value to DSCP value.

[Default]

Default setting is untrust; that is untrust status.

[Command Modes]

PMAP-C configuration mode;Privileged user.

[Usage Guide]

User can set the cos,ip priority or dscp of the trust packet as the internal QoS priority.

[Explanation of command execution echo]

Set the trust state for the class map successfully.

Set the trust state for the class map unsuccessfully.

[Example]

*Raisecom(config-pmap-c)#**trust cos***
*Raisecom(config-pmap-c)#**no trust cos***

[Related command]

Command	description
show policy-map [policy-map-name**]**	Show policy-map information.

3.289. upload

[Introduction]

Use the command to upload configuration file of system or system-boot file to ftp server.

upload {system-boot | startup-config} {ftp}

[Parameter]

system-boot file to boot system

startup-config file to configure system

ftp use ftp protocol to download

tftp use tftp protocol to download.

[Default]

N/A

[Command Modes]

Privileged EXEC, privileged user

[Usage Guide]

Use the command to upload system configuration file or system boot file to ftp server as a backup file. The command can use different transfer protocols to download and support ftp protocol now. Before use the command, ftp server should be configured beforehand and switch system is connected to the server for sure.

[Explanation of command execution echo]

Read error.

Error occurred when reading from the server

Invalid input ftp protocol port.

Error occurred when input invalid protocol port number

Invalid input file name

Invalid file name

User name is empty!

User password is empty!

[Example]

*Raisecom# **upload system-boot ftp***
Please input server IP Address:1.0.0.1
Please input FTP User name:test
Please input FTP Password:test
Please input FTP Server File Name:system_boot.Z
Use ftp protocol download system boot file from ftp server.
*Raisecom# **upload startup-config tftp***
Please input server IP Address:1.0.0.1
Please input TFTP port(default 69):
Please input TFTP Server File Name:start_config.conf
Use ftp protocol to download startup file from ftp server.

[Related command]

Command	Description
download	Download configuration file or startup file of system.

3.290. user

[Introduction]

Add user and set the password of the user.

Use the command of “no user” to delete user.

user *USERNAME* **password** { **no-encryption | md5 }** *PASSWORD*

no user *USERNAME*

[Parameter]

USERNAME	username
password	password
no-encryption	Lain Text Password without encryption
md5	password with MD5 encryption
PASSWORD	password information.

[Default]

The default priority for adding a user is 15.
use **user privilege** command to change the priority of user.
The user's default enable password is 123 added by the command, enable password is used to change password.

[Command Modes]

Privileged EXEC, privileged user (Priority 15)

[Usage Guide]

There is at least one user whose priority is 15 in system user database.

Only users whose priority is 15 can use the command.

[Explanation of command execution echo]

You have no enough right to change user information!
This echo shows when privileged user whose priority is not 15 tries to create a new user. Only 15-priority users can perform this command.
Set successfully!
Set fail!

[Example]

Add a user whose ID is abc and password is 123.
*Raisecom# **user** abc **password** no-**encrypt** 123*
Delete a user whose ID is abc.
*Raisecom# **no user** abc*

[Related command]

Command	Description
hostname	Change hostname specified by special user.
user privilege	Change the priority of user
enable password	Change the password of user enable
password	Change the password of current user

3.291. user login

[Introduction]

Set the login mode for authentication.

user login { local-user | radius-user | local-radius | radius-local }

[Parameter]

local-user Use local configuration file to authenticate user.
radius-user User RADIUS server to authenticate user.
local-radius use local configuration file to check login user, do not need to login RADIUS server to get authentication once more.
radius-local should pass RADIUS server authentication, do not need to login local configuration file to get the authentication once more.

[Default]

Local configuration file is used in default.

[Command Modes]

Privileged EXEC, privileged user (priority 15)

[Usage Guide]

Based on RADIUS authentication, user is “ENABLE” and password is 123, hostname is Raisecom, tip is Enter keyboard in default, default priority is 15.

[Explanation of command execution echo]

Set User Login Method failed.
Set User Login Method successfully.

[Example]

Set local-user as the authentication type of login.
Raisecom# ***user login local-user***

[Related command]

Command	Description
radius host	Set RADIUS authentication IP server address.
radius-key	Set the shared key for RADIUS authentication server and client PC.

3.292. user name privilege

Use **user name privilege** command to set the user priority for particular user.

user name USERNAME **privilege** <1-15>

[Parameter]

USERNAME user name;

<1-15> user privilege;

[Default]

Default user priority is 15.

[Command Modes]

Privileged configure mode; privileged user (Only the user with priority 15 can apply this command).

[Usage Guide]

Use this command when it’s needed to limit the user priority for particular user, if the user priority is less than 5, it will change to normal user.

[Explanation of command execution echo]

Set successfully.

can not change user privilege !

You have no enough right to change user information !

[Example]

set the user priority of user abc to 4.
Raisecom# ***user name*** *abc* ***privilege*** *4*

[Related command]

Command	Description
user	Add user and set user password.
show user	Show user information.

3.293. Vlan

[Introduction]

Create VLAN or enter static VLAN mode.

vlan <*1-4094*>

no vlan {all | <*2-4094*>}

[Parameter]

<*3-4094*> VLAN ID

all All the static VLAN except default VLAN(VLAN ID is 1).

[Default]

In default, there are default VLAN and cluster VLAN available in the system, that is VLAN 1 and VLAN 2is available in the system. all the ports are saved in VLAN 1 as extend-access mode.

[Command Modes]

Global configuration mode; privileged user

[Usage Guide]

The user use command VLAN to enter configuration mode of static VLAN, if referenced VLAN is not available, system will create automatically. The state of static VLAN newly created is hung up, user must activate it's configuration in configuration mode and quit configuration mode of VLAN, the referenced mode will be enabled.

User can use **no vlan** to delete static VLAN in the system.

[Example]

Enter configuration mode of static VLAN 4094.

*Raisecom(config)# **vlan** 4094*

Delete VLAN 3 form system.

*Raisecom(config)#**no vlan** 3*

[Related command]

Command	Description
name	The name static VLAN.
state	Set activation state of static VLAN.
shutdown	Shut down/startup configuration of static VLAN

3.294. Write

[Introduction]

The command is used to save configuration information of current system.

write [**schedule-list** list-no]

[Parameter]

schedule-list set the starting time, ending time and time interval of schedule

list-no schedule list range is<0-99>;

[Command Modes]

Privileged EXEC, privileged user

[Usage Guide]

Use the command to save configuration information of current system, then the saved system command will be executed automatically after reset the system, a new configuration of the switch is not needed.

[Explanation of command execution echo]

Save current configuration successfully!

Save current configuration Fail!

[Example]

*Raisecom#**write***

[Related command]

Command	Description
show startup-config	Show startup configuration of system.
download	Download configuration file or startup file of system.
upload	Upload configuration file or startup file of system.
erase	Delete referenced files in system