



ISCOM 3026 Series Switch Command Notebook

Software Version - ISCOMOS 1.4

Beijing Raisecom Science & Technology Co., Ltd

April 2005

CONTENTS

ISCOM 3026 SERIES SWITCH	1
COMMAND NOTEBOOK.....	1
SOFTWARE VERION - ISCOMOS 1.4.....	1
APRIL 2005	1
CHAPTER 1 PREFACE	1
1.1 PURPOSE.....	1
1.2 ABBREVIATION.....	1
1.3 REFERENCE	2
CHAPTER 2 COMMAND LINE INTERFACE	3
2.1 ENVIRONMENT	3
2.2 COMMAND MODE	3
CHAPTER 3 COMMAND-LINE OF SYSTEM.....	5
3.1 ARP ADD	5
3.2 ARP TIMEOUT	11
3.3 CLEAR	12
3.4 CLEAR ARP	13
3.5 CLOCKSET	13
3.6 CONFIG	14
3.7 DEBUG	14
3.8 DHCP SERVER ACTIVE.....	15
3.9 DHCP-SERVER ENABLE	18
3.10 DHCP-SERVER DEFAULT-LEASE	19
3.11 DHCP-SERVER MAX-LEASE.....	19
3.12 DHCP-SERVER MIN-LEASE.....	20
3.13 DHCP-SERVER IP-POOL.....	21
3.14 DHCP-SERVER RELAY-IP.....	22
3.15 DIR.....	23
3.16 DISABLE	23
3.17 DOWNLOAD.....	24
3.18 ENABLE	26
3.19 ENABLE PASSWORD.....	26
3.20 ERASE	27
3.21 EXIT	27
3.22 FILTER.....	28
3.23 FLOWCONTROL	29
3.24 GARP.....	30
3.25 GMRP	31
3.26 GVRP.....	31
3.27 HELP	32
3.28 HISTORY	32

3.29	HOSTNAME	33
3.30	IP-ACCESS-LIST.....	33
3.31	IP-CONFINE-LIST	错误! 未定义书签。
3.32	IP ADDRESS	34
3.33	IP FORWARDING	35
3.34	IP IGMP-SNOOPING	36
3.35	IP IGMP-SNOOPING	36
3.36	IP IGMP-SNOOPING STATIC <i>MAC-ADDRESS</i> PORT <i>PORTID</i>	37
3.37	IP IGMP-SNOOPING TIMEOUT	38
3.38	IP ROUTE	38
3.39	IP ROUTE AGE	50
3.40	IP ROUTE GATEWAY	50
3.41	IP STATIC-ROUTE-DISTANCE	51
3.42	INTERFACE IP	52
3.43	INTERFACE PORT	52
3.44	INTERFACE AGGREGATOR	53
3.45	LACP	53
3.46	LACP ADMIN-KEY	54
3.47	LAG LOADING-SHARING.....	55
3.48	LACP MODE.....	56
3.49	LACP PRIORITY.....	57
3.50	LACP SYSTEM-PRIORITY.....	57
3.51	LIST.....	58
3.52	LOGGING CONSOLE	59
3.53	LOGGING FILE	60
3.54	LOGGING HOST	60
3.55	LOGGING MONITOR.....	61
3.56	LOGGING ON	63
3.57	LOGGING RATE	63
3.58	LOGGING TIME-STAMP.....	64
3.59	LOGOUT	64
3.60	NAME	65
3.61	PVID	67
3.62	MAC-ACCESS-LIST.....	67
3.63	MAC-ADDRESS-TABLE AGING-TIME.....	69
3.64	MAC-ADDRESS-TABLE LEARNING	69
3.65	MAC-ADDRESS-TABLE STATIC	70
3.66	MIRROR MONITOR_PORT.....	70
3.67	MIRROR SOURCE_PORT.....	71
3.68	PASSWORD	72
3.69	PORT-ACCESS-LIST	75
3.70	QOS COSQ	76
3.71	QOS IP-COS	77
3.72	QOS MAC-COS.....	78
3.73	QOS MAP PRIORITY QUEUE.....	79

3.74	QOS PORT	79
3.75	QOS TOS-COS	80
3.76	QOS VLAN-COS	81
3.77	QUIT	81
3.78	RATE-LIMIT PORT	82
3.79	RATE-LIMIT VLAN	83
3.80	REBOOT	83
3.81	RMON ALARM	84
3.82	RMON EVENT	85
3.83	RMON QUEUESIZE	86
3.84	SEARCH MAC-ADDRESS	86
3.85	SHOW ACCESS-LIST	88
3.86	SHOW IP-ACCESS-LIST PORT-ACCESS-LIST MAC-ACCESS-LIST IP-CONFINE-LIST	错误! 未定义书签。
3.87	SHOW AGING-TIME	88
3.88	SHOW ARP	89
3.89	SHOW CLOCK	89
3.90	SHOW DHCP-SERVER	90
3.91	SHOW DHCP-SERVER IP-POOL	93
3.92	SHOW DHCP-SERVER RELAY-IP	94
3.93	SHOW FILTER	94
3.94	SHOW GARP	95
3.95	SHOW GMRP	95
3.96	SHOW GVRP	95
3.97	SHOW IP IGMP-SNOOPING	96
3.98	SHOW IP ROUTE	97
3.99	SHOW INTERFACE PORT	105
3.100	SHOW INTERFACE VLAN	106
3.101	SHOW LACP LAG-ID	107
3.102	SHOW LACP PORT	107
3.103	SHOW LOGGING	108
3.104	SHOW MAC-ADDRESS-TABLE L2-ADDRESS	109
3.105	SHOW MAC-ADDRESS-TABLE MULTICAST	112
3.106	SHOW MAC-ADDRESS-TABLE STATIC	113
3.107	SHOW MIRRORING	114
3.108	SHOW MONITOR_PORT	114
3.109	SHOW QOS COSQ	115
3.110	SHOW QOS MAP	115
3.111	SHOW QOS PRI-CONTROL	116
3.112	SHOW RATE-LIMIT	116
3.113	SHOW RMON ALARMS	117
3.114	SHOW RMON EVENTS	117
3.115	SHOW RMON HISTORY	118
3.116	SHOW RMON STATISTICS	119
3.117	SHOW RUNNING-CONFIG	119
3.118	SHOW SERVICE	120

3.119	SHOW SNMP	121
3.120	SHOW SNMP COMMUNITY	122
3.121	SHOW SNMP CONTACT	122
3.122	SHOW SNMP HOST	123
3.123	SHOW SNMP LOCATION	123
3.124	SHOW SNMP VIEW.....	124
3.125	SHOW SNTP	124
3.126	SHOW STARTUP_CONFIG.....	125
3.127	SHOW STORM_CONTROL	126
3.128	SHOW STP	126
3.129	SHOW SVL.....	128
3.130	SHOW TERMINAL.....	128
3.131	SHOW VLAN CURRENT.....	129
3.132	SHOW VLAN STATIC.....	130
3.133	SHOW UPLINK-PORT	130
3.134	SHOW USER	131
3.135	SHOW VERSION	131
3.136	SHUTDOWN	132
3.137	SHUTDOWN VLAN	132
3.138	SNMP-SERVER COMMUNITY	133
3.139	SNMP-SERVER CONTACT	134
3.140	SNMP-SERVER ENABLE TRAPS.....	135
3.141	SNMP-SERVER HOST.....	135
3.142	SNMP-SERVER LOCATION	136
3.143	SNMP-SERVER VIEW	136
3.144	SNTP BROADCAST CLIENT	137
3.145	SNTP SERVER.....	138
3.146	SPEED	138
3.147	SPEED AUTO-NEGOTIATE	139
3.148	STATE	139
3.149	STORM_CONTROL	140
3.150	STP	141
3.151	STP FORWARD-DELAY	142
3.152	STP HELLO-TIME	142
3.153	STP MAX-AGE	143
3.154	STP PATH-COST	144
3.155	STP PRIORITY	144
3.156	STP PRIORITY	145
3.157	SVL	146
3.158	TERMINAL HISTORY.....	146
3.159	TERMINAL TIME-OUT	147
3.160	TRANS-EAPOL	147
3.161	UPLINK-PORT	150
3.162	UPLOAD	151
3.163	USER.....	151

3.164	USER LOGIN	152
3.165	USER PRIVILEGE	154
3.166	VLAN	155
3.167	VLAN-ACCESS	155
3.168	WRITE.....	156

Chapter 1 Preface

1.1 Purpose

This notebook mainly introduces the command line interface of the ISCOMOS software. It systematically introduces the human-machine interface of the command line in the software whose version is ISCOMOS1.3 used by the ISCOM3026 Switch. It is for the ISCOM3026 and related ISCOMOS software clients.

1.2 Document organization

This notebook includes the following contents:

Chapter 2: The usage of command lines

It introduces the visit control of the ISCOMOS software command line, and the configuration of Switch.

Chapter 3: Command in the system

Systematically introduce the configuration command in the command line supported in the ISCOMOS software in the alphabetical order.

1.3 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

1.4 Reference

1. <ISCOM3026 Series Switch Configuration Manual>

Chapter 2 Command Line Interface

2.1 Environment

ISCOM3026 hardware environment: ISCOM3026 REV.A.0.

Software environment: ISCOMOS 1.3.

2.2 Command Mode

Mode	What you use it for	How to access	Mode id
User exec	To connect the remote device, change terminal settings on a temporary basis, perform basic tests, and display system information.	Login	Raisecom>
Privileged user exec	To set operating parameters. the privileged command set includes the commands in users exec mode, as well as configure command. Use configure command to access other command mode	From user exec mode, enter the enable command and enable password	Raisecom#
Global configuration	To configure features that affect the system as whole.	From privileged EXEC mode enter config .	Raisecom(config)#
interface configuration	To enable or modify the operation of a Gigabit or fast Ethernet interface.	From global configuration mode, enter interface port portid	Raisecom(config-port)#
Layer 2 interface config mode	Configure the L2 interface parameter under this mode	Under global exec, enter interface aggregator id command.	Raisecom(config-aggregator)#

Layer 3 interface config mode	Configure the L3 interface parameter under this mode	Under global exec, enter interface ip id command.	Raisecom(config-ip)#
VLAN config mode	Configure VLAN operation parameter	Under global exec, enter Vlan vlan_id command.	Raisecom(config-vlan)#
Route config mode	Configure routing parameters, including RIP routing mode and OSPF routing mode	Under global exec, enter route protocol name command.	Raisecom(config-router-rip)#

Chapter 3 command-line of system

3.1 area default-cost

[Introduction]

When the Stub or the NSSA areaal Router comes to the outside of autonomy system, it goes through the default Router. Appoint the cost of the default Router through this command.

[Parameter]

·*areaid* areaal ID of the stub or NSSA area, a decimal integer between 0-3758096383;

·*cost* the cost of default Router, range 0—0xfffff;

[Default]

1

[Mode]

OSPF protocol configuration mode; Privileged user.

[Guide]

This command is only used for connecting to the ABR in the stub or NSSA. For all the Switches connecting to the stub area, they must use the **area stub** to configure the area to stub area. For all the Switches connecting to the NSSA area, they must use the **area stub** to configure the area to NSSA area. Command **area default—cost** are only used to connect the ABR in the stub or NSSA area. This command configures the default Router cost from ABR to the stub or NSSA area.

[Command Execution Echo]

- *set stub area metric successful*
- *set stub area metric fail*
- *set nssa area metric successful*
- *set nssa area metric fail*
- *error!specified area is not exist*
- *error!specified area is neither stub nor nssa*

[For example]

- Configure the cost of the stub area 1 to 20
Raisecom (config-router-ospf)#**area 1 stub**
Raisecom (config-router-ospf)#**area 1 default-cost 20**
- Configure the cost of the nssa area 2 to 10
Raisecom (config-router-ospf)#**area 2 nssa**
Raisecom (config-router-ospf)#**area 2 default-cost 10**

[Relevant command]

Command	Description
area stub	Set some area to stub area
area nssa	Set some area to nssa area

3.2 area nssa

[Introduction]

Set some area to NSSA area (make the area where the ASBR exists not to become a totally stub or totally stubby area)

[no] area area-id nssa [no-summary]

[Parameter]

- *area-id* areaal ID of the NSSA area, an decimal integer between 0-3758096383;
- **no-summary** Set this area to NSSA area, but not allow to gather LSA for adding to the nssa;

[Default]

Non-NSSA area

[Mode]

OSPF protocol configuration mode; Privileged user.

[Guide]

NSSA (Not-So-Stubby area) . The stub area does not accept Router information outside the autonomy system. NSSA is similar to the stub area, but it allows accepting the outside Router information sent in the LSA YTYPE 7. Using of this command will configure some area to NSSA area.

Use the command **no area areaid stub** to delete stub area

Attention: the command **no area area —id** (not including other key word) will delete the appointed area, for ecample: the areas created in the command **area nssa, area range, area stub, area virtual-link , network area.**

[Command Execution Echo]

- create nssa area successful
- create nssa area fail
- set nssa area no-summary successful·
- set nssa area no-summary fail·
- error! nssa area has been existed·

[For example]

- Set the area 1 to NSSA area
Raisecom (config-router-ospf)#**area 1 nssa**
- Set area 1 to the NSSA area not accepting summary-LSA
Raisecom (config-router-ospf)#**area 1 nssa no-summary**

[Relevant command]

Command	Description
Area default-cost	Set the default Router cost of the stub area or the nssa area
show ip ospf	Display the ospf configuration information

3.3 area range

[Introduction]

Gather the Routers matching the address/mask in the ABR.

[no] area area-id range ip-address mask [{advertise|not-advertise}]

[Parameter]

- area-id* areaal ID, a decimal integer between 0-3758096383;
- ip-address* IP address
- mask* IP address mask
- advertise** generate a type 3 gathering Router to gather LSA advertise

·**not-advertise** not generate a type 3 gathering Router to gather LSA advertise

[Default]

No gathering Router

[Mode]

OSPF protocol configuration mode; Privileged user.

[Guide]

Area range is only used on area boundary Router, in which it can help centralizing and gathering Router. Single gathering Router broadcasts to the other area through ABR. The Router information is simple on the area boundary. For the outside of the area, it broadcasts for the single Router of every address range, so it will simplify the Router list. The parameters of the command decide whether broadcasting the gathering Router or not.

[Command Execution Echo]

- create area aggregate successful
- the input address is invalid
- the input mask address is invalid
- create area aggregate fail
- set area aggregate advertise successfully
- set area aggregate advertise fail
- set area aggregate not-advertise successfully
- set area aggregate not-advertise fail
- area aggregate with advertise has been existed
- area aggregate with not-advertise has been existed
- area aggregate has been existed

[For example]

If in the ABR Router list , there is a Router to 200.16.10.65 and to 200.16.10.33, and the Router to the two network is the same, what we need is a Router to the network 200.16.0.0, as it includes all of the two subnets. In other words, we want to gather the two Routers into one Router. The area range command is as follow:

Raisecom (config-router-ospf)#**area 2 range 200.16.0.0 255.255.255.0 advertise**

Gather the Router to the 200.16.0.0 network in area 2, and send the overall LSA to the other areas.

[Relevant command]

None

3.4 area stub

[Introduction]

Set some area to stub

[no] area area-id stub [no-summary]

[Parameter]

- area-id* sub areaal ID, a decimal integer between 0-3758096383;
- no-summary** set the area to complete stub area

[Default]

None stub area

[Mode]

OSPF protocol configuration mode; Privileged user

[Guide]

Stub area is a area into which AS External LSAs is not flooded. To reduce the number of Link-state Advertisement (LSA) transmitted to the stub area, **no-summary** could be installed on the boundary Router of the stub area to set the stub area to totally stubby area. The totally stubby area not only block the flood of AS External LSAs, but also all the flood of summary-LSAs, except the default summary-LSAs.

The Router information outside the autonomy system will not be flooded into the stub area, so to set a area to stub area could save the memory space of Router in the area and enhance the efficiency of managing the Router.

Use the command: **no area areaid stub** to delete the sub area.

[Command Execution Echo]

- create stub area successful
- create stub area fail
- set stub area no-summary successful
- set stub area no-summary fail
- error! stub area has been existed

When the input stub area already exists and the no-summary character outputs this information all the time

[For example]

- Set the area 1 to stub area
Raisecom (config-router-ospf)#**area 1 stub**
- Set the area 1 to total stub area
Raisecom (config-router-ospf)#**area 1 stub no-summary**

[Relevant command]

Command	Description
area default-cost	The cost of setting the default Router of the stub area or the nssa area
show ip ospf	Display the ospf configuration information

3.5 area virtual-link

[Introduction]

Set the virtual link and its interface parameters

[no] area area-id virtual-link router-id

[hello-interval hello-interval]

[retransmit-interval retransmit-interval]

[transmit-delay transmit-delay]

[dead-interval dead-interval]

[authentication-type {simple-password | message-digest | none}]

[authentication-key authentication-key]

[message-digest-key message-digest-key md5 md5]

[Parameter]

- area-id* Set the area number passed through when configuring the virtual link, a decimal integer between 0-3758096383;
- router-id* The Router ID of the virtual neighbor, dot separated decimal format, viz the IP address format
- hello-interval* The time interval of sending the hello package by the virtual interface a decimal integer between 0-65535, the unit is second
- retransmit-interval* The time interval of retransmitting the LSA by the virtual

interface, a decimal integer between 0-65535, the unit is second

- *transmit-delay* The transmit delay of the virtual interface, a decimal integer in 0-65535, the unit is second
- *dead-interval* The time interval for the death of the virtual interface neighbor, a decimal integer between 1-65535, the unit is second
- *simple-password* The type of authentication of the virtual interface is simple authentication
- *message-digest* The type of authentication of the virtual interface is MD5 authentication
- *none* The type of authentication of the virtual interface is no authentication
- *authentication-key* The character string of the simple password set by the virtual interface, it has 1-8 bit character, and the maximum is 8 bit character string
- *message-digest-key* The Md5 key index of the virtual interface, a decimal integer between 1-255
- *md5* Md5 key of the virtual interface, a 1-16 bit character

[Default]

- *hello-interval* default time is 10 seconds;
- *retransmit-interval* default time is 5 seconds;
- *transmit-delay* default time is 1 seconds;
- *dead-interval* default time is 40 seconds;
- *authentication-key* default is none;
- *message-digest-key* default is not setting the Md5 key index;
- *md5* default is not setting the Md5 key;
- *In the default situation, the validating type of the virtual link is without validation*

[Mode]

OSPF protocol configuration mode; Privileged user

[Guide]

The virtual link goes through the non backbone area to the backbone area (area 0). It is mainly used in the following situations:

- 1) Connect a area to backbone area through non backbone area.
- 2) Link the separated two parts of the backbone area through non backbone area.

The two situations are used to realize or boost up the connectivity of the backbone area. Virtual link must be configured between the two ABR. When configuring the virtual link, area ID of the transmitting area and the opposite Router ID connecting the two virtual neighbors must be pointed out clearly. In this case, virtual link is activated after calculating the other's Router. It forms a point to point link between the two ends. On this link, interface parameters could be configured.

Using command **area areaid virtual-link router-id** only create a virtual link, the parameters of the virtual link is the default value.

When using this command with parameters, if the virtual link already exists, change the parameters configuration according to the parameters in the command. If the virtual link do not exists, create a virtual link and change the interface parameter configuration.

This command can configure with several parameters at the same time.

The smaller the Hello time interval is, the quicker the network topology been detected, but at the same time, the network communication quantity will increase. The value of retransmit-interval should be conservative, or else it will cause unnecessary rebooting. For serial line and virtual link, its value should be bigger.

Use the command **no area areaid virtual-link router-id** to delete the virtual link.

[Command Execution Echo]

- create virtual link successful
- create virtual link fail
- Area 1 is a stub or nssa, so virtual link is not permitted·
- Error!virtual link has been existed
- set virtual link hello interval fail·
- set virtual link hello interval successful·
- set virtual link retransmit interval fail·
- set virtual link retransmit interval successful·
- set virtual link transmit delay fail
- set virtual link transmit delay successful
- set virtual link dead interval fail
- set virtual link dead interval successful
- set virtual link authentication type fail
- set virtual link authentication type successful
- set virtual link simple authentication key fail
- set virtual link simple authentication key successful·
- set virtual link MD5 key fail
- set virtual link MD5 key successful

[For example]

- Configure the virtual link through the area 1, the Router ID of the virtual neighbor is 10.0.0.1
raisecom(config-router-ospf)#**area 1 virtual-link 10.0.0.1**
- Configure the parameters of the virtual interface; the appointed virtual interface hello interval is 15 seconds.
raisecom (config-router-ospf)#**area 1 virtual-link 10.0.0.1 hello-interval 15**
- Configure the MD5 key authentication of the virtual interface, the MD5 authentication key is 3, and the password is abcd
raisecom(config-router-ospf)#**area 1 virtual-link 10.0.0.1 message-digest-key3 md5 abcd**

[Relevant command]

Command	Description
show ip ospf virtual-links	Show all the virtual link an virtual neighbor information

3.6 arp add

[Introduction]

Add ARP new items.

arp add ip-address mac-address

[Parameter]

- ip-address format: A.B.C.D

· *mac-address* format: HHHH.HHHH.HHHH
 [Default]
 None
 [Mode]
 Privileged configuration
 [Guide]

ARP mapping table is maintained by dynamic ARP protocol on general circumstance. ARP searches the resolving result of IP address mapping to MAC. It is not required to involve administrator. When it is required to add static ARP table items, manually operation for ARP mapping table is required. This kind of IP address in ARP table item must belong to layer 3 interfaces.

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

[Command Execution Echo]

- *set successfully!*
 Adding static MAC address list successfully
- *set fail!*
 Adding static MAC address list fails

[For example]

- Add a static MAC address item. Set IP address as 10.0.0.1 and MAC address 0050.8d4b.fd1e
Raisecom(config)#arp add 10.0.0.1 0050.8d4b.fd1e
- Delete table IP address 10.0.0.1 in ARP mapping table
Raisecom(config)# no arp add 10.0.0.1

[Relevant command]

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

3.7 arp timeout

[Function Introduction]

Set dynamic ARP table existing time. If it is timeout, arp dynamic items will be deleted.

arp timeout secs

[Parameter]

- *secs* - seconds, 0-2147483 integer.

[Default]

The default timeout value of ARP dynamic table item is 1200 seconds.

[Mode]

Global configuration and privileged users

[Guide]

Set timeout value of ARP dynamic table item. If the value is 0 second, ARP dynamic table item isn't aging.

[Command Execution Echo]

- *set successfully!*
- *set fail!*

[For Example]

- Set timeout value of ARP dynamic table item is 1500 seconds.
Raisecom(config)# arp timeout 1500
- Restore default timeout value of ARP dynamic table item is 1200 seconds.
Raisecom(config)# no arp timeout

[Relevant commands]

Command	Description
clear arp	Delete all arp table items
show arp	Show all arp table items

3.8 english

[Introduction]

Use **english** to display the command line help information in English.

english

[Parameter]

·None

[Default]

Display the command line help information in English.

[Mode]

Primary mode, privileged mode, global configuration mode, vlan configuration mode, interface configuration mode, Router protocol configuration mode; normal user, privileged user.

[Guide]

This command gives the help information in English, and it contains abundant and clear help information.

[Command Execution Echo]

·None

[For example]

- **english**

[Relevant command]

Command	Description
chinese	Show the help information in Chinese

3.9 clear

[Function Introduction]

Use **clear** to clear the screen.

clear

[Parameter]

None

[Mode]

Initial mode, privileged configuration mode, global configuration mode, VLAN configuration mode, interface configuration mode, router protocol configuration mode; common user, and privileged user

[Guide]

Clear the shown information on the screen.

[Command Execution Echo]

None

[For example]

Raisecom> **clear**

[Relevant command]

None

3.10 clear arp

[Function introduction]

Clear all items of ARP mapping table

clear arp

[Parameter]

None

[Default]

None

[Mode]

Privileged exec and privileged users

[Guide]

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

[Command Execution Echo]

- set successfully!
Clear ARP list successfully
- set fail!
Clear ARP list unsuccessfully

[For example]

Clear ARP table
Raisecom(config)#clear arp

[Relevant command]

command	Description
arp add	Add a static MAC address item
show arp	Show all items of ARP mapping table

3.11 clear dot1x statistics

[Introduction]

Clear all the statistics information of all the port or the specified port

clear dot1x statistics [interface port]

[Parameter]

·port Port number , integer between 1-26

[Mode]

Global configuration and privileged users

[Guide]

The unit of these statistics information is port

[Command Execution Echo]

- Clear 802.1X statistics successfully.

[For example]

Clear the authentication statistics information in port 5:
Raisecom(config)# clear dot1x statistics interface 5

[Relevant command]

Command	Description
show dot1x statistics	Show the specified port statistics information

3.12 clockset

[Function 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

[Mode]

Privilege exec and privilege users

[Guide]

Use **clockset** to modify date and time and they are saved in NVRAM. They can not disappear although the power supply is off.

[Command Execution Echo]

set successfully.
Command executed successfully

[For example]

*Raisecom# **clockset** 8 30 0 2003 9 30*
System date is modified as 30th Sep, 2003, 8:30:00

[Relevant command]

command	Description
show clock	Show the current time of system

3.13 config

[Function introduction]

Use **config** to access global configuration mode.

config [terminal]

[Parameter]

terminal

[Mode]

Privileged exec and privileged user

[Guide]

None

[Command Execution Echo]

set successfully.
Command executed successfully

[For example]

*Raisecom#**config terminal***

[Relevant command]

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

3.14 debug

[Function 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 open
System module open
Others debug functionalities closed

[Mode]

Privileged exec and privileged user

[Guide]

Use this command to be some or all module debug functionalities available.

[Command Execution Echo]

None

[For example]

*Raisecom#**debug all***

[Relevant command]

Command	Description
logging	Configure system log

3.15 dhcp-relay enable

[Introduction]

Start the DHCP Relay function. Command **dhcp-relay disable** will stop the DHCP Relay function.

dhcp-relay enable

[Parameter]

·None

[Default]

The default configuration is that the DHCP Relay protocol is invalidation.

[Mode]

Global configuration and privileged users

[Guide]

Start the DHCP Relay function through command **dhcp-relay service**. Command **no dhcp-relay service** can set the state of DHCP Relay protocol to be invalidation.

[Command Execution Echo]

- Enable DHCP Relay success
- Enable DHCP Relay failure
- Disable DHCP Relay success·
- Disable DHCP Relay failure

[For example]

- Set the state of DHCP Relay protocol to be valid
Raisecom(config)# **dhcp-relay service**
- Set the state of DHCP Relay protocol to be invalidation.
Raisecom(config)# **no dhcp-relay service**

[Relevant command]

Command	Description
dhcp-relay listen	Start DHCP Relay on DHCP Relay
show dhcp-relay	Show the configuration and statistics information of the DHCP Relay

3.16 dhcp-relay listen

[Introduction]

Start the DHCP Relay function in the specified VLAN. Command **no dhcp-relay listen** will stop the DHCP Relay function in the specified VLAN.

[no] dhcp-relay listen

[Parameter]

- None

[Default]

When the global DHCP Relay started, the default configuration on the VLAN is that the DHCP Relay protocol is valid.

[Mode]

VLAN configuration mode; privileged user

[Guide]

Start DHCP Relay function in the specified VLAN through the command **dhcp-relay listen**. Command **no dhcp-relay listen** will set the state of DHCP Relay protocol to be invalidation.

[Command Execution Echo]

- Enable DHCP Relay on this VLAN success
- Enable DHCP Relay on this VLAN failure·
- Disable DHCP Relay on this VLAN success
- Disable DHCP Relay on this VLAN failure·

[For example]

- Set the state of DHCP Relay protocol on VLAN 1 to be valid

- Raisecom(config-vlan)# **dhcp-relay listen**
- Set the state of DHCP Relay protocol on VLAN 1 to be invalidation
- Raisecom(config-vlan)# **no dhcp-relay listen**

[Relevant command]

Command	Description
dhcp-relay service	Start global DHCP Relay
show dhcp-relay listen	Show the configuration information of DHCP Relay on the VLAN

3.17 dhcp-relay server-ip

[Introduction]

Configure the adjacent DHCP Relay address. Delete the DHCP Relay address using the command **no dhcp-relay server-ip**.

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

[Parameter]

·*ip-address* Configure the adjacent DHCP Relay IP address, the format is dot decimal, such as A.B.C.D;

·*ip-mask* Configure the adjacent DHCP Relay IP mask, the format is dot decimal, such as A.B.C.D;

[Default]

There is no IP address of DHCP Relay. It is necessary to configure it when starting the DHCP Relay

[Mode]

Global configuration and privileged users

[Guide]

Configure the adjacent DHCP Relay address through the command of **dhcp-relay server-ip**. Delete the adjacent DHCP Relay address using the command of **no dhcp-relay server-ip**. The maximum number of the adjacent DHCP Relay address is 8.

[Command Execution Echo]

- Set DHCP Relay IP address success
- Set DHCP Relay IP address failure
- Delete DHCP Relay IP address success
- Delete DHCP Relay IP address failure

[For example]

- Set the adjacent DHCP Relay address to 10.0.0.1, the mask is 255.0.0.0
Raisecom(config)# **dhcp-relay server-ip 10.0.0.1 255.0.0.0**
- Delete the adjacent DHCP Relay address to 10.0.0.1
Raisecom(config)# **no dhcp-relay server-ip 10.0.0.1**

[Relevant command]

Command	Description
show dhcp-relay server-ip	Show the address information of the configured adjacent DHCP Relay

3.18 dhcp server active

[Function Introduction]

In the appointed VLAN, enable DHCP SERVER. **dhcp-server deactive** disable

DHCP SERVER.

dhcp-server active

dhcp-server deactivate

[parameter]

none

[default]

after DHCP SERVER is enabled, DHCP protocol is available in VLAN default config.

[mode]

VLAN configuration; Privileged user.

[guide]

[Command Execution Echo]

- active DHCP server success on VLAN
- active DHCP server failure on VLAN
- deactivate DHCP server success on VLAN
- deactivate DHCP server failure on VLAN

[for example]

- set DHCP SERVER available on VLAN1
Raisecom(config)# **vlan 1**
Raisecom(config-vlan)# **dhcp-server active**
- set DHCP SERVER unavailable on VLAN1
Raisecom(config-vlan)# **dhcp-server deactivate**

[relevant command]

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

3.19 dhcp-server enable

[Function Introduction]

dhcp-server enable start DHCP SERVER. **dhcp-server disable** stop DHCP SERVER.

[parameter]

none

[default]

the default setting is DHCP SERVER protocol disable.

[mode]

global configuration;Privileged user.

[guide]

[Command Execution Echo]

- Enable DHCP server success
- Enable DHCP server failure
- Disable DHCP server success
- Disable DHCP server failure

[for example]

- Raisecom(config)# **dhcp-server enable**
- Raisecom(config)# **dhcp-server disable**

[relevant command]

Command	Description
dhcp-server active	Start DHCP SERVER on some VLAN
show dhcp-server	Show DHCP SERVER config and statistical information

3.20 dhcp-server default-lease

[Function Introduction]

set DHCP SERVER default lease time of lease table. **no dhcp-server default-lease** Restore default value.

[no] dhcp-server default-lease timeout

[parameter]

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

[default]

default timeout value is 30 minutes.

[mode]

global configuration;priviledged user.

[guide]

use **dhcp-server default-lease** to set DHCP SERVER default lease time for lease table. When the timer is timeout,callback the assigned IP address. Use **no dhcp-server default-lease** to Restore the default setting.

[Command Execution Echo]

- set DHCP server default lease timeout success.
the previous message is displayed, when it is successful;
- set DHCP server default lease timeout failure.
the previous message is displayed, when it fails;
- set DHCP server default lease timeout success.
the previous message is displayed, when it is successful;
- set DHCP server default lease timeout failure.
the previous message is displayed, when it fails;

[for example]

- set DHCP SERVER lease timeout value as 60 minutes:
Raisecom(config)# **dhcp-server default-lease 60**
- Restore DHCP SERVER default lease time:
Raisecom(config)# **no dhcp-server default-lease**

[relevant commmand]

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

3.21 dhcp-server max-lease

[Function Introduction]

set DHCP SERVER max-lease time. **no dhcp-server max-lease** Restore 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.

[mode]

global configuration;privileged user.

[guide]

use **dhcp-server default-lease** to set DHCP SERVER default lease time for lease table. When the timer is timeout,callback the assigned IP address. Use **no dhcp-server default-lease** to Restore the default setting.

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

[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

[for example]

- set DHCP SERVER max-lease time of lease table as 3600 minutes:
Raisecom(config)# **dhcp-server max-lease 3600**
- Restore DHCP SERVER max-lease time:
Raisecom(config)# **no dhcp-server max-lease**

[relevant command]

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

3.22dhcp-server min-lease

[Function Introduction]

set DHCP SERVER min-lease time for lease table.**no dhcp-server min-lease**

Restore 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.

[mode]

global configuration;privileged user.

[guide]

use **dhcp-server default-lease** to set DHCP SERVER default lease time for lease table. When the timer is timeout,callback the assigned IP address. Use **no dhcp-server default-lease** to Restore the default setting.

[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.

[for example]

- set DHCP SERVER min-lease timeout value as 3600 minutes:
Raisecom(config)# **dhcp-server min-lease 3600**
- Restore DHCP SERVER min-lease timeout value:
Raisecom(config)# **no dhcp-server min-lease**

[relevant command]

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

3.23 dhcp-server ip-pool

[Function Introduction]

set DHCP SERVER ip-pool information.

dhcp-server ip-pool name *pool-name start-ip end-ip mask mask-ip vlan vlanlist*

[**gateway** *gtw-address*] [**dns** *dns-address*]

no dhcp-server ip-pool name *pool-name*

[parameter]

pool-name ip-pool name, it must be exclusive name,8 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; but the whole is less than 50 characters.

This property means that some ip-pool belongs to one VLAN.

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

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

[default]

None

[mode]

priviledged exec;priviledged user.

[guide]

use **dhcp-server ip-pool** to set DHCP SERVER ip pool information. Gateway and DNS are optional. If they are not set,the default is 0.0.0.0; note: ip-pool name is 8 characters,and ir is exclusive.Start ip can not be over end ip; Tthe ip must be belong to same network segment, and the range don't exceed 4k.the number of ip address in the pool isn't over 20.

[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.

[for 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

[relevant commmand]

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

3.24 dhcp-server relay-ip

[Function Introduction]

set neighboring DHCP Relay address. **no dhcp-server relay-ip** 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.

[default]

there is not DHCP Relay IP address,when start DHCP SERVER, it can be set with requirement.

[mode]

global configuration;priviledged user.

[guide]

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

[Command Execution Echo]

- Set DHCP Server IP address success
 the previous message is displayed, when set neighboring DHCP Server IP address success;
- 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 the possible reason is the address is nonexistent.

[for example]

- set neighboring DHCP Relay ip address as 10.0.0.1,mask as255.0.0.0:
Raisecom(config)# **dhcp-server relay-ip** 10.0.0.1 255.0.0.0
- delete neighboring DHCP Relay ip address 10.0.0.1:
Raisecom(config)# **no dhcp-server relay-ip** 10.0.0.1

[relevant commmand]

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

3.25dir

[Function Introduction]

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

dir

[parameter]

none

[mode]

priviledged exec;priviledged user.

[guide]

none

[Command Execution Echo]

none

[for 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.
```

[relevant commmand]

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

3.26disable

[Function Introduction]

use **disable** to exit priviledged exec.

disable

[parameter]

none

[mode]

priviledged exec;priviledged user.

[guide]

none

[Command Execution Echo]

none

[for example]

Raisecom#**disable**

[relevant command]

Command	Description
Enable	Access privileged exec from normal exec

3.27 distance

[Introduction]

Set the distance vector of RIP. Using the command **no distance** to Restore the default configuration

distance *value*

no distance

[Parameter]

·*value* The value of the distance vector, the data type is integer, the range is between 1~200

[Default]

The default distance vector value of RIP is 120

[Mode]

RIP protocol configuration mode; privileged user

[Guide]

Set the RIP distance vector by the command **distance**. Restore the default configuration by the command **no distance**.

[Command Execution Echo]

·set rip distance is success·

·set rip distance is failure

The cause of failure might be the exceeding of the parameter range

[For example]

- Set the distance vector in the RIP protocol to 100
Raisecom(config-router-rip)# **distance 100**
- Restore the distance vector in the RIP protocol to default value
Raisecom(config-router-rip)#**no distance**

[Relevant command]

Command	Description
router rip	Set the RIP protocol to be valid, and enter the RIP protocol configuration mode
show ip protocol	Show the information of the Router protocol configuration

3.28 distance

[Introduction]

Set the distance vector of the ospf. Restore to the default configuration by the command **no distance**.

[Parameter]

·*value* The value of the distance vector, the data type is integer, and the range is between 1~200

[Default]

The default value of the distance vector of OSPF is 110

[Mode]

OSPF protocol configuration mode; privileged user

[Guide]

Set the OSPF distance vector by the command **distance**. Restore the default configuration by the command **no distance**.

[Command Execution Echo]

·set ospf distance successfully

·set ospf distance fail

The cause of failure might be the exceeding of the parameter range.

[For example]

- Set the distance vector in the OSPF protocol to 50
Raisecom(config-router-ospf)# **distance 50**
- Restore the distance vector in the OSPF protocol to default value
Raisecom(config-router-ospf)#**no distance**

[Relevant command]

Command	Description
router ospf	Set the OSPF protocol to be valid, and enter the OSPF protocol configuration mode
show ip protocol	Show the information of the Router protocol configuration

3.29download

[Function Introduction]

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

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

[Parameter]

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

[Default]

None

[Mode]

Privileged exec and privileged user

[Guide]

Use **download** to download boot file and config file to flash file system. When it is restarted, the download file will be available automatically. This command can be realized with different file transport protocols. At present, **ftp** protocol are available. Before using these two protocols, it is guaranteed that ftp server is set properly and connected to the switch.

[Command Execution Echo]

· *Read error.*

Errors occurred when reading from 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

[For 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

[Relevant command]

Command	Description
Upload	Upload start-up file or boot file

3.30enable

[Function Introduction]

Use **enable** to access privileged exec.

enable

[Parameter]

None

[Mode]

Initial exec and normal user

[Guide]

Access privileged exec from normal exec.

[Command Execution Echo]

None

[For example]

*Raisecom>**enable***
Password:

[Relevant command]

Command	Description
Enable	Modify the password of accessing privilege exec
password	
disable	Exit privileged exec and return normal exec

3.31enable password

[Function Introduction]

Use **enable password** to set the password of accessing privileged exec.

no enable password Restore password to default value.

enable password (null|PASSWORD)

no enable password

[Parameter]

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

[Default]

Default password is "123" from normal exec to privileged exec.

[Mode]

Privileged exec and privileged user

[Guide]

None

[Command Execution Echo]

None

[For example]

Raisecom#enable password 123

Modify accessing privileged mode password to“123”。

[Relevant command]

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

3.32erase

[Function Introduction]

Use **erase** delete the appointed file in flash file system.

erase [FILENAME]

[Parameter]

FILENAME

[Default]

Delete the current startup_config.conf

[Mode]

Privileged exec and privileged user

[Guide]

None

[Command Execution Echo]

· Erase current specified file successfully!

Command executed successfully

· Erase current specified file Fail!

Command fails

[For example]

Raisecom#erase aaa

Delete 'aaa' file in flash file system.

[Relevant command]

Command	Description
Write	Save the current system config file

3.33exit

[Function Introduction]

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

exit

[Parameter]

None

[Mode]

Initial exec, privileged exec, global exec, VLAN exec, interface configuration exec, routing protocol configuration exec, normal user, and privileged user

[Guide]

None

[Command Execution Echo]

None

[For example]

```
Raisecom>exit
```

[Relevant command]

Command	Description
Quit	Return to parent mode or exit login

3.34filter access-list

[Function Introduction]

This command is used to add a filter rule into the linked list of the filter rules. Using command **no** to delete a filter rule in the linked list of the filter

**[no] filter (ip-access-list | mac-access-list | user-access-list) (all | {0-99})
port-list (all | {1-26}) (ingress | egress | both)**

**[no] filter (ip-access-list | mac-access-list | user-access-list) (all | {0-99})
vlan-list (all | {1-4094})**

[parameter]

- **ip-access-list|mac-access-list|user-access-list:** The type of the control list used in the filter rules

all|{0-99}: The serial number of the visit control list, if it is all, it means the entire defined visit control list.

port-list (all | {0-99}): Physical port list. If it is all, it means the entire physical ports.

ingress: Filtering in the receiving port

egress: Filtering in the transmitting port

both: Filtering in both the receiving and transmitting ports

vlan-list (all | {1-4094}): VLAN list. If it is all, it means all of the VLAN.

[default]

None.

[mode]

global configuration mode; privileged user.

[guide]

This command adds a filter rule to the linked list of the filter. The filter rules are composed of the defined visit control list and port or VLAN. The order of adding the matching rules when configuring the filter will decide the PRI of these rules. The latter the higher. If there are some conflicts of some rules when configuring the computer, it follows the priority rule, so when configuring the command, if there is conflict, please arrange properly the order of these rules, so that the matching message could be rightly filtered.

The command only configures the related filter rule. Whether the filter rules work at once will be decide by the global command switch. If the global command switch is on, it will be working at once, or else, it just adds the rules to the linked list of the filter rule, and it is not valid.

[Command Execution Echo]

- Set filter fail, lack of space!
- Set access list XX failed!
- Delete access list XX fail, there is no this filter!
- SUCCESS!
- The operation fail!

[example]

- filter ip-access-list 0 portlist 5 ingress

[relevant command]

Command	Description
Show filter	Show the related information of the filter configuration of the matching rules
filter enable disable	Start/Cancel the filter function

3.35 filter enable|disable

[Introduction]

This command will globally start the filter function of matching rules or disable the filter function.

filter enable | disable

[Parameter]

- **enable** start the filter function
- **disable** cancel the filter function

[Default]

disable

[Mode]

global configuration mode; privileged user.

[Guide]

None

[Command Execution Echo]

- SUCCESS!
- The operation fail!

[For example]

- **filter enable**

[Relevant command]

Command	Description
filter access-list	Add filter rule to the linked list of the rule filter
show filter	Show the related information of the filter setting of the matching rule

3.36 flowcontrol

[Function Introduction]

Enable or disable the flow control function at the physical port

flowcontrol { on | off }

[Parameter]

- **on** Enable flow control function
- **off** Disable flow control function

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

[Mode]

Ethernet physical interface configuration exec and privileged user

[Guide]

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

[Command Execution Echo]

- **SUCCESS!**
Flow control is set successfully

- *This operation failed!*
Flow control setup failed

[For example]

- Enable flow control function of physical port
*Raisecom(config-port)# **flowcontrol on***
- Disable flowcontrol function of physical port
*Raisecom(config-port)# **flowcontrol off***

[Relevant command]

Command	Description
Show interface port	Show flow control configuration of one or all physical ports.

3.37garp

[Function Introduction]

Set three timer value of GARP.

garp join <20-20000>

garp leave <60-20000>

garp leaveall <500-20000>

no garp join

no garp leave

no garp leaveall

[parameter]

- <20-20000> Timer value of GARP Join,unit is 10ms.
- <60-20000> Timer value of GARP Leave,unit is 10ms.
- <500-20000> Timer value of GARP LeaveAll,unit is 10ms.

[default]

- Join Default value is 20;
- Leave Default value is 60;
- LeaveAll Default value is 1000;

[mode]

Ethernet lay-2 interface configuration exec; privileged user.

[guide]

GARP agreement defined in 802.1D, third kinds of value of timer, should meet relation the following could guarantee GARP agreement work rationally.

Leave Time > 2 * (Join Time)

LeaveAll Time > Leave Time

[Command Execution Echo]

- set successfully.
- set fail.

[for example]

Set value of GARP timer is 30

Raisecom(config-aggregator)# **garp join 30**

[relevant commmand]

Command	Description
show garp timer	Show value of GARP timer

3.38 gmrp

[Function Introduction]

Enable or disable GMRP Protocol

gmrp {enable | disable}

[parameter]

- **enable** enable GMRP Protocol
- **disable** disable GMRP Protocol

[default]

GMRP Protocol is enabled on default condition.

[mode]

Global configuration mode or ethernet layer 2 interface configuration mode; privileged user.

[guide]

User can global enable or disable GMRP Protocol under global configuration mode
User can enable or disable GMRP Protocol under ethernet layer 2 interface configuration mode.

[Command Execution Echo]

- set successfully.
- set fail.

[for example]

- disable GMRP Protocol in global
Raisecom(config)# **gmrp disable**
- Disable GMRP on ethernet layer 2 interface
Raisecom(config-aggregator)# **gmrp disable**

[relevant command]

Command	Description
show gmrp	Show configuration information of GMRP

3.39 gvrp

[Function Introduction]

Enable or disable GVRP Protocol

gvrp {enable | disable}

[parameter]

- **enable** enable GVRP Protocol
- **disable** disable GVRP Protocol

[default]

GVRP Protocol is enabled on default condition.

[mode]

Global configuration mode or ethernet layer 2 interface configuration mode; privileged user.

[guide]

User can global enable or disable GMRP Protocol under global configuration mode.
User can enable or disable GMRP Protocol under ethernet layer 2 interface configuration mode.

[Command Execution Echo]

- set successfully.

- set fail.

[for example]

- disable GVRP Protocol in global
Raisecom(config)# **gvrp disable**
- Disable GMRP on ethernet layer 2 interfac
Raisecom(config-aggregator)# **gvrp disable**

[relevant commmand]

Command	Description
show gvrp	Show configuration information of GVRP

3.40help

[Function Introduction]

Use “help” to show the help information of system.

help

[Parameter]

None

[Mode]

Initial exec, privileged exec, global exec, VLAN exec, interface configuration exec, routing protocol configuration exec, normal user, and privileged user

[Guide]

Use this command to show using help information of command line.

[Command Execution Echo]

·ISCOMOS software provides advanced help feature. When you need help, you can press '?' in the command line at anytime.

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?').

[For example]

Raisecom>help

[Relevant command]

None

3.41 history

[Function Introduction]

Use this command to show history command.

history

[Parameter]

None

[Default]

The number of history command in memory is 20.

[Mode]

Initial exec, privileged exec, global exec, VLAN exec, interface configuration exec, routing protocol configuration exec, normal user, and privileged user

[Guide]

Use this command to show history command of each mode.

[Command Execution Echo]

```
· ter time-out 65535  
  enable  
  chin  
  enable  
  help  
  eng
```

[For example]

```
Raisecom>history
```

[Relevant command]

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

3.42hostname

[Function Introduction]

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

Use “no hostname” command to resume default value.

hostname *HOSTNAME*

no hostname

[Parameter]

HOSTNAME: System name of new appoint to user.

[Default]

The default value of hostname is raisecom.

[Mode]

Privileged exec and privileged user

[Guide]

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

[Command Execution Echo]

```
· Hostname length must less than 16 !  
· set successfully.
```

[For example]

```
Raisecom#hostname switch  
Change the hostname of the Switch to “switch”
```

[Relevant command]

None

3.43ip-access-list

[Function Introduction]

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

Set binding of IP address and physical port.

ip-access-list *list-number ip-confine-list list-number port port-number*

Set binding of IP address and VLAN.

ip-access-list *list-number ip-confine-list list-number vlan vlan_id*

no ip-access-list [*list-number*]

[parameter]

- **list-number** IP address access control list or confine of IP,range of 0-99.
- **ip-confine-list** IP confine list
- **port** physical port
- **port-number** the number of physical port,range from 1 to 26;
- **vlan** VLAN;
- **vlan_id** VLAN ID, range from 1 to 4094;

[default]

Not set IP address control list on default condition.

[mode]

global configuration mode; privileged user.

[guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- The ip-access-list X has been set.
- NO ip-confine-list X !
- IP access-list X in use ! Operation NOT accomplete!
- No IP access-list X !
- SUCCESS!

[for example]

- Set binding of IP address and physical port.
Raisecom(config)# **ip-access-list 0 ip-confine-list 2 port 5**
- Set binding of IP address and VLAN.
Raisecom(config)# **ip-access-list 1 ip-confine-list 3 vlan 3**
- Delete IP access control list 5
Raisecom(config)# **no ip-access-list 5**
- Delect all IP access control list
Raisecom(config)# **no ip-access-list**

[relevant commmand]

Command	Description
Filter ip-access-list	Set filter state of IP address access list.
show ip-access-list	Show one or all IP address access control list.
show access-list	Show all access control list.
no access-list	Delete all access control list.

3.44ip address

[Function Introduction]

Set IP address of current interface.

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

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

no ip address *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]

The current interface is not assigned IP address.

[Mode]

Ethernet layer 3 interface Configuration exec and privileged user

[Guide]

This command is used to assign interface IP address. 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.

[Command Execution Echo]

- Set successfully.
- This interface already associated with VLAN 4.
Command failed when associating an VLAN-associated interface with another VLAN ID
- Invalid network mask.
Command failed when setting an invalid subnet mask
- Invalid IP address or network mask.
Command failed when setting an invalid IP address or subnet mask
- VLAN 2 already associated with interface 2 (ifIndex: 1100003).
Command failed when associating a VLAN that associated with another IP interface
- 192.168.1.4 overlaps with interface 2 (ifIndex: 1100003).
Command failed when setting an interface IP address that confronted with other interfaces

[For example]

·Set IP address of current interface is 192.168.1.2, VLAN 2 associate with it.

```
Raisecom(config-ip)# ip address 192.168.1.2 255.255.255.0 2
```

·Delete IP address of current interface.

```
Raisecom(config-ip)# no ip address 192.168.1.2
```

[Relevant command]

Command	Description
State	Active current VLAN
vlan-access	Add current interface to VLAN
show ip route	Show VLAN information
show interface	Show interface of VLAN information
vlan	

3.45 ip forwarding

[Function Introduction]

Use "**ip forwarding**" to enable the ability of software transmit ip message, use "**no ip forwarding**" to stop this operation.

[no] ip forwarding

[parameter]

None

[default]

System forbid software to transmit ip message on default condition.

[mode]

(E)global configuration mode; privileged user.

[guide]

[Command Execution Echo]

set successfully.

[for example]

```
Raisecom(config)# ip forwarding
```

Enable IP transmission ability of software.

[relevant command]

None

3.46 ip igmp-snooping

[Function Introduction]

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

[no] ip igmp-snooping

[Parameter]

None

[Default]

IGMP Snooping protocol is valid on default condition.

[Mode]

Global configuration exec and privileged user

[Guide]

When IGMP Snooping is enabled, All the VLAN interfaces available will enable IGMP Snooping; when the function is cancelled, all the VLAN interfaces will cancel the function.

[Command Execution Echo]

- Enable igmp snooping success
- Enable igmp snooping failure
- Disable igmp snooping success
- Disable igmp snooping failure

[For example]

- Enable IGMP Snooping
Raisecom(config)# ip igmp-snooping
- Disable IGMP Snooping
Raisecom(config)#no ip igmp-snooping

[Relevant command]

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

3.47 ip igmp-snooping

[Function Introduction]

Use “**ip igmp-snooping**” to enable IGMP snooping on VLAN. Use “no ip igmp-snooping” to stop IGMP snooping function on VLAN.

[Command format]

ip igmp-snooping
[no] ip igmp-snooping

[Parameter]

None

[Default]

When IGMP Snooping is enabled, all VLAN enable IGMP Snooping on default condition.

[Mode]

VLAN configuration exec and privileged user

[Guide]

Use this command to enable IGMP snooping on VLAN. Use “**no ip igmp-snooping**” to disable IGMP snooping on VLAN.

[Command Execution Echo]

- enable igmp snooping on VLAN 1 success
- enable igmp snooping on VLAN 1 failure
- Disable igmp snooping on VLAN 1 success
- Disable igmp snooping on VLAN 1 failure

[For example]

- Enable IGMP Snooping on VLAN 1.
Raisecom(config-vlan)# ip igmp-snooping
- Disable IGMP Snooping on VLAN 1.
Raisecom(config-vlan)#no ip igmp-snooping

[Relevant command]

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

3.48 **ip igmp-snooping static mac-address port portid**

[Function Introduction]

Use this command to add a layer 2 port for the member of multicast group, use no to cancel this configuration.

[no] ip igmp-snooping static mac-address port portid

[parameter]

- *mac-address* appoint MAC address of static state group,format is HHHH.HHHH.HHHH;
- *portid* appoint the configured static switch port number, range 1-26, Integer type,

[default]

None

[mode]

VLAN configuration mode, privileged user.

[guide]

Use this command to add a layer 2 port for the member of multicast group, use no to cancel this configuration.

[Command Execution Echo]

- multicast MAC address ERROR
- join port in a assigned group on assigned VLAN success
- join port in a assigned group on assigned VLAN failure
- disable join port in a assigned group on assigned VLAN success
- disable join port in a assigned group on assigned VLAN failure

[for example]

- This example explain how add port 1 to group of 0100.5e02.0203.
Raisecom (config-vlan)# ip igmp snooping static 0100.5e02.0203 port 1
- This example explain how delete port 1 from group of 0100.5e02.0203.
Raisecom (config-vlan)# no ip igmp snooping static 0100.5e02.0203 port 1

[relevant commmand]

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

show ip-igmp snooping mrouter	Display multicast route port information of dynamic study of manual configuration.
show mac-address-table multicast	Display the L2 group cast entity of Switch or VLAN

3.49 ip igmp-snooping timeout

[Function 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 Appoint time of timeout, unit is second, range from 30 second to 3600 second-class is integer.

[Default]

Default value of timeout is 300 second.

[Mode]

Global configuration exec and privileged user

[Guide]

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

[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

[For 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

[Relevant command]

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

3.50 ip ospf authentication-password

[Introduction]

Set the password of the simple password authentication at the present port.

[no] ip ospf authentication-password *string*

[Parameter]

- *string* Set the password of the simple password authentication, 1-8 character

[Default]

The default state is without the setting of the simple password authentication

[Mode]

Ethernet layer 3 port configuration mode; privileged user.

[Guide]

The password created by this command will be written into the hello package, so that all the Router equipment in the same network must have the same password, so that the

OSPF information changing is possible.

Using **no ip ospf authentication-password** to delete the simple password authentication

[Command Execution Echo]

- set interface simple authentication password successful
- set interface simple authentication password fail

[For example]

- Set the password of the simple password authentication to qaz
Raisecom (config-ip)# **ip ospf authentication-password qaz**

[Relevant command]

Command	Description
network area	Define the interface of running OSPF and the area ID of these defined interface

3.51 ip ospf authentication-type

[Introduction]

Set the authentication type of the interface

[no] ip ospf authentication-type { simple-password | message-digest | none }

[Parameter]

- simple-password* simple password authentication
- message-digest* MD5 key authentication
- none* no authentication

[Default]

The default state is without authentication

[Mode]

Ethernet layer 3 port configuration mode; privileged user.

[Guide]

The authentication makes the message transmitting safer. The HELLO package of OSPF includes the authentication type and value, so the authentication type and value of Router equipment at the same net section must be consistent, or else, it will block the communication in the neighboring Router equipment.

Using **no ip ospf authentication_type** to delete the authentication configuration

[Command Execution Echo]

- set interface authentication type successful
- set interface authentication type fail

[For example]

- Set the interface authentication type to MD5
Raisecom (config-ip)# **ip ospf authentication-type message-digest**

[Relevant command]

Command	Description
network area	Define the OSPF interfaces and the defined area ID of these interfaces

3.52 ip ospf cost

[Introduction]

Set the transmitting cost at the present interface

[no] ip ospf cost cost

[Parameter]

·cost The cost value of the defined interface, an integer between 1-65535

[Default]

The default cost value is 10.

[Mode]

Ethernet layer 3 port configuration mode; privileged user.

[Guide]

When the transmitting interface of the Router equipment connects to the different types of network, the cost of the interface could be configured according to the transmitting ability of the practical network. Usually the cost configuration value is $10^8/BW$. BW is the configured band width of the interface. This value could be used when calculating the minimum route. OSPF will choose the minimum route of the cost value to be the best route.

Using the command **no ip ospf cost** to restore the parameter to the default value.

[Command Execution Echo]

·set interface cost successful
·set interface cost fail

[For Example]

Set the cost value of the interface to 128:

```
Raisecom(config-ip)# ip ospf cost 128
```

[Relevant command]

Command	Description
network area	Define the OSPF interfaces and the defined area ID of these interfaces

3.53 ip ospf dead-interval

[Introduction]

Set the invalid time interval of the present port neighbors

[no] ip ospf dead-interval seconds

[Parameter]

·seconds The time interval of the neighbors death, viz, if the hello package has not been received at this time interval, the communication between neighbors is considered to be broken, an integer between 1-65535, the unit is second.

[Default]

The invalid time interval of the present port neighbors is 40 seconds.

[Mode]

Ethernet layer 3 port configuration mode; privileged user.

[Guide]

The dead-interval value will be written into the HELLO package. When this equipment receives the HELLO package, it will check the dead-interval value in the HELLO package. If the dead-interval value in the HELLO package is not consistent with the received dead-interval, this message will be abandoned, so the dead-interval of the Router equipment at the same network must be consistent, or else it will affect the neighboring communication.

Using the command **no ip ospf dead-interval** to restore the parameter to the default value.

Dead-interval and hello-interval have a four times default relation, when hello-interval changes, the dead-interval will automatically change by four times, but when dead-interval changes, hello-interval will not change.

[Command Execution Echo]

- set interface dead interval successful
- set interface dead interval fail

[For example]

- Set the interface dead-interval to 120 seconds
Raisecom(config-ip)# **ip ospf dead-interval 120**

[Relevant command]

Command	Description
network area	Define the OSPF interfaces and the defined area ID of these interfaces

3.54 ip ospf hello-interval

[Introduction]

Set the time interval of sending hello package at the present port. When setting this value, it will automatically set the dead-interval value to four times the hello-interval.

[no] ip ospf hello-interval seconds

[Parameter]

·seconds The time interval for sending hello package, an integer between 1-65535, the unit is second.

[Default]

The default time interval of sending hello package at the present port is 10 seconds.

[Mode]

Ethernet layer 3 port configuration mode; privileged user.

[Guide]

The hello-interval value will be written into the HELLO message. When the Router equipment receives the HELLO package, it will check the hello-interval value in the HELLO package. If the dead-interval value in the HELLO package is not consistent with the received hello-interval, this message will be abandoned, so the hello-interval of the Router equipment at the same network must be consistent, or else it will affect the neighboring communication. The hello-interval should not be too small, or else the communication in the network will increase.

Using the command **no ip ospf hello-interval** to restore to the default value.

[Command Execution Echo]

- set interface hello interval successful
- set interface hello interval fail

[For example]

- Set the interface hello-interval to 60 seconds.
Raisecom(config-ip)# **ip ospf hello-interval 60**

[Relevant command]

Command	Description
network area	Define the OSPF interfaces and the defined area ID of these

3.55 ip ospf message-digest-key

[Introduction]

Set the md5 key.

[no] ip ospf message-digest-key *keyid md5 key*

[Parameter]

·*keyid* md5 key index, a decimal integer between 1-255

·*key* md5 key, 1-16 character

[Default]

The default state is without Md5 key.

[Mode]

Ethernet layer 3 port configuration mode; privileged user.

[Guide]

Usually every interface has a key, which is used to generate the confirmation information when sending the package and affirming the incoming package. The same key index on the neighboring Router equipment must have the same key value. It is suggested that every port has several keys. Every time a new key is added, the old one must be deleted, so that it will prevent that the old system continues to communicate with the hostility system knowing the old key. Assume that the present configuration is:

```
interface ip 4
```

```
ip ospf message-digest-key 10 md5 old
```

Now the configuration is changed to:

```
ip ospf message-digest-key 11 md5 new
```

The system assumes that the neighbors haven't got the new key, and it will send several copies of the same package, which is affirmed by different keys. In this case, the system will send two copies of the same package----the first one is confirmed by key 10, and the other one is confirmed by key 11.

When all the neighbors are using the new key, the old key should be deleted.

```
no ip ospf message-digest-key 10
```

So that the key is used on the interface for confirming.

Using the command **no ip ospf message-digest-key** to delete md5 key index and the key of this index. Using **no ip ospf authentication-type message-digest-key** to delete the md5 key authentication.

[Command Execution Echo]

```
·add message digest authentication key successful
```

```
·add message digest authentication key fail
```

[For example]

- Configuring the interface according to MD5 authentication:
Raisecom (config-ip)# **ip ospf message-digest-key 3 md5 aaa**
Raisecom (config-ip)# **ip osp authentication-type message-digest**

[Relevant command]

Command	Description
network area	Define the OSPF interfaces and the defined area ID of these interfaces

3.56 ip ospf priority

[Introduction]

Set the priority of the present interface. If the priority is 0, the Router cannot be DR/BDR.

[no] ip ospf priority *priority*

[Parameter]

·*priority* Set the present interface priority, and decimal integer between 0-256.

[Default]

The default priority is 1.

[Mode]

Ethernet layer 3 port configuration mode; privileged user.

[Guide]

The priority of the Router will affect the Defined Router(DE) and the election of the Backup Defined Router(BDR). If the priority is 0, it has no qualification to become DR or BDR. When the priority is the same, choose the bigger Router ID to be the DR or BDR.

DR is a special Router equipment on the broadcast network or the NBMA network. It takes charge of generating network-LSA and forming neighboring relations with the other Router equipment on the same network, so it avoids generating neighboring relations among all the Router equipment in the network and the communication quantity of the Router protocol will be decreased, so that the stability of the network will be enhanced.

Using command **no ip ospf priority** to restore to the default value.

[Command Execution Echo]

·set interface priority successful
·set interface priority fail

[For example]

- Set the Router equipment priority to 20:
Raisecom (config-ip)# **ip ospf priority 20**

[Relevant command]

Command	Description
network area	Define the OSPF interfaces and the defined area ID of these interfaces

3.57 ip ospf retransmit-interval

[Introduction]

Set the time interval for the present port to resend the lost LSA.

[no] ip ospf retransmit-interval *seconds*

[Parameter]

·*seconds* The time interval for the present port to resend the lost LSA. The value should not be too small, or else it will increase unnecessary communication quantity, an integer between 1-65535, the unit is second.

[Default]

5 seconds

[Mode]

Ethernet layer 3 port configuration mode; privileged user.

[Guide]

When a Router equipment sends the link route state bulletin to its neighbors, it will add the bulletin to the resending list and keep it until receiving the confirming form the other side. If in the resending interval no confirming is received, it will be send again. The defined resending interval should at least twice the time for sending and receiving a message. If the defined interval is too small, it will increase the unnecessary communication quantity.

Using **no ip ospf retransmit-interval** to restore to the default value.

[Command Execution Echo]

```
·set interface retransmit interval successful
·set interface retransmit interval fail·
```

[For example]

- Set the interval to 15 seconds
Raisecom (config-ip)# **ip ospf retransmit-interval 15**

[Relevant command]

Command	Description
network area	Define the OSPF interfaces and the defined area ID of these interfaces

3.58ip ospf transmit-delay

[Introduction]

Set the present port transmit delay

[no] ip ospf transmit-delay *seconds*

[Parameter]

```
·seconds Transmit delay, an integer between 1-65535, the unit is second.
```

[Default]

The default transmit delay is 1 second.

[Mode]

Ethernet layer 3 port configuration mode; privileged user.

[Guide]

To update the link route state bulletin, there must be the increased time quantity defined by the transmit-delay before transmitting. In the flood process, AGE will add an increased time quantity through every LSA jump. This increased time is the transmit delay.

Using **no ip ospf transmit-delay** to restore to the default value.

[Command Execution Echo]

```
·set interface transmit delay successful
·set interface transmit delay fail
```

[For example]

- Set the delay to 10 seconds
Raisecom (config-ip)# **ip ospf transmit-delay 10**

[Relevant command]

Command	Description
network area	Define the OSPF interfaces and the defined area ID of these interfaces

3.59ip rip auth-key

[Introduction]

Set the writing authentication password at the present port RIP protocol. Using command **no ip rip auth-key** to restore to the default configuration.

ip rip auth-key *string*

no ip rip auth-key

[Parameter]

·*string* writing authentication password, its data type is character string, its length is 1-16; no space in the password

[Default]

Vacant

[Mode]

Ethernet layer 3 port configuration mode; privileged user.

[Guide]

This command configures authentication for RIP protocol in the interface, it should be used with the command **ip rip auth-mode**. In the configuration of RIP authentication, whether the authentication mode is configured or not will decide the effectiveness of RIP authentication. If the mode is writing authentication without password, the authentication is effective and the password is vacant. If only the password is configured without the mode, it will not work, so when configuring the password, the authentication mode of the RIP protocol should be set to the writing authentication. When canceling the authentication, the mode should be set to non-authentication first. Only RIPv2 supports the authentication. RIPv1 do not support it.

[Command Execution Echo]

·set rip auth key is success

·set rip auth key is failure

[For example]

- Set the password to aaa
Raisecom(config-ip)# **ip rip auth-key** *aaa*
- Restore to the default configuration
Raisecom(config-ip)# **no ip rip auth-key**

[Relevant command]

Command	Description
ip rip auth-mode	Set the authentication mode of RIP protocol at the present interface
router rip	Set the RIP protocol to be effective, and enter the RIP protocol configuration mode
show ip protocol	Show the Router protocol configuration information

3.60 ip rip auth-mode

[Introduction]

Set the authentication mode of the RIP protocol at the present interface, Command **no ip rip auth-mode** will restore to the default configuration.

ip rip auth-mode { **none** | **text** }

no ip rip auth-mode

[Parameter]

·*none* There is no authentication

·*text* The mode is writing authentication.

[Default]

No authentication.

[Mode]

Ethernet layer 3 port configuration mode; privileged user.

[Guide]

The command **ip rip auth-mode** will set the authentication mode of the RIP protocol at the present interface to be writing or no authentication. Only RIPv2 supports this authentication. RIPv1 do not support it, but the configuring is successful. Command **no ip rip auth-mode** could easily restore to the default configuration.

[Command Execution Echo]

- set rip auth mode is successful
- set rip auth mode is failure

The cause of failure might be that the interface does not configure IP address.

[For example]

- Set it to writing authentication
Raisecom(config-ip)# **ip rip auth-mode text**
- Set it to on authentication
Raisecom(config-ip)# **no ip rip auth-mode**

[Relevant command]

Command	Description
ip rip auth-key	Set the authentication mode of RIP protocol at the present interface
router rip	Set the RIP protocol to be effective, and enter the RIP protocol configuration mode
show ip protocol	Show the Router protocol configuration information

3.61 ip rip metric-default

[Introduction]

The attaching measuring value added to the Router when configuring the receiving and transmitting RIP message at the present interface. Command **no ip rip metric-default** will restore to the default configuration.

ip rip metric-default value

no ip rip metric-default

[Parameter]

·value The attaching measuring value added to the Router when configuring the receiving and transmitting RIP message at the present interface set by the client. The data type is integer, and the range is [0, 15].

[Default]

The default value is 1.

[Mode]

Ethernet layer 3 port configuration mode; privileged user.

[Guide]

Using the command **ip rip metric-default**, the attaching measuring value added to the received RIP router by the present interface could be configured. It means the cost of the Router going through this node. The clients can configure properly according to the needs. Using command **no ip rip default-metric** will restore to the default value.

[Command Execution Echo]

- set rip default metric is success
- set rip default metric is failure

[For example]

- Set the value to 6
Raisecom(config-ip)# **ip rip metric-default 6**
- Restore to the default configuration
Raisecom(config-ip)# **no ip rip metric-default**

[Relevant command]

Command	Description
router rip	Set the RIP protocol to be effective, and enter the RIP protocol configuration mode
show ip protocol	Show the Router protocol configuration information

3.62ip rip receive-version

[Introduction]

Set the RIP message version that could be received by the present interface. Using command **no ip rip receive-version** will restore to the default value.

ip rip receive-version { v1 | v2 | v1v2 | donotrecieve }
no ip rip receive-version

[Parameter]

- v1 The present interface only accepts RIPv1 message
- v2 The present interface only accepts RIPv2message
- v1v2 The present interface accepts both the RIPv1 and RIPv2message
- donotrecieve The present interface accepts no version.

[Default]

The present interface can receive any version of RIP message.

[Mode]

Ethernet layer 3 port configuration mode; privileged user

[Guide]

Through the command **ip rip receive-version** the version of the RIP message could be configured at the present interface. Some version of the message could be masked without dealing with. When it is configured to RIPv2, RIPv1 message will not be accepted.

Using command **no ip rip receive-version** any version of RIP message will not be accepted.

[Command Execution Echo]

- set rip receive version is success
- set rip receive version is failure

[For example]

- Set the version to RIPv2
Raisecom(config-ip)# **ip rip receive-version v2**
- Restore to default configuration
Raisecom(config-ip)# **ip rip receive-version v1v2**
- Restore to default configuration
Raisecom(config-ip)#**no ip rip receive-version**

[Relevant command]

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

router rip	Set the RIP protocol to be effective, and enter the RIP protocol configuration mode
show ip protocol	Show the Router protocol configuration information

3.63 ip rip send-version

[Introduction]

Set the RIP version sending at the present interface. Using command **no ip rip send-version** will restore to the default configuration.

ip rip send-version { v1 | multicastv2 | broadcastv2 | donotsend }
no ip rip send-version

[Parameter]

- v1 The present interface only sends RIPv1 message.
- multicastv2** The present interface only sends RIPv2 multicast message.
- broadcastv2** The present interface only sends RIPv2 broadcast message.
- Donotsend** The present interface sends no version.

[Default]

Only sending version 1 RIP message.

[Mode]

Ethernet layer 3 port configuration mode; privileged user

[Guide]

The version of the RIP message that could be sent by the present interface could be configured using the command **ip rip send-version**. Using command **no ip rip send-version** will restore to the default configuration.

[Command Execution Echo]

- set rip send version is success
- set rip send version is failure

[For example]

- Only send the RIPv2 message
Raisecom(config-ip)# **ip rip send-version multicastv2** or **broadcastv2**
- Restore to default configuration
Raisecom(config-ip)# **ip rip send-version v1**
- Restore to default configuration
Raisecom(config-ip)# **no ip rip send-version**

[Relevant command]

Command	Description
passive	Any version of RIP message will not be sent
router rip	Set the RIP protocol to be effective, and enter the RIP protocol configuration mode
show ip protocol	Show the Router protocol configuration information

3.64 ip rip split-horizon

[Introduction]

Start the horizon split mechanism to prevent Router loopback. Using the command **no ip rip split-horizon** to shut down the mechanism.

[no]ip rip split-horizon

[Parameter]

None

[Default]

In the default state, the horizon split mechanism is already started.

[Mode]

Ethernet layer 3 port configuration mode; privileged user

[Guide]

The horizon split mechanism will stop the Router message to return to the original sending direction. The horizon split mechanism could be simply described as follow: If the interface for sending the RIP Router is the same with the one receiving it, it is necessary to set the Router measuring value to infinity (viz 16) before sending. In this way, the loopback in the network could be effectively prevented and the unreachable message will be informed to the neighboring in time, so that it effectively shorten the convergence time, but the broadcasting of a route whose cost is a 16 invalid Router will bring in attached information. Using command **no ip rip split-horizon** will restore to the default value.

[Command Execution Echo]

- set rip split is success
- set rip split is failure·

[For example]

- Set the horizon split mechanism
Raisecom(config-ip)# **ip rip split-horizon**
- Cancel the horizon split mechanism
Raisecom(config-ip)# **no ip rip split-horizon**

[Relevant command]

None.

3.65 ip route

[Function Introduction]

Use "ip route" to add static route, use "no ip route" to delete static route.

ip route *A.B.C.D₁ E.F.G.H₂ a.b.c.d₃*

no ip route [*A.B.C.D₁ [E.F.G.H]*]

[parameter]

- *A.B.C.D₁* network prefix
- *E.F.G.H₂* mask
- *a.b.c.d₃* 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.

[mode]

global configuration mode; privileged user.

[guide]

Static route is configured by network administrator, this route transmission will change with network topology, next-hop route must be direct route when use "**ip route**" to add route.

[Command Execution Echo]

- Invalid Destination IP address.
- Invalid Destination MASK.

- Invalid Next-hop IP address.
- Can not set Connected Route to Static.
- set successfully.

[for 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**

[relevant commmand]

Command	Description
show ip route	Show information of route

3.66 ip route age

[Function Introduction]

Use “**ip route age**”to set aging time of route in hardware.

ip route age <60-65535>

no ip route age

[parameter]

<60-65535> age time of hardware route,unit is second.

[default]

The default value of route aging time is 180 second.

[mode]

global configuration mode; privileged user.

[guide]

Route number is limited of hardware,it need to be aged periodic,this command set or resume the route age of hardware.

[Command Execution Echo]

set successfully.

[for example]

- Set aging time of route in hardware is 100 second.
Raisecom(config)# **ip route age** 100
- Resume aging time of route in hardware is 180 second.
Raisecom(config)#**no ip route age**

[relevant commmand]

Command	Description
show ip route hardware	Show ip route, which is in hardware

3.67 ip route gateway

[Function Introduction]

Use “**ip route gateway**”to set default gateway,use “ **no ip route gateway**”to delete default gateway.

ip route gateway A.B.C.D

no ip route gateway

[parameter]

A.B.C.D IP address of default gateway.

[default]

There is no default gateway in default.

[mode]

global configuration mode; privileged user.

[guide]

When a output message not find the route of destination network,use command to transmit all message to default gateway.

[Command Execution Echo]

set successfully.

[for example]

- Set default gateway is 10.0.0.1
Raisecom(config)# **ip route gateway** 10.0.0.1
- Delete default gateway
Raisecom(config)# **no ip route gateway**

[relevant commmand]

Command	Description
show ip route	Show route information of system

3.68ip route fast

[Introduction]

Using **ip route fas** to start the ip fast transmitting function. Using the command in the no format to prohibit this operation.

[Parameter]

None

[Default]

The default state is ip fast transmitting.

[Mode]

Global configuration mode; privileged user.

[Guide]

Using this command, the load on CPU could be released. The added static Router and direct linking Router will be directly written in to the network Router. The direct linking Router interface is 27 (stand for CPU), and the MAC address is the on of the Switch. In the fast transmit mode, RIP/OSPF only sends Router, but not learns Router. It is suggested not to use RIP OSPF and related Router protocol in this mode.

[Command Execution Echo]

- set ip route fast successful.
- set ip route fast failure.

[For example]

- A
-

[Relevant command]

Command	Description
show ip route hardware	Show the Router in the hardware

3.69ip static-route-distance

[Function Introduction]

Use "**ip static-route-distance**"to set protocol distance of static route,use "**no ip static-route-distance**"to resume default value.

ip static-route-distance <1-200>

no ip static-route-distance

[parameter]

<1-200> Protocol distance of be set.

[default]

Default protocol distance of static route protocol is 185.

[mode]

global configuration mode; privileged user.

[guide]

Protocol distance let route appear difference that is studied by different route. Use this order to alter the distance of the agreement, while making the protocol inn transmit, to the same route, choose to be used according to different distance of protocol.

[Command Execution Echo]

set successfully.

[for example]

- Set protocol distance of static route is 100.
Raisecom(config)# **ip static-route-distance 100**
- Resume default value of static route.
Raisecom(config)# **no ip static-route-distance**

[relevant commmand]

Command	Description
show ip protocol	Show information of IP route protocol

3.70 interface ip

[Function Introduction]

Enter IP interface mode.

interface ip <0-15>

[Parameter]

<0-15> the number of IP interface

[Default]

All IP interface of system is not assigned address on default condition.

[Mode]

Global configuration exec and privileged user

[Guide]

Use “interface ip” to enter IP interface mode.

[For example]

Enter configuration mode of IP interface 4.
Raisecom (config)# **interface ip 4**

[Relevant command]

Command	Description
ip address	Set IP address of current interface.
show interface vlan	Show interface of layer 3

3.71 interface port

[Function Introduction]

Enter physical interface mode.

interface port <1-26>

[Parameter]

<1-26> Number of physical interface

[Default]

All physical interface of system is not assigned on default condition.

[Mode]

Global configuration exec and privileged user

[Guide]

Use “**interface port**” to enter configuration mode of physical interface.

[For example]

Enter configuration mode of physical interface 4.

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

[Relevant command]

Command	Description
show interface port	Show information of physical port

3.72 interface aggregator

[Function Introduction]

Enter aggregation interface mode.

interface aggregator <1-26>

[parameter]

<1-26> Number of aggregation interface.

[default]

All aggregation interface of system is not configured on default condition.

[mode]

global configuration mode; privileged user.

[guide]

Use “**interface aggregator**” to enter configuration mode of aggregation interface.

[for example]

Enter configuration mode of aggregation interface 4.

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

[relevant command]

None

3.73 lacp

[Function Introduction]

Enable and disable Link Aggregation Control Protocol.

lacp {**enable** | **disable**}

[parameter]

- **enable** Enable Link Aggregation Control Protocol;
- **disable** Disable Link Aggregation Control Protocol;

[default]

On default condition, Link Aggregation Control Protocol of switch is disabled.

[mode]

global configuration mode; privileged user.

[guide]

Link Aggregation Control Protocol must be enabled before use relevant command of other Link Aggregation function.

[Command Execution Echo]

- set successfully.
- set fail.

[for example]

Enable Link Aggregation Control Protocol
 Raisecom (config)# **lACP enable**

[relevant command]

Command	Description
lACP	Set system priority of LACP
system-priority	
lag	Set loading-sharing mode of aggregation link
loading-sharing	
lACP admin-key	Set LACP admin-key of Ethernet physical interface.
lACP priority	Set LACP priority of ethernet physical interface.
lACP mode	Set link aggregation mode of ethernet physical interface.
show lACP lag-id	Show aggregation ID information of LACP.
show lACP ports	Show aggregation and configuration information of LACP physical interface and aggregation interface.

3.74 lACP admin-key

[Function Introduction]

Set LACP admin-key of ethernet physical interface.

lACP admin-key <1-1024>

no lACP admin-key

[parameter]

<1-1024> Admin-key value that is used by LACP in aggregation negotiation process.

[default]

On default condition, the LACP admin-key value of physical interface is 1.

[mode]

Ethernet physical interface configuration mode; privileged user.

[guide]

Physical interface can be aggregated only if they have same physical interface admin-key.

[Command Execution Echo]

- set successfully.
- set fail.

[for example]

Set LACP admin-key of physical interface is 2.
 Raisecom (config-port)# **lACP admin-key 2**

[relevant command]

Command	Description
LACP	enable or disable LACP
lACP	Set system priority of LACP
system-priority	
lag loading-sharing	Set loading-sharing mode of LACP aggregation link
lACP admin-key	Set LACP admin-key of Ethernet physical interface.
lACP priority	Set LACP priority of ethernet physical interface.

lacp mode	Set link aggregation mode of ethernet physical interface.
show lacp lag-id	Show aggregation ID information of LACP.
show lacp ports	Show aggregation and configuration information of LACP physical interface and aggregation interface.

3.75lag loading-sharing

[Function Introduction]

Set loading-sharing mode of aggregation link.

lag loading-sharing {1 | 2 | 3 | 4 | 5 | 6}

no lag loading-sharing

[parameter]

- 1 Loading-sharing mode 1,select transmission port according to source MAC address.
- 2 Loading-sharing mode 2, select transmission port according to destination MAC address.
- 3 Loading-sharing mode 3, select transmit port based on the result of logic xor of destination and source MAC address.
- 4 Loading-sharing mode 4, select transmission port according to source IP address.
- 5 Loading-sharing mode 5, select transmission port according to destination IP address.
- 6 Loading-sharing mode 6, select transmit port based on the result of logic xor of destination and source IP address.

[default]

Loading-sharing mode of aggregation link is 1,on default condition.

[mode]

Ethernet layer 2 interface configuration mode; privileged user.

[guide]

Users can select different loading shared mode based on LACP lag-link,such as the link is used to connect layer 3 switch,so that router is afford to access layer,loading shared mode based on source MAC address must be selected,because destination MAC address of data stream is the same by lag-link but source MAC address is not.

[Command Execution Echo]

- set successfully.
- set fail.

[for example]

Set loading-sharing mode of aggregation link is 2, select transmission port according to destination MAC address.

raisecom(config-aggregator)# **lacp loading-sharing 2**

[relevant commmand]

Command	Description
lacp	enable or disable LACP
lag system-priority	Set system priority of LACP
lacp admin-key	Set LACP admin-key of Ethernet physical interface.
lacp priority	Set LACP priority of ethernet physical interface.
lacp mode	Set link aggregation mode of ethernet physical interface.
show lacp lag-id	Show aggregation ID information of LACP.
show lacp ports	Show aggregation and configuration information of LACP

3.76 lACP mode

[Function Introduction]

Set link aggregation mode of ethernet physical interface.

lACP mode {*on* | *off* | *active* | *passive*}

no lACP mode

[parameter]

- *on* Manual link aggregation mode, which according to admin-key aggregate not negotiate with counterpart.
- *off* Disable link aggregation mode
- *active* LACP active negotiation link aggregation mode.
- *passive* LACP passive negotiation link aggregation mode.

[default]

On default condition, every link aggregation mode of physical interface is passive.

[mode]

Ethernet physical interface configuration mode; privileged user.

[guide]

- When physical interface is on mode, it happens link aggregation with other coincident physical interface of on mode not through LACP negotiation.
- When physical interface is off mode, it will not happen link aggregation.
- When physical interface is active mode, it will negotiate with counterpart, and transmit LACP frame actively, it turns coincident port to aggregation link maximum through negotiation.
- When physical interface is passive mode, it takes part in negotiation with counterpart passively, this port transmits LACP responsive frame only when counterpart is active mode.

A pair of ports happens link aggregation only when they accord with three combinations.

- on corresponding on;
- active corresponding passive;
- active corresponding active;

[Command Execution Echo]

- set successfully.
- set fail.

[for example]

Set link aggregation mode of physical interface is active.
Raisecom(config-port)# **lACP mode active**

[relevant command]

Command	Description
lACP	enable or disable LACP.
lACP system-priority	Set system priority of LACP
lag loading-sharing	Set loading-sharing mode of LACP aggregation link.
lACP admin-key	Set LACP admin-key of ethernet physical interface.
lACP priority	Set LACP priority of ethernet physical interface.
show lACP lag-id	Show aggregation ID information of LACP.
show lACP ports	Show aggregation and configuration information of LACP physical interface and aggregation interface.

3.77 lACP priority

[Function Introduction]

Set LACP priority of ethernet physical interface.

lACP priority <1-255>

no lACP priority

[parameter]

<1-255> The value of LACP port priority.

[default]

On default condition, the value of physical interface LACP priority is 128.

[mode]

Ethernet physical interface configuration mode; privileged user.

[guide]

LACP use physical interface priority and physical interface number to confirm physical interface ID only, port of smaller priority value take priority of happen aggregation.

[Command Execution Echo]

- set successfully.
- set fail.

[for example]

Set LACP physical interface priority of physical interface is 2.

Raisecom(config-port)# **lACP priority 2**

[relevant command]

Command	Description
lACP	enable or disable LACP
lACP system-priority	Set system priority of LACP
lAG loading-sharing	Set loading-sharing mode of LACP aggregation link.
lACP admin-key	Set LACP admin-key of ethernet physical interface.
lACP mode	Set link aggregation mode of ethernet physical interface
show lACP lAG-id	Show aggregation ID information of LACP.
show lACP ports	Show aggregation and configuration information of LACP physical interface and aggregation interface.

3.78 lACP system-priority

[Function Introduction]

Set system priority of Link Aggregation Control Protocol.

lACP system-priority <1-65535>

no lACP system-priority

[parameter]

<1-65535> System priority value of Link Aggregation Control Protocol.

[default]

On default condition, the system priority of Link Aggregation Control Protocol is 32768.

[mode]

global configuration mode; privileged user.

[guide]

Link Aggregation Control Protocol use system priority and system MAC address to confirm one ID of system,use it during link aggregation negotiation,the switch port of lower system ID is selected aggregation port priority.

[Command Execution Echo]

- set successfully.
- set fail.

[for example]

Set system priority of Link Aggregation Control Protocol is 10000.
 Raisecom(config)# **lacp system-priority 10000**

[relevant commmand]

Command	Description
lacp	enable or disable LACP
lag	Set loading-sharing mode of LACP aggregation link.
loading-sharing	
lacp admin-key	Set LACP admin-key of ethernet physical interface.
lacp priority	Set LACP priority of ethernet physical interface
lacp mode	Set link aggregation mode of ethernet physical interface
show lacp lag-id	Show aggregation ID information of LACP.
show lacp port	Show aggregation and configuration information of LACP physical interface and aggregation interface.

3.79list

[Function Introduction]

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

list

[Parameter]

None

[Mode]

Initial exec, privileged configuration exec, global configuration exec, VLAN configuration exec, interface configuration exec, routing protocol configuration exec; normal user and privileged user

[Guide]

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

[Command Execution Echo]

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

[For example]

Raisecom>list

[Relevant command]

None

3.80 logging console

[Function Introduction]

Configure and start to output the log information and parameters to console, the “no” command will disable the log output direction.

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

no logging console

[Parameter]

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

[Default]

The direction of console log host is open.

Output grade is informational.

[Mode]

Global configuration exec and privileged user

[Guide]

Use this command to configure output to console.

Log description of output to console.

Grade	key	Grade	Description
word			
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

[Command Execution Echo]

·set successfully!
·set fail!

[for example]

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

logging console alerts

[Relevant 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

3.81 logging file

[Function Introduction]

Configure and start to output the log information and parameters to console, the “no” command will disable the log output direction.

logging file

no logging file

[Parameter]

None

[Default]

Enable file direction output of log.

The mode of output is config.

[Mode]

Global configuration exec and privileged user

[Guide]

Use this command to configure log information output to flash file.

[Command Execution Echo]

.set successfully!

.set fail!

[For example]

Use this command to record log information output to file.

logging file

[Relevant 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

3.82 logging host

[Function Introduction]

Configure and start to output the log information and parameters to console, the “no” command will disable the log output direction.

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	(grade=1)
·critical	serious state	(grade=2)
·debugging	debug information	(grade=7)
·emergencies	system not available	(grade=0)
·errors	error condition	(grade=3)
·informational	informational event	(grade=6)
·notifications	normal and critical event	(grade=5)
·warnings	warning condition	(grade=4)

[Default]

No configuration information of log host

[Mode]

Global configuration exec and privileged user

[Guide]

Use this command to configure output to host log.

Log description of output to console

Grade	Grade	Description
keywords		
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

[Command Execution Echo]

·set successfully!
· set fail!

[For example]

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

logging host 10.0.0.1 local7 alerts

[Relevant 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

3.83 logging monitor

[Function Introduction]

Configure and start to output the log information and parameters to console, the “no”

command will disable the log output direction.

logging monitor {<0-7> | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings}
no logging monitor

[Parameter]

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

[Default]

The direction of monitor log host is close.

[Mode]

Global configuration exec and privileged user

[Guide]

Use this command to configure output to monitor.

Log description of output to monitor

Grade	Grade	Description
keywords		
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

[Command Execution Echo]

· *set successfully!*
· *set fail!*

[For 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

[Relevant 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

3.84 logging on

[Function Introduction]

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

[no] logging on

[Parameter]

None

[Default]

Log function is enabled

[Mode]

Global configuration exec and privileged user

[Guide]

Enable log function

[Command Execution Echo]

·set successfully!

·set fail!

[For example]

Enable log function

logging on

[Relevant 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

3.85 logging rate

[Function Introduction]

Set send speed of log information, use “no” to resume default setting.

logging rate <1-65535>

no logging rate

[Parameter]

<1-65535> Log number of every second send

[Default]

Not limit send speed of log

[Mode]

Global configuration exec and privileged user

[Guide]

Set send speed of log information

[Command Execution Echo]

· set successfully!

·set fail!

[For example]

Set every second to send 100 item logs most.

logging rate 100

[Relevant 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

3.86 logging time-stamp

[Function Introduction]

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

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

[no] logging time-stamp

[Parameter]

standard standard time
relative-start relative time of system enabled
null not add time stamp

[Default]

Use standard time

[Mode]

Global configuration exec and privileged user

[Guide]

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

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

Relative time hh-mm-ss

[Command Execution Echo]

.set successfully!
.set fail!

[For example]

Enable log relative time

logging time-stamp relative-start

[Relevant 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

3.87 logout

[Function Introduction]

Use "logout" to exit login state.

logout

[Parameter]

None

[Mode]

Privileged configuration exec and privileged user

[Guide]

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

[Command Execution Echo]

None

[For example]

Raisecom#logout

[Relevant command]

None

3.88 Loopback-detection

[Introduction]

Start/Close the loopback detection function of the specified port

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

[Parameter]

- *enable* start the loopback detection function
- *disable* close the loopback detection function
- *portlist* start the interface list of the loopback detection function, range between 1-26
- *all* all the interface

[Default]

All the port loopback detection function is enabled

[Mode]

Global configuration mode, privileged user (privilege 15)

[Guide]

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

[Command Execution Echo]

- The input port list is wrong!
- The interface number is not between 1-26
- Failed to set loopback-detection on port X!
- SUCCESS!
- FAILED !

[For example]

- Start the loopback detection function on interface 6-10
Raisecom(config)# **loopback-detection** enable **port-list** 6-10
- Start the loopback detection function on all the interface
Raisecom(config)# **loopback-detection** enable **port-list** all
- Close the loopback detection function on interface 7-9
Raisecom (config)# **loopback-detection** disable **port-list** 7-9
- Close the loopback detection function on all the interface
Raisecom (config)# **loopback-detection** disable **port-list** all

[Relevant command]

Command	Description
show loopback-detection	Show the interface loopback detection state

3.89 Loopback-detection interval

[Introduction]

Set the period for loopback detecting (viz the time interval of the interface sending the checking package). Restore to default using **no**.

loopback-detection interval <1-65535>

no loopback-detection interval

[Parameter]

· 1-65535 Loopback checking period, the unit is second

[Default]

The period is 4 seconds

[Mode]

Global configuration mode, privileged user (privilege 15)

[Guide]

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

[Command Execution Echo]

· Failed to set sending interval !

· SUCCESS!

[For example]

- Set the period to 3 seconds
Raisecom(config)# **loopback-detection interval 3**
- Restore to default value
Raisecom (config)# **no loopback-detection interval**

[Relevant command]

Command	Description
show loopback-detection	Show the interface loopback detection state

3.90name

[Function Introduction]

Set name of static VLAN.

name *WORD*

[Parameter]

The name shall not be more than 80 characters

[Default]

On default condition, the name of system default VLAN(VLAN1) is "Default", other name of static VLAN is character "VLAN" add four numerical digit VLAN ID, for example, the default name of VLAN1 is "VLAN0001", VLAN 4094 default name is "VLAN4094"

[Mode]

Static VLAN configuration exec, privileged user

[Command Execution Echo]

- set successfully.
- set fail.

[For example]

Set name of VLAN 2 is "R&D"
Raisecom(config-vlan)# **name R&D**

[Relevant command]

Command	Description
vlan	Enter static VLAN configuration mode
state	Set activity state of static VLAN

shutdown	Disable/enable static VLAN configuration
pvid	Set port VLAN ID attribute of port
vlan-access	Set VLAN access attribute of port
show vlan static	Show configuration information of static VLAN
show vlan current	Show configuration information of current activity VLAN

3.91 pvid

[Function Introduction]

Set port VLAN ID of port

pvid <1-4094>

[Parameter]

<1-4094> VLAN ID

[Default]

On default condition, the port VLAN ID (PVID) of all ports is 1

[Mode]

Ethernet physical interface configuration exec; privileged user

[Guide]

When switch port receive untagged message, switch use this port PVID to fill default 802.1Q label, the VLAN ID in label use PVID of this port's can isolate network equipment of without 802.1Q function through setting port PVID, equal to port VLAN.

[Command Execution Echo]

- *VLAN VID not exist.*
VID stands for VLAN ID. This echo shows when there is no such VLAN is system
- *Port PORTID not in vlan VID.*
This echo shows when the port is not in the designated VLAN, it is not permitted to set the PVID of this port to the designated VLAN ID.
- *set successfully.*
- *set failed.*

[For example]

Set port PVID is 2

Raisecom(config-port)# pvid 2

[Relevant command]

Command	Description
vlan	Enter static VLAN configuration mode
name	Set name of static VLAN
state	Set activity state of static VLAN
shutdown vlan	Disable/enable static VLAN
vlan-access	Set VLAN access attribute of port
show vlan static	Show configuration information of static VLAN
show vlan current	Show configuration information of current activity VLAN

3.92 mac-access-list

[Function Introduction]

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

Set binding of MAC and physical port

mac-access-list *list-number mac-address HHHH.HHHH.HHHH port port-number*

{ **deny** | **permit** }

Set binding of MAC and VLAN.

mac-access-list *list-number* **mac-address** *HHHH.HHHH.HHHH* **vlan** *vlan_id* { **deny** | **permit** }

Set binding of MAC and IP address.

mac-access-list *list-number* **mac-address** *HHHH.HHHH.HHHH* **ip-address** *A.B.C.D* [**mask** *A.B.C.D*] { **deny** | **permit** }

no mac-access-list [*list-number*]

[parameter]

- *list-number* The number of MAC access control list,range from 0 to 99
- *HHHH.HHHH.HHHH* MAC address,input format is hexadecimal character,dotted by every 4 characters.
- **port** physical port
- *port-number* the number of physical port,range from 1 to 26
- **vlan** VLAN;
- *vlan_id* VLAN ID,range from 1 to 4094
- **ip-address** IP address
- *A.B.C.D* IP address or mask,input format is dotted decimal;
- **mask** IP address mask;
- **deny** deny access;
- **permit** permit access

[default]

It is not configurate MAC access control list on default condition.

[mode]

global configuration mode, privileged user.

[guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- The mac-access-list X has been set.
- Set failed! This MAC address has been set!
- SUCCESS!
- The ip address is wrong!
- The mask is wrong!
- Set failed! This MAC address with this ip address has been set!
- MAC access-list X in use ! Operation NOT accomplete!
- No MAC access-list X !

[for example]

- Set binding of MAC address and port 5,deny access
Raisecom(config)# **mac-access-list 0 mac-address 1111.2222.3333 port 5 deny**
- Set binding of MAC address and VLAN 2,deny access
Raisecom(config)# **mac-access-list 1 mac-address 2222.3333.4444 vlan 2 deny**
- Set binding of MAC address and IP address,permit access
Raisecom(config)# **mac-access-list 2 mac-address 3333.4444.5555 ip-address 10.2.3.5 permit**
- Delete MAC access list 5
Raisecom(config)# **no mac-access-list 5**
- Delete all MAC access list
Raisecom(config)# **no mac-access-list**

[relevant commmand]

Command	description
filter mac-access-list <i>list-number</i> { enable disable } { source destination }	Set filter state of MAC access list

show mac-access-list [<i>list-number</i>]	Show one or all MAC access control list
show access-list	Show all access control list
no access-list	Delete all access control list

3.93 mac-address-table aging-time

[Function Introduction]

Set aging time of MAC address,use “no”command to detete this operation.

mac-address-table aging-time { *0* | *time* }

no mac-address-table aging-time

[parameter]

- **aging-time** aging time
- *0* forbid aging
- *time* aging time,unit is second,range from 10 to 1000000;

[default]

Aging time is 300 second,on default condition.

[mode]

global configuration mode, privileged user.

[guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- SUCCESS!
- This operation failed !

[for 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**

[relevant commmand]

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

3.94 mac-address-table learning

[Function Introduction]

Set enable and disable MAC address study function of physical port.

mac-address-table learning { **enable** | **disable** } **port** *port-number*

[parameter]

- **enable** enable study function
- **disable** disable study function
- **port** physical port
- *port-number* the number of port,range from 1 to 26;

[default]

On default condition,the study function of MAC address is enabled.

[mode]

global configuration mode, privileged user.

[guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- SUCCESS!
- This operation failed!

[for example]

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

[relevant command]

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

3.95 mac-address-table static

[Function Introduction]

Set static MAC address, use “no” to cancel this operation.

[no] mac-address-table static HHHH.HHHH.HHHH vlan vlan_id port port-number

[parameter]

- **static** static address
- *HHHH.HHHH.HHHH* MAC address, input format is hexadecimal character, dotted by every 4 characters.
- **vlan** VLAN;
- *vlan_id* VLAN ID, range from 1 to 4094;
- **port** physical port
- *port-number* the number of physical port, range from 1 to 26

[default]

Not set static MAC address on default condition.

[mode]

global configuration mode, privileged user.

[guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- SUCCESS!
- ERROR! Port X is not in vlan Y!
- This static mac address has been set!
- no this static mac address
- Failed! Port X is DOWN!

[for example]

- Set static MAC address that binding with VLAN 1 for port 3
Raisecom(config)# **mac-address-table static 1234.abcd.0000 vlan 1 port 3**
- Delete static MAC address that binding with VLAN 1 for port 3
Raisecom(config)# **no mac-address-table static 1234.abcd.0000 vlan 1 port 3**

[relevant command]

Command	Description
show mac-address-table static	Show one or all static address of port or VLAN.

3.96 mirror monitor_port

[Function Introduction]

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

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.

[Mode]

Global configuration exec and privileged user

[Guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- The monitor port has been set, please clear it!
This echo shows when setting a monitoring port that has been set to monitoring port before. Please set up after deletion of previous setup.
- The port X has been set to be mirror port !
The physical port X has been set to mirroring port, and cannot be set to monitoring port. Please set up other non-mirroring port or cancel mirroring port at port X.
- SUCCESS!
Set up mirroring port successful
- No mirror-to port!
This echo shows when deleting a mirroring port before setting it

[For example]

- Set port 5 is monitor port of mirror function.
Raisecom(config)# mirror monitor_port 5
- Delete mirror port
Raisecom(config)# no mirror monitor

[Relevant command]

Command	Description
mirror source_port	Set mirror port and rule
no mirror all	Delete all mirror configuration
show mirroring	Show all mirror configuration
show monitor	Show monitor port of set

3.97 mirror source_port

[Function Introduction]

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

mirror source_port *port_number*

no mirror source_port *port_number*

no mirror all

[Parameter]

- **source_port** mirror port
- *port_number* the number of physical port, range from 1 to 26, use “,”, “-” to multi port input.
- **all** all setting of mirror

[Default]

- On default condition, not set mirror port.

[Mode]

Global configuration exec and privileged user (priority 15)

[Guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- The mirror is off, please let it on first!
The mirroring function is disabled.
- The port list wrong!
Error occurred when enter multi ports using “-“ and “,”.
- Wrong! The port X is monitor port!
The port X is already a monitoring port.
- SUCCESS!
Command successful.
- This operation failed!
Command failed.
- The port %d has not been mirror!
Error occurred when performing deletion at non-mirroring port X.

[For 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**

[Relevant command]

Command	Description
mirror monitor_port <i>port_number</i>	Set monitor port of mirror rule
show mirroring source_port <i>port_number</i>	Show mirror setting of one port
show mirroring	Show all mirror setting

3.98 Network

[Introduction]

Start the RIP protocol of the specified network. When the specified network is the same with the one where the interface IP is located, the transmitting of RIP message on the interface can be started. Using the command **no network** to cancel this configuration.

[no] network *ip-address ip-mask*

[Parameter]

·ip-address The network segment address specified for the client. It could be natural network or subnetwork. The format is dot separated decimal: A.B.C.D;

·ip-mask The network mask corresponded to the network segment address specified by the client. In this case, it is inverse mask, the format is: A.B.C.D

[Default]

No specified network

[Mode]

RIP protocol configuration mode; privileged user

[Guide]

The RIP message could transmit RIP message only after starting RIP protocol on the Switch interface. Using command **network** to start the RIP protocol of the specified network. When the specified network is the same with the one where the interface IP is located, the transmitting of RIP message on the interface can be started. You can first configure the IP address of the interface, and then use the command **network** to specify the network for starting the RIP protocol on the interface for the transmitting of the RIP message. You can also specify a network using **network**, and then configure the corresponding network IP address for the interface to start the RIP protocol on the

interface for the transmitting of RIP message. When specifying the network, the corresponding mask should be specified at the same time. On the same Switch, there is no limit for the number of network specified by the command **network**. Using the command **no network** will cancel this configuration.

[Command Execution Echo]

- set rip network is success
- set rip network is failure

[For example]

- The specified network is 10.0.0.0 0.255.255.255
Raisecom(config-router-rip)# **network** 10.0.0.0 0.255.255.255
- The specified subnetwork is 10.1.0.0 0.0.255.255
Raisecom(config-router-rip)# **network** 10.1.0.0 0.0.255.255
- Cancel the specified network 10.0.0.0 0.0.0.255
Raisecom(config-router-rip)# **no network** 10.0.0.0 0.255.255.255
- Cancel the specified subnetwork 10.1.0.0 0.0.255.255
Raisecom(config-router-rip)# **no network** 10.1.0.0 0.0.255.255

[Relevant command]

Command	Description
router rip	Set the RIP protocol to be valid and enter the RIP protocol configuration mode
show ip protocol	Show the information of the Router protocol configuration

3.99network area

[Introduction]

Define the interfaces for running OSPF and the defined area ID related to these interfaces.

[no] network network-number netmask **area** area-id

[Parameter]

·*network-number* Network IP address of the related interface added to the specified area, dot separated decimal, viz the format of IP address.

·*netmask* Network inverse mask added to the regional network, dot separated decimal format.

·*area-id* Area ID number of the specified area, a decimal integer between 0~3758096383

[Default]

This interface dose not belong to any area.

[Mode]

RIP protocol configuration mode; privileged user

[Guide]

To run the OSPF protocol on the interface, the interface should be added to some OSPF area first. Using this command, the specified interface could be added to the specified area, so that the interface can run the OSPF. When configuring using this command, if no interface in this equipment matches with <network-number, netmask> and the specified area do not exist, this command only creates a new area without interface. When they match, the interface will be automatically added to the specified area and the interface will run OSPF.

Using command **no network** to delete this configuration.

[Command Execution Echo]

- set successful
- set fail
- the input mask is invalid
- the input network has existed

[For example]

Add the interface to area 1, the network of the interface is 192.17.0.0:
Raisecom (config-router-ospf)#**network 192.17.0.0 0.0.255.255 area 1**

[Relevant command]

Command	Description
router ospf	Set the OSPF protocol to be valid
show ip ospf	Show the information of the OSPF protocol

3.100 passive

[Introduction]

Set every interface to no RIP message sending mode. Using the command **no passive** to cancel this configuration and the sending edition of the interface will restore to the default value.

[no] passive

[Parameter]

None

[Default]

Every interface is able to send RIP message.

[Mode]

RIP protocol configuration mode; privileged user

[Guide]

This command forbids all the interface to send RIP message, so this equipment can only receive RIP message. Using command **no passive** to cancel this configuration and restore to the default value.

[Command Execution Echo]

- set rip passive is seccuss
- set rip passive is failure

[For example]

- forbid the interface to send RIP message
Raisecom(config-router-rip)# **passive**
- cancel this configuration
Raisecom(config-router-rip)#**no passive**

[Relevant command]

Command	Description
router ospf	Set the OSPF protocol to be valid
show ip ospf	Show the information of the OSPF protocol

3.101 password

[Function Introduction]

Use "password" to change landing password of current user.

password

[Parameter]

None

[Default]

The default user landing password of Raisecom switch is "Raisecom".

[Mode]

Privileged configuration exec, privileged user

[Guide]

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

[Command Execution Echo]

- set successfully.
- set fail!
- password not same!

[For example]

```
Raisecom#password
Please input password:xxxx
Please input again:xxxx
Password input does not have echo
```

[Relevant command]

Command	Description
user privilege	Set user privilege

3.102 port-access-list

[Function Introduction]

Set access control list of port,use "no"to delete this operation.

Set binding of physical port and protocol type.

port-access-list list-number port port-number { udp | tcp | icmp } { deny | permit }

Set binding of physical port and protocol port.

port-access-list list-number port port-number protocol-port protocol-port-number { deny | permit }

no port-access-list [list-number]

[parameter]

- *list-number* the number of port access list,range from 0 to 99
- **port** physical port
- *port-number* the number of physical port,range from 1 to 26.
- **udp** UDP protocol
- **tcp** TCP protocol
- **icmp** ICMP protocol
- **protocol-port** protocol port
- *protocol-port-number* the number of protocol port,range from 1 to 5000
- **deny** deny access
- **permit** permit access

[default]

On default condition,not set access control list of port.

[mode]

global configuration mode, privileged user.

[guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- The port-access-list X has been set.
- SUCCESS!

- Port access-list X in use ! Operation NOT complete!
- No Port access-list X !

[for example]

- Set binding of port and TCP protocol,deny access.
Raisecom(config)# **port-access-list 0 port 5 tcp deny**
- Set binding of port and protocol port 80,deny access.
Raisecom(config)# **port-access-list 2 port 7 protocol-port 80 deny**
- Delete access control list 5 of port
Raisecom(config)# **no port-access-list 5**
- Delete all access control list of port.
Raisecom(config)# **no port-access-list**

[relevant commmand]

Command	Description
filter	Set filter state of port access list
show port-access-list	Show access control list of one or all port
show access-list	Show all access control list
no access-list	Delete all access control list

3.103 qos cosq

[Function Introduction]

Set the method of cos queue scheduling,use “no”to resume default strict priority mode.

qos cosq { weight w0 w1 w2 w3 | bounded w0 w1 w2 w3 delay }
no qos cosq

[parameter]

- **weight** Weighted Round Robin scheduling mode, transmit certain amount packets of weighted scheduling policy according to each queue.
- **bounded** Bound-dela scheduling mode, set data and weight for each queue.
- *w0* the maximum transmit packet of cos queue 0,integer of <1-255>
- *w1* the maximum transmit packet of cos queue 1,integer of <1-255>
- *w2* the maximum transmit packet of cos queue 2,integer of <1-255>
- *w3* the maximum transmit packet of cos queue 3,integer of <1-255>
- *delay* Maximal delay time for data packets in each queue before sending, <1-255> integer.

[default]

In default,the scheduling mode of cos queue is strict priority.
the default value of *w0*, *w1*, *w2*, *w3* is 0.

[mode]

global configuration mode, privileged user.

[guide]

COS queue scheduling policy of system is strict priority in default, once user changes the ploicy to Weighted Round Robin mode or Bound-delay mode, the corresponding weight parameter must not be 0.

[Command Execution Echo]

- Set the scheduling mode of cos queue for weighted round robin successfully .
- Set the scheduling mode of cos queue for weighted round robin failed.
- Set the scheduling mode of cos queue for bounded-delay successfully .
- Set the scheduling mode of cos queue for bounded-delay failed.
- Set the scheduling mode of cos queue for strict priority successfully
- Set the scheduling mode of cos queue for strict priority failed.

[for example]

- Appoint queue scheduling mode is Weighted Round Robin mode, weight of 4 queue is following:
Raisecom(config)# **qos cosq weight 10 20 20 100**
- Appoint queue scheduling mode is Bound-delay mode, weight of 4 queue and maximal delay time is following:
Raisecom(config)# **qos cosq bounded 10 30 30 200 200**
- Resume queue scheduling is strict priority mode.
Raisecom(config)# **no qos cosq**

[relevant command]

Command	Description
show qos cosq	Show scheduling method of queue configuration

3.104 qos ip-cos

[Function Introduction]

Set priority control to referred port based on source or destination IP address. Use no to cancel referred compatible rule.

qos ip-cos {src | dst } destinationipaddr netmask priority on { portist | all}

no qos ip-cos {src | dst } destinationipaddr netmask on { portist | all}

[parameter]

- *sourceipaddr* source IP address, dotted decimal notation
- *destinationipaddr* destination IP address, dotted decimal notation
- *netmask* network mask, dotted decimal notation
- *portist* port number, use ',' or '-' to connect continuous port number
when there is a multiplicity of ports, range from 1 to 26.
- **all** all the ports
- *priority* vpt (Vlan Priority Tag) , range from 0 to 7

[mode]

global configuration mode; privileged user

[guide]

there is no control rule of priority based on IP

[Command Execution Echo]

- Invalid parameters.
- Set qos priority control based on ipaddress failed.
- On port *portnum*, based on src ip address *sourceipaddr* netmask *netmask* , Set qos priority *priority* failed.
- Set qos priority control based on ipaddress successfully.
- On port *portnum*, based on dst ip address *destinationipaddr* netmask *netmask* , Set qos priority *priority* failed.
- Set qos priority control based on ipaddress successfully.
- Delete configuration of qos priority : On port *portnum*, based on src ip address *sourceipaddr* netmask *netmask* failed.
- Delete configuration for qos priority control based on src ip address successfully.
- Delete configuration of qos priority : On port *portnum* , based on dst ip address *destinationipaddr* netmask *netmask* failed.
- Delete configuration for qos priority control based on dst ip address successfully.

[for example]

- set the priority of diagram coming from IP address range from 10.0.0.1 to 255.0.0.0 4 on port 3.
Raisecom(config)# **qos ip-cos src 10.0.0.1 255.0.0.0 4 on 3**
- set the priority of diagram coming from IP address range from 10.0.0.2 to 255.0.0.0 4 7 on port 4.
Raisecom(config)# **qos ip-cos dst 10.0.0.2 255.0.0.0 7 on 4**
- delete first rule.
Raisecom(config)# **no qos ip-cos src 10.0.0.1 255.0.0.0 on 3**
- delete second rule.
Raisecom(config)# **no qos ip-cos dst 10.0.0.2 255.0.0.0 on 4**

[relevant commmand]

Command	Description
show qos pri-control	show priority control of current system

3.105 qos mac-cos

[Function Introduction]

Set priority control to referred port based on source or destination MAC address. Use no to cancel referred compatible rule.

qos mac-cos {src | dst } mac priority on { portist | all}
no qos mac-cos {src | dst } mac on { portist | all}

[parameter]

- *mac* MAC address, format of input is xxxx.xxxx.xxxx
- *portist* port number, use ‘,’ or ‘-’ to connect continuous port number when there is a multiplicity of ports, range from 1 to 26.
- **all** all the ports
- *priority* vpt(Van Priority Tag), range from 0 to 7.

[mode]

global configuration mode; privileged user

[guide]

There is no priority control rule of based on MAC in default.

[Command Execution Echo]

- Invalid parameters.
- Set qos priority control based on mac address failed.
- On port *portnum* , based on mac address *mac* , set qos priority *priority* failed.
- Set qos priority control based on mac address successfully.
- Delete configuration of qos priority: On port *portnum* , based on src mac *mac* , failed.
- Delete configuration of qos priority: On port *portnum* , based on dst mac *mac* , failed.
- Delete configuration for qos priority control based on mac address successfully.

[for example]

- On port 3, set qos priority 4 of message based on MAC address 002.2d34.4d5e.
Raisecom(config)# **qos mac-cos src 0023.2d34.4d5e 4 on 3**
- On port 4, set qos priority 7 of message based on MAC address 0133.8a34.4d6c.
Raisecom(config)# **qos mac-cos dst 0133.8a34.4d6c 7 on 4**
- delete first rule.
Raisecom(config)# **no qos mac-cos src 0023.2d34.4d5e on 3**
- delete second rule.
Raisecom(config)# **no qos mac-cos dst 0133.8a34.4d6c on 4**

[relevant commmand]

Command	Description
show qos pri-control	show the priority control configuration control of current system.

3.106 qos map priority queue

[Function Introduction]

Configure the mapping relation between vpt priority and output queue. Use “no” command to restore default mapping relation.

qos map priority *priority* queue *num*

no qos map priority *priority*

[Parameter]

- *priority* vpt (Vlan Priority Tag), integer range form 0 to 7.
- *num* queue number, integer range from 0 to 1

[Default]

The mapping relation between vpt priority and queue is that all priority maps queue 0.

[Mode]

Global configuration exec; privileged user

[Guide]

When user is setting priority matching to the specified queue, if different priority matches different queue, some priority should be configure specially.

[Command Execution Echo]

- Set priority matching to the specified cos queue successfully.
This echo shows when matching VPT with queue successfully.
- Set priority *priority* matching to cos queue *num* failed
This echo shows when matching vpt priority with queue num unsuccessfully. The “priority” and “num” mean priority and number of the queue. Please check the parameter format and range when fails
- Set priority matching to default cos queue 0 successfully.
This echo shows when setting the relationship between vpt and queue to default successful.
- Set priority *priority* matching to default cos queue 0 failed.
This echo shows when setting the relationship between vpt and queue to default unsuccessful. The “priority” is the designated priority. Please check the parameter format and range when fails.

[For example]

- Set priority of vpt 7 matching to queue 3.
Raisecom(config)# qos map priority 7 queue 3
- Restore priority of vpt 3 matching to queue to be default
Raisecom(config)# no qos map priority 3

[Relevant command]

Command	Description
show qos map	Show the matching relation between vpt and priority queue in current system.

3.107 qos port

[Function Introduction]

Set the priority of specified port default..Use no to restore the priority of

port to be default 0.

qos port { *portist* | **all**} **default-prio** *priority*

no qos port { *portist* | **all**}

[parameter]

- *portist* port number,use ','or '-' to connect continuous port number when there is a multiplicity of ports,range from 1 to 26.
- **all** all the ports
- *priority* vpt(Van Priority Tag),range from 0 to 7.

[default]

The default priority of port is priority 0.

[mode]

global configuration mode; privileged user

[guide]

The default priority set by using the command only affects UNTAG message input from the port and has no effect on TAG message.

[Command Execution Echo]

- Set default priority for the specified port successfully.
- On port *portnum* ,set default priority *priority* failed.
- Delete configuration about default priority for the specified port.
- On port *portnum*,set default configuration for default priority failed.

[for example]

- Configure port 3,the default priority range form 5 to 8 is 4.
Raisecom(config)# **qos port 3,5-8 default-prio 4**
- Restore all the ports default priority as default configuration.
Raisecom(config)# **no qos port all**

[relevant commmand]

Command	Description
show qos pri-control	show the priority control configuration information of current system.

3.108 qos tos-cos

[Function Introduction]

Specify the compatible relation between IP packet priority to COS priority.Use no to cancel the compatible rule.

qos tos-cos *tos to priority*

no qos tos-cos *tos*

[parameter]

- *tos* priority Tag in IP packet,range from 0 to 7.
- *priority* vpt(Vlan Priority Tag), range from 0 to 7.

[mode]

global configuration mode; privileged user

[guide]

There is no priority control rule of compatible relation between IP packet priority and COS priority in default.

[Command Execution Echo]

- Set the mapping rule from TOS Precedence value and qos priority failed.
- Set TOS *tos* matching to COS *priority* failed.
- Set the mapping rule from TOS Precedence value and qos priority

- successfully .
- Delete configuration of TOS *tos* matching to COS failed.
- Delete configuration for the mapping rule from TOS Precedence value and qos priority successfully.

[for example]

- Set the IP packet of TOS 3 vpt priority 4.
Raisecom(config)# **qos tos-cos 3 to 4**
- cancel the rule above
Raisecom(config)# **no qos tos-cos 3**

[relevant commmand]

Command	Description
show qos pri-control	Show the priority control configuration information of current system.

3.109 qos vlan-cos

[Function Introduction]

Set priority control for specified VLAN.Use no to cancel the compatible rule.

qos vlan-cos *vid priority*

no qos vlan-cos *vid*

[Parameter]

- *vid* Specified VLAN ID, use ',' or '-' to connect continous VID if there is a multiplicity of VLAN,range from 1 to 4094.
- *priority* vpt (Vlan Priority Tag),range from 0 to 7.

[Mode]

Global configuration exec; privileged user

[Guide]

There is no priority control rule based on VLAN in default.

[Command Execution Echo]

- Set qos priority control based on the specific vlan failed.
Input VID parameter is invalid
- On vlan *vid*, set qos priority *priority* failed.
Set VLAN priority policy failed.
- Set qos priority control based on the specified VLAN successfully.
- Delete qos priority control configuration :based on the given VLAN *vid* failed .
- Delete configuration for qos priority control based on the specified VLAN successfully.

[For Example]

- Set VLAN 1,priority rule is 4.
Raisecom(config)# **qos vlan-cos 1 4**
- Cancel the rule above.
Raisecom(config)# **no qos vlan-cos 1**

[relevant commmand]

Command	Description
show qos pri-control	Show the priority control configuration information of current system.

3.110 quit

[Function Introduction]

Use the command to return parent mode or quit login state.

quit

[Parameter]

None

[Mode]

Initial exec, privileged configuration exec, global configuration exec, vlan configuration exec, interface configuration exec, router protocol configuration exec; common user, privileged user.

[Guide]

Use the command to quit login state on original mode.

Use the command to return parent mode on valn configuration mode,interface configuration mode or router protocol configuration mode.

[Command Execution Echo]

None

[for example]

Raisecom>**quit**

[relevant commmand]

Command	Description
exit	Return parent mode or quit login state.

3.111 rate-limit port

[Function Introduction]

Set the bandwidth limit of physical port,use no to cancel the operation.

rate-limit port *port-number* **input** *rate* **burst** *burst* **output** *rate* **burst** *burst*

no rate-limit port [*port-number*]

[Parameter]

- **port** physical port.
- *port-number* physical port,range from 1 to 26.
- **input** uplink direction of physical port.
- **output** downlink direction of physical port
- *rate* rate value,range from 1 to 99 Mbps.
- **burst** peak value
- *burst* peak rate,range from 4 to 64 KBps.

[Default]

There is no rate limit of physical port in default.

[Mode]

Global configuration exec; privileged user

[Guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- SUCCESS!
- This operation failed!
- No rate limit for port X!

[For Example]

- Set the uplink rate 5Mbps,peak value 32KBps,downlink rate 10Mbps,peak value 64KBps
Raisecom(config)# **rate-limit port 5 input 5 burst 32 output 10 burst 64**
- Cancel the rate limit of port 5.
Raisecom(config)# **no rate-limit port 5**

[Relevant Commmand]

Command	Description
show rate-limit port [<i>port_number</i>]	Show the rate limit of specified of one or all the port.

3.112 rate-limit vlan

[Function Introduction]

Set the rate limit of vlan ,use no to cancel the operation.

rate-limit vlan *vlan_id* **input** *rate* **burst** *burst* **output** *rate* **burst** *burst*

no rate-limit vlan [*vlan_id*]

[Parameter]

- **vlan** VLAN;
vlan_id VLAN ID, range from 1 to 4094.
- **input** uplink of VLAN
- **output** downlink of VLAN
- **rate** setting of rate value, range from 1 to 99.
- **burst** peak vlue.
- **burst** peak rate, range from 4 to 64 KBps.

[default]

There is no rate limit to VLAN in default.

[mode]

Global configuration exec; privileged user

[guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- The uplink port X is not in VLAN Y ,please reset uplink port or VLAN!
- SUCCESS!
- SUCCESS ! Please set uplink port!
- Can not set rate-limit more!
- NO rate limit for vlan X!

[for example]

- Set the uplink rate 4Mbps to VLAN ID,peak value 32KBps,downlink rate 10Mbps,peak value 64KBps.
Raisecom(config)# **rate-limit vlan 3 input 5 burst 32 output 10 burst 64**
- Cancel the rate limit to VLAN ID 3.
Raisecom(config)#**no rate-limit vlan 3**

[relevant commmand]

Command	Description
show rate-limit vlan	Show rate limit of some or all the VLAN.
uplink-port	Set uplink-port

3.113 reboot

[Function Introduction]

Use reboot to restore switch.

reboot

[parameter]

None

[mode]

privileged configuration exec, privileged user.

[guide]

'yes'should be input to idenitify the operation when the command is used to reboot switch.

[Command Execution Echo]

None

[for example]

- Raisecom#**reboot**
Please input 'yes' to confirm:yes
Rebooting ...

[relevant command]

None

3.114 rmon alarm

[Function Introduction]

Use the command to add rmon alarm table unit, use no to delete table unit.

rmon alarm <1-512> MIBVAR <2-2000000> { **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> the index of Alarm table
- MIBVAR remote control MIB variable
- <2-2000000> the time between checking MIB variable (unit: second)
- **delta** check between the value of MIB variable.
- **absolute** check the absolute alteration of MIB variable.
- **rising-threshold** the rising-threshold of MIB variable.
- <1-65535>₁ the rising-threshold value of MIB variable
- <1-65535>₂ index of events to rising threshold
- **falling-threshold** the falling threshold of MIB variable.
- <1-65535>₃ the falling-threshold value of MIB variable
- <1-65535>₄ index of events to falling threshold
- **owner** the owner of Alarm table
- STRING the string of owner

[Default]

There is no configuration of Alarm table.

[Mode]

Global configuration exec; privileged user

[Guide]

The format of MIBVAR must be dotted decimal notation, the variable must be right remote control MIB variable, and else it is not remote control

[Command Execution Echo]

·*ERROR MIB Variable!*

The MIB variable by command is wrong

·*set successfully.*

Command successful

·*set fail.*

Command failed

[For example]

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

The command set RMON alarm 10, inspect MIB variable 1.3.6.1.2.1.2.2.1.20.1
 20 seconds once, detect the rising or falling of the variable, if it rises by 15, from
 10000 to 10015 for example, alarm will be triggered.

[Relevant command]

Command	Description
rmon	Enable rmon on the interface.
show rmon alarm	Show the rmon alarm table.

3.115 rmon event

[Function 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.

[Mode]

Global configuration exec; privileged user

[Guide]

Use the command to add and set the attribute of event

[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

[For example]

Raisecom(config)#rmon event 1 trap private

[Relevant command]

Command	Description
Show rmon event	show RMON EVENT table.

3.116 rmon queue size

[Function Introduction]

Use rmon queue size to set the size of rmon queue.

rmon queue size <60-65535>

no rmon queue size

[Parameter]

The size of rmon setting ranges from 60 to 65535

[Default]

The size of queue is 100 in default.

[Mode]

Global configuration exec; privileged user

[Guide]

Set the size of rmon queue.

[Command Execution Echo]

- *Set successfully.*
Command successful

[For example]

Set the size of RMON queue 200.

Raisecom(config)# rmon queue size 200

[Relevant command]

None

3.117 router ospf

[Introduction]

Command **router ospf** will set the OSPF protocol to be valid

Command **no router ospf** will set the OSPF protocol to be invalid

[no] router ospf

[Parameter]

None

[Default]

The default configuration of OSPF protocol is invalid.

[Mode]

Global configuration mode, privileged user.

[Guide]

Using command **router ospf** to set the OSPF protocol to be valid, and enter its configuration mode. This is the precondition of configuring other parameters of OSPF protocol. Using command **no router ospf** will set the OSPF to be invalid. If the OSPF protocol is invalid, the other parameters will all be invalid, and the Router learnt by the OSPF protocol will be deleted.

[Command Execution Echo]

- set ospf up success!
- set ospf up fail!

[For example]

- Set the state of OSPF to be valid
Raisecom (config)# router ospf

[Relevant command]

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

show ip protocol	Show the configuration information of Router protocol
-------------------------	---

3.118 router rip

[Introduction]

Set the RIP protocol to be valid, and enter the configuration mode of the RIP protocol. Using command **no router rip** to set the configuration of RIP protocol to be invalid.

[no] router rip

[Parameter]

None

[Default]

Invalid

[Mode]

Global configuration mode, privileged user.

[Guide]

Using command to set the RIP protocol to be valid, and enter the RIP protocol configuration mode through it. This is the precondition of configuring other RIP protocol parameters. Using command **no router rip** will set the RIP protocol state to be invalid.

[Command Execution Echo]

- rip startup is seccuss/ rip shutdown is seccuss
- rip startup is failure/ rip shutdown is failure
- rip has been shutdown

[For example]

- Set the RIP protocol state to be valid
Raisecom(config)# **router rip**
- Set the RIP protocol state to be invalid
Raisecom(config)# **no router rip**

[Relevant command]

Command	Description
network	Start the RIP protocol of the specified network
show ip protocol	Show the configuration information of Router protocol

3.119 search mac-address

[Function 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 character.

[Default]

Don't search in default.

[Mode]

Privileged configuration exec, privileged user (priority 5)

[Guide]

Only privileged user whose priority is above or equal 5 can use the command.

[Command Execution Echo]

Information of layer 2 address in the switch:

MAC address Port number VLAN identifier Layer 2 flags

[For example]

Raisecom# **search mac-address** 0050.8d47.d4cc

[Relevant command]

Command	Description
show mac-address-table l2-address	Show all the MAC addresses that fit in with some condition.

3.120 show access-list

[Function Introduction]

Show all the information of access-control list.

show access-list

[parameter]

access-list list of access.

[default]

[mode]

Privileged configuration exec, privileged user.

[guide]

Only privileged user whose priority is above or equal 5 can use the command.

[Command Execution Echo]

mac access list:

List No. MAC-address BindType ID AccessType Ref

.....

ip access list:

List No. ip-confine-list No. BindType ID Ref

.....

port access list:

List No. Port No. BindType protocol-port AccessType Ref
-----.....

[for example]

Show all access control list.

Raisecom# **show access-list**

[relevant command]

Command	Description
show { ip-access-list port-access-list mac-access-list ip-confine-list }	Show one or all the same type access list

3.121 show aging-time

[Function Introduction]

Show the aging time of MAC address

show aging-time

[Parameter]

aging-time the aging time of MAC address

[Default]

None

[Mode]

Privileged configuration exec, privileged user

[Guide]

Only privileged user whose priority is above or equal 5 can use the command.

[Command Execution Echo]

- *The age timer value is: seconds.*
- *This operation failed!*

[For example]

Show the aging time of current
Raisecom# show aging-time

[Relevant command]

Command	Description
mac-address-table aging-time	Set the aging time of MAC address
no mac-address-table aging-time	Restore the aging time of mac address

3.122 show arp

[Function Introduction]

Show the item of ARP mapping table

[Command Format]

show arp

[Parameter]

None

[Default]

None

[Mode]

Privileged configuration exec; privileged user

[Guide]

Use show arp to search all the item in arp address list, every item includes IP address, MAC address and the type information.

[Command Execution Echo]

- *Set sucessfully!*
Show ARP table:

<i>IP Address</i>	<i>MAC Address</i>	<i>Type</i>
<i>10.0.0.5</i>	<i>0050.8d4b.fd1e</i>	<i>static</i>
<i>10.0.0.6</i>	<i>0050.0a3c.ac2e</i>	<i>dynamic</i>
<i>10.0.0.7</i>	<i>0050.1c4e.15a7</i>	<i>dynamic</i>

[For example]

Show ARP list
Raisecom#show arp

[Relevant command]

Command	Description
arp add	Add a static MAC address item.
clear arp	Clear all the items in ARP address table.

3.123 show clock

[Function Introduction]

Use show clock to show current system time.

show clock

[Parameter]

None

[Mode]

Privileged configuration exec, privileged user

[Guide]

Use the command to show current system time.

[Command Execution Echo]

None

[For example]

Raisecom#show clock

The switch current system Time is : Sep-30-2003 00:28:07

[Relevant command]

Command	Description
clockset	set current system time

3.124 show dhcp-relay

[Introduction]

Show the configuration and statistics information of DHCP Relay

[Parameter]

None

[Default]

None

[Mode]

Privileged user mode, privileged user

[Guide]

The main content showed by using this command is whether DHCP Relay has started or not and the statistics of DHCP Relay.

[Command Execution Echo]

None

[For example]

- Show the DHCP Relay information

Raisecom# **show dhcp-relay**

DHCP Relay enabled!

the VLAN that disabled the DHCP Relay include:

VLAN ID = 1,2

The total disabled VLAN num is 2

statistics information 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 Unknowns received: 0

the total Num of Packets received: 2

[Relevant command]

Command	Description
dhcp-relay enable/disable	Start the global DHCP Relay
dhcp-relay listen	Start or stop the DHCP Relay function on VLAN

3.125 show dhcp-relay listen

[Introduction]

Show the specified or all the VLAN situation of the DHCP Relay

show dhcp-relay listen [vlan *vlanid*]

[Parameter]

·*vlanid* specified vlan, the range is between 1~4094.

[Default]

None.

[Mode]

Privileged user mode, privileged user

[Guide]

Using the command **show dhcp-relay listen** to show every DHCP configuration on the VLAN.

Using the command **show dhcp-relay listen vlan *vlanid*** to show the specified DHCP configuration on the VLAN.

[Command Execution Echo]

·None

[For example]

- Show every configuration on the VLAN
Raisecom# **show dhcp-relay listen**
the VLAN that disabled the DHCP Relay include:
VLAN ID = 1, 2
The total disabled VLAN num is 2
- Show the specified configuration on the VLAN
Raisecom# **show dhcp-relay listen vlan 2**
VLAN 2 disabled DHCP Relay

[Relevant command]

Command	Description
dhcp-relay enable/disable	Start the global DHCP Relay
dhcp-relay listen	Start or stop the DHCP Relay function on VLAN

3.126 show dhcp-relay server-ip

[Introduction]

Show the server-ip information of the configured DHCP

show dhcp-relay server-ip

[Parameter]

None

[Default]

None

[Mode]

Privileged user mode, privileged user

[Guide]

The main content shown by using this command is the server-ip information of the configured DHCP.

[Command Execution Echo]

None

[For example]

- Show the server-ip information of the DHCP

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

[Relevant command]

Command	Description
dhcp-relay server-ip	Configure or delete the server-ip of DHCP

3.127 show dhcp-server

[Function Introduction]

Show the configuration information and statistic information of DHCP server.

show dhcp-server

[parameter]

None

[default]

None

[mode]

Privileged configuration mode; privileged user.

[guide]

The command is used to show the configuration information and statistic information of DHCP server.

[Command Execution Echo]

[for example]

Show the information of adjacent DHCP server.

Raisecom#show dhcp-server

DHCP Server enabled !

the VLAN that enabled the DHCP Server include:

VLAN ID = 2

The total enabled VLAN num is 1

DHCP max lease timeout is 10080 minutes

DHCP min lease timeout is 30 minutes

DHCP default lease timeout is 30 minutes

statistics information of DHCP Server:

```

DHCP StartUp time:      0 hours 0 munites 48 seconds
the Num of Bootps      received:      0
the Num of Discover    received:      0
the Num of Request     received:      0
the Num of Release     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 Unknowns    received:      0
the total Num of Packets received:  0

```

[relevant commmand]

Command	Description
dhcp-server enable	enable dhcp-server
dhcp-server active	enable dhcp-server on VLAN

3.128 show dhcp-server ip-pool

[Function Introduction]

Show the configuration information of DHCP-server ip-pool.

show dhcp-server ip-pool

[parameter]

None

[default]

None

[mode]

Privileged configuration mode; privileged user.

[guide]

The command is used to show the configuration information of DHCP-server ip-pool.

[Command Execution Echo]

[for example]

- show the information of adjacent DHCP server.

```

Raisecom#show dhcp-server ip-pool
-----
the name of ip pool table is aaaaaaaa
the status of ip pool table is active
the ip address range from 2.0.0.200 to 2.0.0.220
the mask is 255.0.0.0
the VLAN that used the ip pool include:
VLAN ID = 2,3,4,5
the gateway ip address is 2.0.0.3
the dns server ip address is 2.0.0.3
-----

the valid ip pool sum is 1
the valid ip address sum is 21

```

the allotted ip address sum is 1

[relevant command]

Command	Description
dhcp-server enable	enable dhcp-server
dhcp-server ip-pool name	configure dhcp-server ip-pool

3.129 show dhcp-server relay-ip

[Function Introduction]

Show the configuration information of adjacent DHCP-server relay-ip address

show dhcp-server relay-ip

[parameter]

None

[default]

None

[mode]

privileged configuration mode; privileged user.

[guide]

The command is used to show the configuration information of adjacent DHCP-server relay-ip address.

[Command Execution Echo]

None

[for 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
```

[relevant command]

Command	Description
dhcp-server relay-ip	Set of delete the adjacent DHCP-server relay-ip address.

3.130 show filter

[Function Introduction]

Show all the status of filter.

show filter

[parameter]

filter the configured filter.

[default]

None

[mode]

privileged configuration mode, privileged user.

[guide]

Only privileged user whose priority is above or equal 5 can use the command.

[Command Execution Echo]

Filter list:
 AccessListType List-number AccessType

[for example]

Show the status of filter.
 rc302(config)# **show filter**

[relevant commmand]

Command	Description
filter	Show the status of access-list.

3.131 show garp

[Function Introduction]

Show the value of garp timer[{{1-26}}]

show garp timer [{{1-26}}]

[parameter]

- **timer** the timer of garp.
- {{1-26}} port list parameter,optional,all the ether second layer port GARP timer will show if there is no the parameter.

[mode]

Privileged configuration mode; privileged user.

[Command Execution Echo]

Port X GARP Timer Configuration

Join: 20

Leave: 60

LeaveAll: 1000

[relevant commmand]

Command	Description
Garp	set the value of GARP timer.

3.132 show gmrp

[Function Introduction]

Show the configuration information of GMRP.

show gmrp

[mode]

Privileged configuration mode; privileged user.

[Command Execution Echo]

Global GMRP Configuration:

GMRP feature is currently enabled on the switch.

Participant ports: 0-25

[relevant commmand]

Command	Description
gmrp	disable/enable GMRP protocol

3.133 show gvrp

[Function Introduction]

Show the configuration information of GVRP

show gvrp

[mode]

Privileged configuration mode; privileged user.

[Command Execution Echo]

Global GVRP Configuration:
GVRP feature is currently enabled on the switch.
Participant ports: 0-25

[relevant command]

Command	Description
gvrp	Disable/enable GVRP protocol

3.134 show ip igmp-snooping

[Function 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]

None

[Mode]

Privileged configuration exec; privileged user

[Guide]

Show the status of IGMP Snooping and each VLAN.

Show the dynamic-studying or manual configuration information of multi-router port.

Show the status of VLAN referred by vlanid.

Show the referred VLAN multi-router port information, if it is no referred, show all the VLAN information.

[Command Execution Echo]

[For example]

- show the configuration information of IGMP Snooping.

```
Raisecom# show ip igmp-snooping  
igmp snooping is globally Disabled  
igmp snooping aging time is 300(s)  
IGMP snooping isn't enabled on any Vlan.
```

- show all the multi-router information of VLAN

```
Raisecom# show ip igmp-snooping mrouter  
Group Addr      Port   Vid   Age   Type  
-----  
224.8.8.8       1      1    270   REPORTv2  
224.8.8.9       2      2    260   REPORTv2
```

- show the configuration information of VLAN 1 IGMP Snooping.

```
Raisecom# show ip igmp-snooping vlan 1  
igmp snooping is globally Disabled  
igmp snooping aging time is 300(s)  
IGMP snooping is disabled on this Vlan.
```

- show the igmp-snooping multi-router of vlan 1.

```

Raisecom#show ip igmp-snooping mrouter vlan 1
Group Addr      Port   Vid   Age   Type
-----
224.8.8.8      1     1    270   REPORTv2

```

[Relevant command]

None

3.135 show ip ospf

[Introduction]

Show the ospf configuration information

show ip ospf

[Parameter]

None

[Default]

None

[Mode]

Privileged configuration exec; privileged user

[Guide]

By using this command, the common information of the OSPF Router protocol could be checked. This command show the RouterID, whether support TOS or not, the state of OSPF Router protocol, the identity of the Router equipment (whether it is ABR, ASBR or not), the area number of the Router equipment, every area ID, number of interface included, The times of executing Shortest Path First (SPF) and the area type. According to the output of this command, it could help with the diagnose of OSPF error.

[Command Execution Echo]

```

·OSPF is ENABLED
Routing protocol ospf with Router ID 10.0.0.1
Doesn't support Tos
It is not an ABR!
It is not an ASBR!
Number of areas in this router is 4
  OSPF AREAS
  REA ID      #Interfaces  #SpfRuns  AreaType
  1           2           180       neither Stub nor Nssa
  2           1           35        neither Stub nor Nssa
  3           1           11        Stub
  4           1           25        NSSA

```

Show the above information when starting the OSPF protocol

```
·OSPF is DISABLED
```

[For example]

- Show the ospf configuration information:

```
Raisecom#show ip ospf
```

[Relevant command]

Command	Description
router ospf	Start OSPF protocol
network	Start the OSPF protocol of the corresponding network segment
area stub	Set the stub area
area nssa	Set the nssa area
router-id	Set routerId

3.136 show ip ospf database

[Introduction]

Show the database of the link route state

show ip ospf database [{router| network| summary| asbr-summary| external}]

[Parameter]

- *router* Router LSA;
- *network* Network LSA;
- *summary* Network gathering LSA;
- *asbr-summary* ASBR gathering LSA;
- *external* LSA outside AS;

[Default]

None

[Mode]

Privileged configuration exec; privileged user

[Guide]

By using this command the database of the link route state could be shown according to the LSA type, the output this command will help with the diagnose of the error.

[Command Execution Echo]

Routing protocol ospf with Router ID

LSA DATABASE OF AREA :0.0.0.1

Lsa	Type	Link	State	ID	ADV	Router	Age	Seq#
		Checknum						

1		10.0.0.1		10.0.0.1		481	0x80000007	0x86C0
1		13.0.0.2		13.0.0.2		743	0x80000002	0x61AD
3		10.0.0.0		10.0.0.1		732	0x8000000B	0xF63F
3		13.0.0.0		10.0.0.1		2103	0x80000002	0xE359
3		172.22.0.0		13.0.0.2		743	0x80000002	0x4249

LSA DATABASE OF AREA : 0.0.0.2

Lsa	Type	Link	State	ID	ADV	Router	Age	Seq#
		Checknum						

1		10.0.0.1		10.0.0.1		936	0x800000011	
0x49F1								
1		10.0.0.2		10.0.0.2		538	0x80000008	0x6B86
2		10.0.0.2		10.0.0.2		538	0x80000003	0x7593
3		13.0.0.0		10.0.0.2		923	0x80000001	0x42CD
3		12.0.0.0		10.0.0.2		880	0x80000001	0xEA30
3		172.22.0.0		10.0.0.2		738	0x80000001	0x2831

When the **show ip ospf database** is successful, this message will show.

[For example]

- Show the database of ospf link route state
Raisecom#**show ip ospf database**

[Relevant command]

None

3.137 show ip ospf interface

[Introduction]

Show every interface information.

[Parameter]

None

[Default]

None

[Mode]

Privileged configuration exec; privileged user

[Guide]

Using this command to show the interface information of running OSPF. **show ip ospf interface**: show all the OSPF interface information, including the virtual interface, If the interface has simple password authentication or MD5 key authentication, the valid information about authentication will show. If there is no display, it means that the configuration fails. **show ip ospf interface broadcast**: show all the interface information whose type is broadcast and who run the OSPF. **show ip ospf interface ptop**: show all the interface information whose type is ptop and who run the OSPF. **show ip ospf interface virtual**: show all the virtual interface information. Client could check the interface OSPF configuration and running state by this command, which will help to remove the fault.

[Command Execution Echo]

```
INTERFACES
```

```
-----  
interface IP address:10.0.0.1  
interface IP Mask:255.0.0.0  
interface index:1  
Area ID:0.0.0.1  
IF type: BROADCAST  
IF Admin status: enabled  
Priority:1  
transmit delay:1  
retransmit interval:5  
hello interval:10  
Rtr Dead interval:40  
If State: otherDesignatedRouter  
DR:10.0.0.10  
BDR:10.0.0.20  
Auth Type: NONE
```

```
-----  
interface IP address:20.0.0.1  
interface IP Mask:255.0.0.0  
interface index:2  
Area ID:0.0.0.2  
IF type: BROADCAST  
IF Admin status: enabled  
Priority:2  
transmit delay:1  
retransmit interval:10  
hello interval:20  
Rtr Dead interval:80  
If State: designatedRouter  
DR:20.0.0.1
```

BDR:20.0.0.2
Auth Type: SIMPLE
Simple Auth password:1234

End of command show ip ospf interface

[For example]

Show the ospf interface information

Raisecom#**show ip ospf interface**

[Relevant command]

Command	Description
network area	Define the interfaces of the running OSPF and the area ID of these interfaces.

3.138 show ip ospf neighbor

[Introduction]

Show neighbor information

show ip ospf neighbor [*router-id*]

[Parameter]

·*router-id* Router ID of the neighbor, dot separated decimal, viz the IP address

format: A.B.C.D

[Default]

None

[Mode]

Privileged configuration exec; privileged user

[Guide]

By using this command, the neighbor information will show. It will help the client to check the communication state between neighbors for problem removing. **show ip ospf neighbor**: show every neighbor information. **show ip ospf neighbor** *number*: show the specified Router ID neighbor information

[Command Execution Echo]

```
NEIGHBORS
NbrAddr  NbrID      STATE      Pri  RxmtLen
-----
10.0.0.1  172.18.0.1 full        2    0
20.0.0.1  182.17.0.1 full        1   10
```

[For example]

- Show ospf neighbor information
Raisecom#**show ip ospf neighbor**

[Relevant command]

None

3.139 show ip ospf virtual-links

[Introduction]

Show the information of virtual link route and the virtual neighbor

show ip ospf virtual-links

[Parameter]

None

[Default]

None

[Mode]

Privileged configuration exec; privileged user

[Guide]

Show the information of virtual link route and the virtual neighbor by using this command.

[Command Execution Echo]

Virtual Link

```
-----  
router ID of the virtual neighbor:20.0.0.1  
transit area that the virtual link traverses:0.0.0.1  
transmit delay:1  
retransmit interval:5  
hello interval:10  
Rtr Dead interval:40  
Auth Type:NONE  
-----
```

```
-----  
router ID of the virtual neighbor:192.168.0.1  
transit area that the virtual link traverses:0.0.0.2  
transmit delay:2  
retransmit interval:10  
hello interval:20  
Rtr Dead interval:80  
Auth Type: SIMPLE  
Auth password:12345  
-----
```

Virtual NEIGHBOR

```
-----  
transit area ID:0.0.0.1  
neighboring router ID: 20.0.0.1  
neighboring router IP Addr:30.0.0.1  
virtual neighbor state: full  
current length of the retrans queue:0  
-----
```

```
-----  
transit area ID:0.0.0.2  
neighboring router ID:192.168.0.1  
neighboring router IP Addr:50.0.0.1  
virtual neighbor state: full  
current length of the retrans queue:20  
-----
```

[For example]

- Show the information of virtual link route and the virtual neighbor
Raisecom#**show ip ospf neighbor**

[Relevant command]

None

3.140 show ip protocol

[Introduction]

Show the configuration information of the global and every interface of the RIP/OSPF protocol. The shown interface is the one that has started RIP/OSPF, or else, the interface information will not show.

show ip protocol

[Parameter]

None

[Default]

If the RIP/OSPF does not start, no message will show.

[Mode]

Privileged configuration exec; privileged user

[Guide]

Show the configuration information of the global and every interface of the RIP/OSPF protocol. The shown interface is the one that has started RIP/OSPF, or else, the interface information will not show.

The output information includes:

The started Router protocol;

For RIP:

The overtime of the timer

Configuration information of every interface

Configured network information

Distance information

For OSPF:

Router ID

Area ID

Configured network information

Distance information

Interface and virtual interface information

Neighbor information

The host information connected to the Router

[Command Execution Echo]

None

[For example]

- Show the RIP configuration information:

Raisecom# **show ip protocol**

Routing Protocol is 'RIP'

RIP global Enable

Default version control:send version 1, receive any version

RIP supply interval is 30 (default 30)second

RIP router expire interval is 180 (default 180)second

RIP router flush interval is 300 (default 300)second

IF index	Send	Recv	Metric	Auth-mode	Auth-key	State
2	1	1 2	1	none		UP
3	1	1 2	1	none		DOWN

Routing for Networks:

172.18.0.0 0.0.255.255

2.0.0.0 0.255.255.255

- Show the OSPF configuration information:

Raisecom# **show ip protocol**

Routing Protocol is 'ospf'

Router ID 0.0.0.0

number of areas in this router is 2

```

Routing for Networks:
    172.18.0.0 0.0.255.255 area 0
    2.0.0.0 0.0.0.255 area 1

```

```

Distance: 110
ospf interface number is 1
ospf vir interface number is 0
neighbor number is 0
hosts attach to this router:
hosts IP area the Host is in:

```

```

-----
172.18.1.1 0

```

Distance(default is 120):120

[Relevant command]

Command	Description
router rip	Start RIP protocol
network	Start the RIP protocol of the corresponding network segment
router ospf	Start OSPF protocol
network	Start the OSPF protocol of the corresponding network segment

3.141 show ip rip statistics

[Introduction]

Show the statistics information of global and very interface of RIP protocol. The shown interface is the one that has started RIP and runs the RIP. If the interface has not started or the state of the interface is DOWN, the interface information will not show.

[Parameter]

None

[Default]

None

[Mode]

Privileged configuration exec; privileged user

[Guide]

The output includes:

The number of the changed Router

The number of the sent answer message

Information on every interface:

The number of the thrown away unlawful message

The number of the unlawful Router list

The number of sent spring update

[Command Execution Echo]

·RIP disabled!

[For example]

- Show the RIP statistics information

Raisecom# **show ip rip statistics**

Num of routes changed :1

Num of responses sent to RIP queries :0

interface 2:

The address of this interface is :172.18.1.1

Num of packets discarded :0

Num of routes discarded :0

Num of triggered updates :1

[Relevant command]

Command	Description
router rip	Start RIP protocol
network	Start the RIP protocol of the corresponding network segment

3.142 show ip route

[Function Introduction]

Show the router of system router list.

show ip route [{ **connected** | **ospf** | **rip** | **static** | **hardware** } |
A.B.C.D [A.B.C.D | **longer-prefixes**]]

[parameter]

- **connected** information of connected router.
- **ospf** information of ospf router.
- **rip** information of rip router.
- **static** information of static router.
- **hardware** information of hardware router.
- A.B.C.D₁ the prifix of IP network
- A.B.C.D₂ the mask of network
- **longer-prefixes** the prifix of longer-network

[default]

Show all the router.

[mode]

Privileged configuration mode, privileged user.

[guide]

Use the command to show the IP router information and show different protocol router information respectively,and show the prifix router information of some network,and show the router information in hardware list.

[Command Execution Echo]

None

[for example]

- Raisecom#show ip route **ospf**
Codes: C - connected, H-HardWare S - static, R - RIP, O - OSPF

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
- 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

```
- ```

Raisecom#show ip route hardware
Codes: C - connected, H-HardWare S - static, R - RIP, O - OSPF
-----

```

Host route table

```
*H 10.0.0.1 Inter= 1 port=1 NextHopMAC = 00.50.8d.47.0c.fa, hit = 3
```

[relevant commmand]

Command	Description
show ip protocol	Show the information of IP router protocol

3.143 show interface port

[Function Introduction]

Show some or all the port status.

```
show interface port [ port-number ] [ statistic | flowcontrol ]
```

[Parameter]

- interface** the interface
- port** the physical port
- port-number* physical port, range from 1 to 26.
- statistic** statistic information.
- flowcontrol** flow control function

[Default]

None

[Mode]

Privileged configuration exec, privileged user (priority 5)

[Guide]

Only privileged user whose priority is above or equal 5 can use the command.

[Command Execution Echo]

- Information of port status:

```
port No. Linkstatus speed-duplex flowcontrol Mac-learning
```

```
-----
Show port status
```

- Statistics for the interface of switch:

```
port No: X
```

```
-----
InOctets:
InUcastPkts:
InMulticastPkts:
InBroadcastPkts:
OutOctets:
OutUcastPkts:
OutMulticastPkts:
OutBroadcastPkts:
DropEvents:
CRCAAlignErrors:
```

UndersizePkts:
 OversizePkts:
 Fragments:
 Jabbers:
 Collisions:
 Show the statistic information of Port X.

- Flowcontrol of port:
 port No. flowcontrol
 Show the flow control status of port.

[For example]

- show the status port 5
raisecom# show interface port 5
- show the statistic information of port 5
raisecom# show interface port 5 statistic
- Show the flow control of all the port.
raisecom# show interface port flow control

[Relevant command]

Command	Description
speed {10 100} duplex {full-duplex half-duplex}	Set the rate and duplex mode of port
speed auto-negotiate	Set the rate of port auto-negotiate.
flowcontrol {on off}	Enable/disable flow control of physical port.
mac-address-table learning {enable disable} port <i>port-number</i>	Enable/disable mac-address-table learning function of physical port.

3.144 show interface vlan

[Function Introduction]

Show the status of all IP interface.

show interface vlan

[Parameter]

None

[Default]

None

[Mode]

Privileged configuration mode, privileged user (priority 5)

[Guide]

Only privileged user whose priority is above or equal 5 can use the command.

[Command Execution Echo]

```

• ifIndex   IP Address      NetMask          Vid   Status   Desc
-----
      01100003  192.168.1.2    255.255.255.0   2     active
      01100005  2.0.0.1        255.0.0.0       4     active
  
```

[For example]

Show the status of IP port.
 Raisecom# **show interface vlan**

[Relevant command]

Command	Description
show ip route	Show the route information.
ip address	Set IP address of current interface.

3.145 show lacp lag-id

[Function Introduction]

Show lag-id of all physical interface.

show lacp lag-id

[mode]

Privileged configuration mode; privileged user.

[Command Execution Echo]

[(actor LAG ID), (partner LAG ID)]

P# A# [(Prio, actor MAC ,key ,pr,P #), (Prio, partner MAC ,key ,pr,P #)]

-----01

01

[(8000,0040.4700.0000,0001,80,0001), (8000,0050.0020.0010,0001,80,0001)]

column 1:

P#,physical interface number of ethernet

column 2:

A#,the second layer interface number of ethernet(LACP lag-port)

column 3:

show lag-id of the port,lag-id comprises of the following parts.

the priority of LACP system.

MAC address of the port.

the key used by LACP protocol negotiation

the priority of LACP port.

the port number of LACP

column 4:

show the lag-id of counter port,lag-id comprises of the following parts:

the priority of LACP system.

MAC address of partner port.

the key used by LACP negotiation.

the priority of LACP port

the port number of LACP

[relevant commmand]

Command	Description
lacp	enable/disable LACP
lacp system-priority	set LACP system-priority
lag loading-sharing	Set the lag loading-sharing mode of LACP
lacp admin-key	Set the LACP admin-key of ethernet physical interface.
lacp priority	set the LACP priority of ethernet physical interface.
lacp mode	Set the lag mode of ethernet physical interface.
show lacp port	show the lacp port and physical port configuration of LACP

3.146 show lacp port

[Function Introduction]

show the information of LACP physical interface,lag-port.

show lacp port

[mode]

privileged configuration mode; privileged user.

[Command Execution Echo]

Link aggregation port information:

Port	AKey	MODE	APort	Pri	TGID	RTAG	PList
1	1	ACTIVE	1	128	n/a	0	Individual

column 1:

port number

column 2:

AKey,Admin Key;

column 3:

MODE,lag-port mode,value can be 'on','off','active','passive';

column 4:

APort,lag-port number;

column 5:

priority of port

column 6:

(lag-group ID)

column 7:

RTAG, loading-sharing mode of lag-group(distribution mode)

column 8:

PList, if the aggregation port includes more than one physical ports, port list will be displayed. Otherwise, "Individual" or "Member" will be displayed.

[relevant commmand]

Command	Description
Lacp	enable/disable LACP
lacp	set the system priority of LACP
system-priority	
lag loading-sharing	set LACP lag-link of loading-sharing mode
lacp admin-key	set LACP admin-key of Ethernet physical port
lacp priority	set the priority of ethernet physical port.
lacp mode	set the lag-link mode of Ethernet physical port.
show lacp lag-id	show all the lag-id of Ethernet physical port

3.147 show logging

[Function Introduction]

Show logging file.

show logging [file]

[Parameter]

file show logging information stored in file.

[Default]

[Mode]

Privileged configuration exec; privileged user

[Guide]

Use the command to show the configuration information of logging file, or information stored in file.

[Command Execution Echo]

- Show logging information

```
Raisecom#show logging
```

```
Syslog logging: enable, 0 messages dropped, messages rate-limited 0 per sec
```

```
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 information stored in 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
```

[For example]

Show logging file

show logging file

[Relevant command]

Command	Description
logging console	Enable output direction of logging console.
logging monitor	Enable output direction of logging monitor.
logging file	Enable output direction of logging file.
logging time-stamp	Set logging time-stamp.

3.148 Show loopback-detection

[Introduction]

Show the loopback detection state of the interface

show loopback-detection

[Parameter]

None

[Default]

None

[Mode]

Privileged configuration exec; privileged user (priority 5)

[Guide]

Only the user with the priority equal to or higher than 5 can use this command.

[Command Execution Echo]

·Show the loopback detection period. Show the loopback detection state of the interface, including the on-off state of the loopback detection function of the interface.

ENABLE——Open, DISABLE——Close;

Loopback: YES——Loopback, NO——Open; interface state; the original interface that has loopback with this interface.

[For example]

- Set the detection period to 3 seconds
 Raisecom(config)# **loopback-detection interval 3**
- Close the function on interface 1,14-16,21-26
 Raisecom(config)# **loopback-detection disable port-list 1,14-16,21-26**
- Show the state
 Raisecom# **show loopback-detection**

The shown content is as follow, interface 2 and 6 form outside loop, interface 9 forms a selfloop. The situations of starting STP and closing STP is different.

Starting STP:

Period of loopback-detection : 3 s

Port No.	detection state	loop flag	state	source port
1	DISABLE	NO	--	--
2	ENABLE	NO	--	--
3	ENABLE	NO	--	--
4	ENABLE	NO	--	--
5	ENABLE	NO	--	--
6	ENABLE	NO	--	--
7	ENABLE	NO	--	--
8	ENABLE	NO	--	--
9	ENABLE	YES	BLOCKING	9
10	ENABLE	NO	--	--
11	ENABLE	NO	--	--
12	ENABLE	NO	--	--
13	ENABLE	NO	--	--
14	DISABLE	NO	--	--
15	DISABLE	NO	--	--
16	DISABLE	NO	--	--
17	ENABLE	NO	--	--
18	ENABLE	NO	--	--
19	ENABLE	NO	--	--
20	ENABLE	NO	--	--
21	DISABLE	NO	--	--
22	DISABLE	NO	--	--
23	DISABLE	NO	--	--
24	DISABLE	NO	--	--
25	DISABLE	NO	--	--
26	DISABLE	NO	--	--

Closing STP:

Period of loopback-detection : 3 s

Port No.	detection state	loop flag	state	source port
----------	-----------------	-----------	-------	-------------

1	DISABLE	NO	--	--
2	ENABLE	NO	--	--
3	ENABLE	NO	--	--
4	ENABLE	NO	--	--
5	ENABLE	NO	--	--
6	ENABLE	YES	BLOCKING	2
7	ENABLE	NO	--	--
8	ENABLE	NO	--	--
9	ENABLE	YES	BLOCKING	9
10	ENABLE	NO	--	--
11	ENABLE	NO	--	--
12	ENABLE	NO	--	--
13	ENABLE	NO	--	--
14	DISABLE	NO	--	--
15	DISABLE	NO	--	--
16	DISABLE	NO	--	--
17	ENABLE	NO	--	--
18	ENABLE	NO	--	--
19	ENABLE	NO	--	--
20	ENABLE	NO	--	--
21	DISABLE	NO	--	--
22	DISABLE	NO	--	--
23	DISABLE	NO	--	--
24	DISABLE	NO	--	--
25	DISABLE	NO	--	--
26	DISABLE	NO	--	--

[Relevant command]

Command	Description
loopback-detection { <i>enable</i> <i>disable</i> }	Start/close the loopback detection function of the specified interface
port-list { <i>all</i> <i>port-list</i> }	
loopback-detection interval <1-65535>	Configure the loopback detection period

3.149 show mac-address-table l2-address

[Function Introduction]

Show all or some MAC address suitable to some condition

show mac-address-table l2-address [{ **port** *port-number* | **vlan** *vlan_id* }]

[Parameter]

- **mac-address-table** table of MAC address.
- **l2-address** layer 2 address
- **port** physical port.
- *port-number* physical port number, range from 1 to 26.
- **vlan** VLAN
- *vlan_id* VLAN ID, range from 1 to 4094.

[Default]

None

[Mode]

Privileged configuration exec, privileged user (priority 5)

[Guide]

Only privileged user whose priority is above or equal 5 can use the command.

[Command Execution Echo]

- Information of layer 2 address in the switch:
MAC address. Port number. VLAN identifier. layer 2 flags
 - Information of layer 2 address with the port X :
MAC address. VLAN identifier. layer 2 flags
 - Information of layer 2 address with the VLAN X:
MAC address. Port number. layer 2 flags
-

[For example]

- Show all mac-address-table
*Raisecom# **show mac-address-table l2-address***
- show all mac-address-table of port 5
*Raisecom# **show mac-address-table l2-address port 5***
- Show all mac-address-table of VLAN ID 4.
*Raisecom# **show mac-address-table l2-address vlan 4***

[Relevant command]

Command	Description
search <i>HHHH.HHHH.HHHH</i>	mac-address show status of mac-address in switch

3.150 show mac-address-table multicast

[Function Introduction]

Use the command to show layer 2 multicast entity of switch or referred VLAN.

[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]

None

[Mode]

Privileged configuration exec; privileged user

[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.

[Command Execution Echo]

[For example]

- Show all VLAN layer 2 multicast router information
Raisecom#show mac-address-table multicast

VLAN ID	MAC address	port
1	0100.5e08.0808	1,2,3
2	0100.5e08.0808	4,5,6
- Show layer 2 multicast router information of VLAN 1.
Raisecom#show mac-address-table multicast vlan 1

VLAN ID	MAC address	port
1	0100.5e08.0808	1,2,3
- Show all VLAN layer 2 multicast router count information.
Raisecom#show mac-address-table multicast count

VLAN ID	MAC address	port
1	0100.5e08.0808	1,2,3
2	0100.5e08.0808	4,5,6

Multicast Mac Entries for all vlans: 2
- Show layer 2 multicast router counter information of VLAN 2.
Raisecom#show mac-address-table multicast vlan 2 count

VLAN ID	MAC address	port
2	0100.5e08.0808	4,5,6

Multicast Mac Entries for all vlans: 1

[Relevant command]

Command	Description
ip igmp snooping static	Add a layer 2 port as multicast member.

3.151 show mac-address-table static

[Function Introduction]

Show all or some physical port as static MAC address.

show mac-address-table static [**port** *port-number* | **vlan** *vlan_id*]

[parameter]

- **mac-address-table** MAC addresss table
- **static** static address.
- **port** physical port.
- *port-number* physical port number ,range from 1 to 26.
- **vlan** VLAN;
- *vlan_id* VLAN ID,range from 1 to 4094.

[default]

None

[mode]

privileged configuration mode, privileged user (priority 5).

[guide]

Only privileged user whose priority is above or equal 5 can use the command.

[Command Execution Echo]

Information of static mac address in switch:
port No. VLAN ID static MAC Addr

[for example]

show static MAC address.

Raisecom# **show mac-address-table static**

[relevant commmand]

Command	Description
mac-address-table static	Set static MAC address.use no to delete.

3.152 show mirroring

[Function Introduction]

Show part of all mirroring rule information setting.

show mirroring [**source_port** *port-number*]

[Parameter]

- **mirroring** mirroring function.
- **source_port** mirroring port.
- *port-number* mirroring port number ,range from 1 to 26.

[Default]

None

[Mode]

Privileged configuration exec, privileged user (priority 5)

[Guide]

Only privileged user whose priority is above or equal 5 can use the command.

[Command Execution Echo]

- *The port list wrong!*
The entered port list number is wrong
- *Rule of mirror for port:*
port No. rule of mirror

- *No monitor port!*
- *Monitor port: X*
The current monitoring port is Port X

[For example]

Show mirroring rule of port 5.

Raisecom# **show mirroring source_port 5**

[Relevant command]

Command	Description
mirror source_port	set mirroring rule
no mirror source_port	delete a mirroring rule
no mirror all	delete all mirroring setting

3.153 show monitor_port

[Function Introduction]

Show mirroring monitor-port of current setting

show monitor_port

[Parameter]

monitor_port port used to monitor.

[Default]

None

[Mode]

Privileged configuration exec, privileged user

[Guide]

Only privileged user whose priority is above or equal 5 can use the command.

[Command Execution Echo]

- No monitor port!
There is no monitoring port.
- The monitor port : X
The current monitoring port is X.

[For example]

Show monitor-port of current setting.

Raisecom# **show monitor_port**

[Relevant command]

Command	Description
mirror monitor_port	set monitor-port
no mirror monitor_port	delete monitor-port

3.154 show qos cosq

[Function Introduction]

Show mode of queue service and parameter.

show qos cosq

[Mode]

Privileged user exec, common user, privileged user

[Guide]

The command shows qos of current system priority and parameter.

[Command Execution Echo]

Output message:

- qos
- queue 0 priority;
- queue 1 priority;
- queue 2 priority;
- queue 3 priority;
- delay-time

[For example]

Show qos of current system and correlation parameter.

Raisecom# **show qos cosq**

[Relevant command]

Command	Description
qos cosq weight	Confine qos as Weighted Round Robin.
qos cosq bounded	confine qos as Bound-delay
no qos cosq	confine qos as rigor priority

3.155 show qos map

[Function Introduction]

Show the compatible relation between vpt and priority queue.

show qos map

[Mode]

Privileged user exec, common user, privileged user.

[Guide]

The command is used to show the matching relation between vpt and priority queue.

[Command Execution Echo]

Getting priority “*priority*” matching cos queue failed.

Get priority matching cos queue failed will show message above. Priority is the vpt priority, successful getting will show matching relation.

[For example]

Raisecom# show qos map

[Relevant command]

Command	Description
qos map priority	Configure map relation of vpt and output queue.
no qos map priority	Restore vpt priority and output queue as default.

3.156 show qos pri-control

[Function Introduction]

show qos pri-control

[mode]

privileged user mode, common user, privileged user.

[guide]

The command show priority rule based on IP address , MAC address, VLAN priority, the mapping rule between TOS Precedence value and qos priority

[Command Execution Echo]

- Show current priority control based on mac address failed.
- Show current priority control based on VLAN ID failed.
- Show current priority control based on ip address failed.
- Show the mapping rule between TOS Precedence value and qos priority failed.
- Show port default priority configuration failed.

[for example]

Raisecom# show qos pri-control

[relevant commmand]

Command	Description
qos port	configure default priority of referred port.
qos ip-cos	configure priority rule based on IP address
qos mac-cos	configure priority rule based on MAC address
qos vlan-cos	configure priority rule based on referred VLAN
qos tos-cos	configure TOS Precedence value and qos priority

3.157 show rate-limit

[Function Introduction]

Show rate limit of setting.

show rate-limit port [*port-number*] [input | output]

[Parameter]

- **rate-limit** rate limit
- **port** physical port
- *port-number* physical port number.
- **input** the upstream direction of physical port.
- **output** the downstream direction of physical port

[Default]

None

[Mode]

Privileged configuration exec, privileged user (priority 5)

[Guide]

Only privileged user whose priority is above or equal 5 can perform the command.

[Command Execution Echo]

- Information of rate limit for port:
port No. rate-limit (Mbps) burst (KBps)

Show the port bandwidth control information
- Information of rate limit for VLAN:
VLAN ID in-rate(Mbps) in-burst(KBps) out-rate(Mbps) out-burst(KBps)

Show the VLAN bandwidth control information

[For example]

- Show all physical port and bandwidth control information.
raisecom# **show rate-limit port**
- Show bandwidth control information of VLAN 5.
raisecom# **show rate-limit vlan 5**

[Relevant command]

Command	Description
rate-limit port <i>port-number</i> rate-limit <i>rate</i> burst <i>burst</i>	set rate-limit of port
rate-limit vlan <i>vlan-id</i> input rate burst	set rate-limit of VLAN

3.158 show rmon alarms

[Function Introduction]

Use show rmon alarms to show information rmon alarm table

show rmon alarms

[Parameter]

None

[Mode]

Privileged configuration exec, privileged user

[Guide]

[Command Execution Echo]

rmon alarms the detailed information of rmon alarms is in RFC 1757.

[For 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
```

[Relevant command]

Command	Description
show rmon event	show the information of rmon events
show rmon history	show the information of rmon history.
show rmon statistics	show information of rmon statistics table

3.159 show rmon events

[Function Introduction]

Use show rmon event to show information of rmon events table.

show rmon event

[Parameter]

None

[Mode]

Privileged configuration exec, privileged user

[Guide]

rmon alarm the detailed information of rmon alarm is in RRFC 1757.

[Command Execution Echo]

None

[For 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.
```

[Relevant command]

Command	Description
show rmon history	show the information of rmon history table.
show rmon statistics	show the information of rmon statistics table.
show rmon alarm	show the information of rmon alarm table

3.160 show rmon history

[Function Introduction]

Use show rmon history to show the information of rmon history table.

show rmon history

[Parameter]

None

[Mode]

Privileged configuration exec, privileged user

[Guide]

rmon history the detailed information of rmon history table is in RFC 1757.

[Command Execution Echo]

None

[For example]

```
Raisecom#show rmon history  
Entry 1 is active, and owned by manager1  
Monitors ifEntry.1.1 every 30 seconds  
Requested # of time intervals, ie buckets, is 5  
Granted # of time intervals, ie buckets, is 5  
Sample # 14 began measuring at 00:11:00  
Received 38346 octets, 216 packets,  
0 broadcast and 80 multicast packets,  
0 undersized and 0 oversized packets,  
0 fragments and 0 jabbers,  
0 CRC alignment errors and 0 collisions.  
# of dropped packet events is 0  
Network utilization is estimated at 10
```

[Relevant command]

Command	Description
show rmon statistics	Show information of rmon statistics table
show rmon alarms	Show information of rmon alarm table.
show rmon events	Show information of rmon events

3.161 show rmon statistics

[Function Introduction]

Use show rmon statistics of rmon statistics table.

show rmon statistics

[Parameter]

None

[Mode]

Privileged configuration exec, privileged user

[Guide]

rmon statistics The detailed information of rmon statistics is shown in RFC 1757

[Command Execution Echo]

None

[For example]

```
Raisecom#show rmon statistics  
Interface 2 is active, and owned by monitorEtherStats  
Monitors 1.3.6.1.2.1.1.17825795(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
```

[Relevant 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.

3.162 show running-config

[Function Introduction]

Use show running-config to show the configuration information of current system.

show running-config

[Parameter]

None

[Mode]

Privileged configuration mode, privileged user

[Guide]

Show the configuration information of current system.!' stands for explanation. Use command write to write to flash memory.

[Command Execution Echo]

None

[For 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  
!
```

[Relevant command]

Command	Description
show startup-config	Show the system boot configuration information
download	Download system configuration file or boot file
upload	Upload the system configuration file or boot file
write	Store the current system configuration

3.163 show service

[Function Introduction]

“Show service” is used to display the running services in the system currently

show service

[Parameter]

None

[Mode]

Privileged configuration exec, privileged user

[Guide]

“Show service” is used to display the running services in the system currently.

[Command Execution Echo]

None

[For example]

```
raisecom#show service  
The switch system service information  
The Qos Service ..... ON  
The Filter Service ..... ON  
The Storm control Service ..... ON
```

The Authentication Service ON
 The IGMP Snooping Service ON
 The STP Service ON
 The RIP protocol Service ON
 The OSPF protocol Service ON
 The PIM-DM protocol Service ON
 The PIM-SM protocol Service ON

[Relevant command]

None

3.164 show snmp

[Function Introduction]

Use show snmp to show the information of sending and receiving of snmp diagram.

show snmp

[Parameter]

None

[Mode]

Privileged configuration mode, privileged user

[Guide]

Use the command to show the statistics of diagram received and sending.

[Command Execution Echo]

None

[For example]

Raisecom#show snmp

SNMP Information

SNMP packets input:36

The total number of Unsupported SNMP version SNMP PDUs: 0

The total number of Unknown SNMP community name SNMP PDUs: 0

The total number of SNMP community not allowed operation SNMP PDUs: 0

The total number of ASN.1 or BER errors SNMP PDUs: 0

The total number of too big SNMP PDUs: 0

The total number of name error SNMP PDUs: 0

The total number of bad value SNMP PDUs: 0

The total number of ReadOnly SNMP PDUs: 0

The total number of GenErrs SNMP PDUs: 0

The total number of Get-Request and Get-Next PDUs MIB objects SNMP PDUs: 0

The total number of Set-Request MIB objects SNMP PDUs: 0

The total number of Get-Request MIB objects SNMP PDUs: 0

The total number of Getnext-Request MIB objects SNMP PDUs: 0

The total number of Set-Request MIB objects SNMP PDUs: 0

The total number of Get-Response PDUs SNMP PDUs: 0

The total number of Received Traps SNMP PDUs: 0

SNMP packets output:0

The total number of error name SNMP PDUs: 0

The total number of too big SNMP PDUs: 0

The total number of bad value SNMP PDUs: 0

The total number of Gen Errs SNMP PDUs: 0
 The total number of Get request SNMP PDUs: 0
 The total number of Get-next SNMP PDUs: 0
 The total number of Set Request SNMP PDUs: 0
 The total number of Get Responses SNMP PDUs: 0
 The total number of Trap SNMP PDUs: 0

[Relevant command]

None

3.165 show snmp community

[Function Introduction]

Use show snmp community to show the community information of snmp protocol.

show snmp community

[Parameter]

None

[Mode]

Privileged configuration mode, privileged user

[Guide]

Use show snmp community to show the community information of snmp protocol.

[Command Execution Echo]

None

[For example]

*Raisecom#***show snmp community**

SNMP community Information

<i>Index</i>	<i>Community Name</i>	<i>View Name</i>	<i>Permission</i>
1	public	internet	rw

[Relevant command]

Command	Description
snmp community	Set snmp community information.
show snmp view	show snmp view information

3.166 show snmp contact

[Function Introduction]

Use show snmp contact to show contact information

show snmp contact

[Parameter]

None

[Mode]

Privileged configuration mode, privileged user

[Guide]

Show the contact information of snmp.

[Command Execution Echo]

None

[For example]

*Raisecom#***show snmp contact**

Contact Information: support@Raisecom.com

[Relevant command]

Command	Description
snmp-server contact	Set the contact information of snmp-server.

3.167 show snmp host

[Function Introduction]

Use show snmp host to show the information of trap server.

show snmp host

[Parameter]

None

[Mode]

Privileged configuration exec, privileged user

[Guide]

Use the command to show the ip address of trap server and the parameter setting of trap server.

[Command Execution Echo]

None

[For example]

```
Raisecom#show snmp host
IP Address Version Community Port Tags
-----
20.0.0.1 V2 public 163 snmp
20.0.0.2 V1 public 162 bridge config interface snmp rmon ospf
```

[Relevant command]

Command	Description
snmp host	Set trap server of snmp

3.168 show snmp location

[Function Introduction]

Use the command to show the location information of snmp.

show snmp location

[Parameter]

None

[Mode]

Privileged configuration mode, privileged user

[Guide]

Show the location information of SNMP

[Command Execution Echo]

None

[For example]

```
Raisecom#show snmp location
Device location: world china raisecom
```

[Relevant command]

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

snmp location Set the location information of snmp

3.169 show snmp view

[Function Introduction]

Use the command to show the view information of snmp.

show snmp view

[Parameter]

None

[Mode]

Privileged configuration mode, privileged user

[Guide]

Show the view information of snmp.

[Command Execution Echo]

None

[for example]

Raisecom#show snmp view

SNMP View Information

<i>Index</i>	<i>View Name</i>	<i>OID Tree</i>	<i>Type</i>
<i>0</i>	<i>system</i>	<i>1.3.6.1.2.1.1</i>	<i>include</i>
<i>1</i>	<i>internet</i>	<i>1.3.6</i>	<i>include</i>

[Relevant command]

Command	Description
show snmp community	Show the community information of SNMP
snmp view)Set the view information of snmp

3.170 show sntp

[Function Introduction]

Show the “snmp” information

show snmp

[Parameter]

None

[Default]

None

[Mode]

Privileged configuration exec; privileged user

[Guide]

Use the history studying information of snmp

[Command Execution Echo]

Show log information

Raisecom#show snmp

SNTP configuration information

SNTP server address:192.168.1.169

<i>SNTP server</i>	<i>Stratum</i>	<i>Version</i>	<i>Last Receive</i>
--------------------	----------------	----------------	---------------------

[For example]

Show log information of stored in file.

show sntp

[Relevant command]

Command	Description
sntp server	Learn the system time form sntp server.
sntp broadcast client	set the device as detector of sntp broadcast

3.171 show startup_config

[Function Introduction]

Use the command to show the stored startup-configuration information

[Parameter]

None

[Mode]

Privileged configuration exec; privileged user

[Guide]

Use the command to show the stored startup-configuration information, use write or download to refresh, or use erase to delete, or use upload to store.

[Command Execution Echo]

None

[For 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
```

[Relevant command]

Command	Description
show startup-config	show system startup configuration information
download	Download system file of startup file.

upload	Upload system configuration file or startup file.
write	Store system configuration of current system.
erase	delete referred file in system

3.172 show storm_control

[Function Introduction]

show storm_control [{ **broadcast** | **multicast** | **dlf** }]

[parameter]

- **storm_control** storm-control function
- **broadcast** broadcast packet.
- **multicast** multicast packet.
- **dlf** packet failed to reach destination

[default]

None

[mode]

privileged configuration mode; privileged user (priority 5)

[guide]

Only privileged user whose priority is above 5 or equal 5 can use this command.

[Command Execution Echo]

- Status of storm control:

Bcast	Mcast	DLF	limit(packets/s)

- This classes of packets have NOT rate limiting
- The rate limiting value is: X packets/s .
- This operation failed!

[for example]

Show storm control rule of setting:
 Raisecom# **show storm_control**

[relevant command]

Command	Description
storm_control	set storm-control rule
no storm_control	delete storm-control rule

3.173 show stp

[Function Introduction]

Show the active status and configuration of stp protocol.

show stp

[Mode]

Privileged configuration exec; privileged user

[Guide]

Show the active status and configuration of stp protocol.

[Command Execution Echo]

Command reactor follows, title column:

Row 1:

RootID, BridgeID show system ID of Root Bridge and self bridge

Root Cost show the cost of self-bridge to root-bridge.

Row 2:

Show whether STP is enabled and fast connecting and the top changing times

detected by STP

Row 3:

Show the common information of STP, including max-age, forward-delay, and hello-time

Row 4:

Show self-bridge information of max-age, forward-delay, hello-time value

Sub-column context:

Column 1:

Port number

Column 2:

portState, Status of the STP port, including "DISABLED", "LISTENING", "LEARNING", "FORWARDING", "BLOCKING"

Column 3:

state stands for the location of port, 'D' stands for referred port, 'R' stands for root port, 'B' stands for BLOCKING port.

Column 4:

The cost of self-port

Column 5:

If Dcost is referred port, the value is the cost of self-bridge to root-bridge. If it is not referred port, it is the cost of connected network to root-bridge.

Column 6:

The priority of STP port

Column 7:

portF stands for whether port fast function is enabled

Column 8:

Protocol stands for whether STP protocol is enabled.

RootID: 8000004047000000 BridgeID: 8000004047000000 Root Cost = 0
Spanning Tree ENABLED fastUplink DISABLED Top. Change = 0
STP Domain : Max Age = 20, Forward Delay = 15, Hello Time = 2
Bridge Info : Max Age = 20, Forward Delay = 15, Hello Time = 2

port	portState	state	Pcost	Dcost	Priority	portF	Protocol
1	DISABLED	D	19	0	128	OFF	Enabled
2	DISABLED	D	19	0	128	OFF	Enabled
3	DISABLED	D	19	0	128	OFF	Enabled
4	DISABLED	D	19	0	128	OFF	Enabled
5	DISABLED	D	19	0	128	OFF	Enabled
6	DISABLED	D	19	0	128	OFF	Enabled
7	DISABLED	D	19	0	128	OFF	Enabled
8	DISABLED	D	19	0	128	OFF	Enabled
9	DISABLED	D	19	0	128	OFF	Enabled
10	DISABLED	D	19	0	128	OFF	Enabled
11	DISABLED	D	19	0	128	OFF	Enabled
12	DISABLED	D	19	0	128	OFF	Enabled
13	DISABLED	D	19	0	128	OFF	Enabled
14	DISABLED	D	19	0	128	OFF	Enabled
15	DISABLED	D	19	0	128	OFF	Enabled
16	DISABLED	D	19	0	128	OFF	Enabled

17	DISABLED	D	19	0	128	OFF	Enabled
18	DISABLED	D	19	0	128	OFF	Enabled
19	DISABLED	D	19	0	128	OFF	Enabled
20	DISABLED	D	19	0	128	OFF	Enabled
21	DISABLED	D	19	0	128	OFF	Enabled
22	DISABLED	D	19	0	128	OFF	Enabled
23	DISABLED	D	19	0	128	OFF	Enabled
24	DISABLED	D	19	0	128	OFF	Enabled
25	DISABLED	D	19	0	128	OFF	Enabled
26	DISABLED	D	19	0	128	OFF	Enabled

[Relevant command]

Command	Description
stp	enable/disable stp
stp priority	Set the system priority or port priority of stp.
stp forward-delay	Set forward-delay
stp hello-time	set hello-time
stp path-cost	Set the path cost of stp

3.174 show svl

[Function Introduction]

Show configuration information of shared VLAN function

show svl

[Parameter]

- **svl** share the function of VLAN

[Default]

None

[Mode]

Privileged configuration exec; privileged user

[Guide]

Only users whose priority is above or equal 5 can use the command.

[Command Execution Echo]

- *The ports which in svl mode: XXX*
The information shows when the Port XXX is set to SVL mode

[For example]

- show the configuration of current SVL
*raisecom# **show svl***

[Relevant command]

Command	Description
svl { enable disable }	Enable/disable svl of shared VLAN

3.175 show terminal

[Function Introduction]

Show the terminal information of system

show terminal

[Parameter]

None

[Mode]

Privileged configuration exec; privileged user

[Guide]

Use the command to detect terminal information of system, including one console and five telnet console.

[Command Execution Echo]

None

[For 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   -              -
```

[Relevant command]

None

3.176 show vlan current

[Function Introduction]

Show the configuration information of all active VLAN of current system.

show vlan current

[mode]

privileged user mode;privileged user.

[guide]

the command shows the configuration information of all active VLAN

[Command Execution Echo]

```
*** Current VLAN X Configuration ***
VLAN member ports: 0-25
VLAN untagged ports: 0-25
VLAN status: Static
VLAN creation time: 0-Days 0-Hours 0-Minutes 0-Seconds
X 代表 VLAN ID;
Row 2 shows the member port list of VLAN
Row 3 shows the untagged port list of VLAN
Row 4 shows whether VLAN is static or dynamic.
Row 5 shows how long has VLAN been created after system starting
```

[relevant commmand]

Command	Description
vlan	enter configuration mode of static VLAN
name	set the name of static VLAN
state	Set the state of static VLAN
shutdown vlan	enable/disable static vlan
pvid	Set port VLAN ID
vlan-access	Set the access priority of static VLAN
show vlan static	show the configuration information of all static VLAN

3.177 show vlan static

[Function Introduction]

Show the configuration information of static VLAN

show vlan static [{1-4094}]

[Parameter]

{1-4094} VLAN ID list

[Mode]

Privileged user exec; privileged user

[Guide]

The command shows all configuration information of static VLAN, including active and suspended ones

[Command Execution Echo]

```
*** Static VLAN X Configuration ***
```

```
VLAN name: Default
```

```
VLAN member ports: 0-25
```

```
VLAN untagged ports: 0-25
```

```
VLAN active state: Active
```

X stands for VLAN ID;

Row 2 shows the name of static VLAN

Row 3 shows member port list of static VLAN

Row 4 shows untagged port list of static VLAN

Row 5 shows current active state of static VLAN

[Relevant command]

Command	Description
vlan	Enter static VLAN configuration mode;
name	Set name of static VLAN
state	Set the active state of static VLAN
shutdown vlan	Enable/disable static VLAN
pvid	Set port VLAN
pvid-space	Set up the ID range of PVID
vlan-access	Set the access priority of static VLAN

3.178 show uplink-port

[Function Introduction]

show current uplink-port.

show uplink-port

[parameter]

uplink-port port to uplink.

[default]

None

[mode]

privileged configuration mode;privileged user.

[guide]

Only users whose priority is above or equal 5 can use the command.

[Command Execution Echo]

- No uplink port !
- The uplink port : X

[for example]

show current uplink-port
 Raisecom# **show uplink-port**

[relevant commmand]

Command	Description
uplink-port	set uplink-port.
no uplink-port	delete uplink-port.

3.179 show user

[Function Introduction]

Use show user to show the user information stored in system.

show user

[Parameter]

None

[Mode]

Privileged configuration mode; privileged user

[Guide]

Use the command to inspect how many users can login the system. The information of users is stored in usertableconf. Users can use erase to delete the file to restore default user status.

[Command Execution Echo]

None

[For example]

```
Raisecom#show user
  User name      priority
  -----
  Raisecom              15
  factory              15
```

[Relevant command]

Command	Description
user	Set up the user information
user privilege	Set the privilege of user

3.180 show version

[Function Introduction]

Use show version to show system version.

[parameter]

None

[mode]

privileged configuration mode, privileged user.

[guide]

Use the command to show the software and system hardware version.

[Command Execution Echo]

None

[for example]

Raisecom#**show version**

Product name: ISCOM3026
Software RaiseComOS. Version 1.3.100.20040419.(Compiled Apr 20 2004, 14:28:44)
HardWare ISCOM3026. Version Rev.A
ISCOM3026 with
64M bytes DRAM
8 M bytes Flash Memory

Switch uptime is 0 days, 0 hours, 3 minutes

[relevant commmand]

None

3.181 shutdown

[Function Introduction]

Close physical port, use no to open.

shutdown

no-shutdown

[Parameter]

None

[Default]

The port is open in default.

[Mode]

Ethernet physical interface configuration mode; privileged user

[Guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- *SUCCESS!*
Set up successfully
- *This operation failed!*
Set up failed

[For example]

- Shut down the physical port
Raisecom(config-port)# shutdown
- Open the physical port
Raisecom(config-port)# no-shutdown

[Relevant command]

Command	Description
show interface port	show the state of some or all interface port

3.182 shutdown vlan

[Function Introduction]

Set the active state of static VLAN

shutdown vlan <2-4094>

no shutdown vlan <2-4094>

[parameter]

<2-4094> VLAN ID.

[default]

The new VLAN is suspend in default.

[mode]

global configuration mode;privileged user.

[guide]

The command is same to command state in static VLAN configuration mode.

[Command Execution Echo]

- static vlan *VID* not exist.
- shutdown successfully.
- shutdown failed.
- activate static vlan *VID* successfully.
- activate static vlan *VID* failed.

[for example]

- shutdown static VLAN 2
Raisecom(config)# **shutdown vlan 2**
- activate static VLAN 2
Raisecom(config)# **no shutdown vlan 2**

[relevant commmand]

Command	Description
vlan	enter the configuration mode of static VLAN
name	set the name of static VLAN
state	set the active state of static VLAN
pvid	set the property of VLAN ID
vlan-access	set the access property of port VLAN
show vlan static	set the configuration information of static VLAN
show vlan current	show the configuration information of all active VLAN

3.183 snmp-server community

[Function Introduction]

Set community name, and the relative view and access-priority.

[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** assign the access privilege to read-only
- **rw** assign the access privilege of community to read-write

[Default]

Community name is public; view is read-only to internet.

[Mode]

Global configuration exec; privileged user mode

[Guide]

In order to protect itself and MIB from unprivileged access, SNMP Agent affords the conception of community. SNMP Agent distributes privileged access users to community; every community has only a community name. Operation Get and Set use the name.

SNMPv1 and SNMPv2 use community name authentication, the SNMP diagrams

those don't coincide with community will be discarded. Different community has read-only or read-write priority. Read-only priority can query device information, read-write priority can also configure device.

Use the command relative view of referred community can be defined, which enable community to access MIB variable in view only. If view name is not input, default view is internet.

[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

[For 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**

[Relevant command]

Command	Description
snmp-server view	Set a view.
show snmp community	show all community
show snmp view	Show all the view

3.184 snmp-server contact

[Function Introduction]

Set up the network administrator ID and contact information.

[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>

[Mode]

Global configuration exec; privileged user mode

[Guide]

The information includes the contact information of network administrator, so when maintain work is needs, this information can be used to contact administrator.

[Command Execution Echo]

- *Set successfully!*
Set up successfully
- *Set fail!*

Set up failed

[For example]

Set up the contact information to service@raisecom.com
Raisecom(config)# snmp-server contact service @raisecom.com

[Relevant command]

Command	Description
show snmp contact	Show the contact information of network administrator.

3.185 snmp-server enable traps

[Function Introduction]

Enable the trap send function of SNMP

[Command Format]

[no] snmp-server enable traps [snmp | if | ospf |lacp |stp]

[Parameter]

- **snmp** snmp trap
- **if** interface trap
- **ospf** ospf trap
- **lacp** lacp trap
- **stp** stp trap

[Default]

[Mode]

Global configuration exec; privileged user mode

[Guide]

Use the command to enable or disable trap diagram. When trap diagram is permitted and device has something happened, SNMP TRAP diagram will be sent to trap server.

[Command Execution Echo]

- *Set successfully!*
Set up successfully
- *Set fail!*
Set up failed

[For example]

Enable trap of ospf
Raisecom(config)# snmp-server enable traps ospf

[Relevant command]

Command	Description
snmp-server host	set server of trap

3.186 snmp-server host

[Function Introduction]

Add or delete IP address of trap host

[Command Format]

[no] snmp-server host ip-address [host-name] [udp-port port-id]

[Parameter]

- *ip-address* the IP address of trap host, dotted decimal notation
- *host-name* trap host name
- *port-id* the udp port to receive trap diagram.

[Default]

Destination host list is empty in default.

[Mode]

Global configuration exec; privileged user mode

[Guide]

The IP address of trap destination host must be set before trap diagram is permitted. If hostname is not given, default name is set as Notify1, Notify2....., if udp port is not given, default value is 162.

[Command Execution Echo]

- *Set successfully!*
- *Set fail!*

[For example]

Set the destination host IP address as 10.0.0.1 and hostname as receiveTrap.
Raisecom(config)# snmp-server host 10.0.0.1 name receiveTrap

[Relevant command]

Command	Description
show snmp host	Show all snmp host.

3.187 snmp-server location

[Function Introduction]

Add or delete IP address of trap host

[Command Format]

[no] snmp-server host *ip-address* [*host-name*] [*udp-port port-id*]

[Parameter]

- *ip-address* the IP address of trap host, dotted decimal notation
- *host-name* trap host name
- *port-id* the udp port to receive trap diagram.

[Default]

Destination host list is empty in default.

[Mode]

Global configuration exec; privileged user mode

[Guide]

The IP address of trap destination host must be set before trap diagram is permitted. If hostname is not given, default name is set as Notify1, Notify2....., if udp port is not given, default value is 162.

[Command Execution Echo]

- *Set successfully!*
- *Set fail!*

[For example]

Set the destination host IP address as 10.0.0.1 and hostname as receiveTrap.
Raisecom(config)# snmp-server host 10.0.0.1 name receiveTrap

[Relevant command]

Command	Description
show snmp host	Show all snmp host.

3.188 snmp-server view

[Function Introduction]

Add a snmp-server view.

[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 32.
- **included** MIB variable in OID tree.
- **excluded** MIB variable out of OID tree.

[Default]

The default view is internet, including all the MIB variables of 1.3.6 tree.

[Mode]

Global configuration exec; privileged user mode

[Guide]

SNMPv3 defines access mode based on view. Users can use the command to define a view. Use `snmp-server community` to set the match relation of community and view, define the access priority of referred community.

[Command Execution Echo]

- Set successfully!
- Name too long !
The view name is longer than 32 bits.
- Oid tree Name too long!
The OID is longer than 32 bits.
- Oid tree Name NOT correct!
The entered the OID is illegal.
- Create View fail
Create view failed.

[For example]

Create view mib2, including all the MIB variable of 1.3.6.1.2.1
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 included

[Relevant command]

Command	Description
snmp-server community	Set snmp-server community.
show snmp view	show all the snmp view

3.189 sntp broadcast client

[Function Introduction]

Set the device as detector of sntp broadcast.

[no] sntp broadcast client

[Parameter]

None

[Default]

The function is disabled

[Mode]

Global configuration exec; privileged user

[Guide]

Use the command to configure detector of sntp diagram, when sntp is detected, set the time as system time.

[Command Execution Echo]

- set successfully!
- set fail!

[For example]

Set the client of sntp broadcast.

sntp broadcast client

[Relevant command]

Command	Description
sntp server	learn the system time of sntp server

3.190 sntp server

[Function Introduction]

Use the command to know the system time of sntp server.

sntp server A.B.C.D

[Parameter]

the IP address of sntp.

[Default]

the function is disabled.

[Mode]

Global configuration exec; privileged user

[Guide]

Use the command to learn system time of sntp server; when receive sntp diagram, set the time as system time

[Command Execution Echo]

·set successfully!
·set fail!

[For example]

Set studying-time of the device

sntp server 10.0.0.1

[Relevant command]

Command	Description
sntp broadcast client	Set broadcast client of sntp diagram

3.191 speed

[Function Introduction]

Use command speed 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.

[Mode]

Ethernet interface configuration mode; privileged user

[Guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- *SUCCESS!*
- *This operation failed!*

[For example]

Set up the physical port 4 to 1000Mbps half duplex
Raisecom(config-port)# speed 10 duplex half-duplex

[Relevant command]

Command	Description
duplex auto-negotiate	Set the duplex mode of port auto-negotiate.
speed auto-negotiate	Set the speed of port auto-negotiate.
show interface port	Show the state of some or all port.

3.192 speed auto-negotiate

[Function Introduction]

Set the speed of port auto-negotiate.

speed auto-negotiate

[Parameter]

auto-negotiate

[Default]

The speed of port is auto-negotiate in default.

[Mode]

Ethernet physical interface configuration mode; privileged user

[Guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- *SUCCESS!*
- *This operation failed!*

[For example]

Set the speed of physical port 5 auto-negotiate.
Raisecom(config-port)# speed auto-negotiate

[Relevant command]

Command	Description
speed	Set the speed of port and duplex mode.
duplex	set the duplex auto-negotiate.
auto-negotiate	
show interface port	show the state of some or all the port.

3.193 state

[Function Introduction]

Set the active state of static VLAN

state {active | suspend}

[Parameter]

- **active** Set static VLAN active
- **suspend** Set static VLAN suspend

[Default]

The state of new static VLAN is suspended state in default.

[Mode]

The configuration exec of static VLAN; privileged user

[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

[Command Execution Echo]

- *Set successfully.*
- *Set fail.*
- *Default vlan is always active.*

[For example]

```
Set VLAN 2 active,exit VLAN configuration mode;  
Raisecom(config-vlan)# state active  
Raisecom(config-vlan)# exit  
Raisecom(config)#
```

[Relevant 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

3.194 storm_control

[Function Introduction]

set the storm-control to broadcast,multicast and destination failed packet.Use no to cancel

```
storm_control { broadcast | multicast | dlf } limit packets-number  
no storm_control [ { broadcast | multicast | dlf } ]
```

[parameter]

- **enable** enable storm-control
- **disable** disable storm-control
- **broadcast** broadcast packet.
- **multicast** multicast packet.
- **dlf** destination failed packet.
- **limit** limit to storm
- *packets-number* the packet number of of strom-control.

[default]

- storm-control is enabled in default.
- storm-control to broadcast is enabled in default.
- storm-control to multicast is enabled in default.
- storm-control to dlf is enabled in default.
- limit to packet is 1024.

[mode]

global configuration mode; privileged user.

[guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- **SUCCESS!**
Setting storm function successfully will output the message.

- This operation failed!
Setting storm function fail will output the message.

[for example]

- enable storm-control function
Raisecom(config)# **storm_control enable**
- disable storm-control function
Raisecom(config)# **storm_control disable**
- Enable the broadcast storm control and the packet limit is 5000
Raisecom(config)# **storm_control broadcast limit 5000**
- disable storm-control to multicast packet.
Raisecom(config)# **no storm_control multicast**
- disable all storm-control
Raisecom(config)# **no storm_control**

[relevant commmand]

Command	Description
show storm_control	show storm-control to all or some packet.

3.195 stp

[Function Introduction]

Enable/disable stp

stp {enable | disable}

[Parameter]

- **enable** enable stp
- **disable** disable stp

[Default]

stp is enabled in default.

[Mode]

Global configuration exec or Ethernet layer 2 interface configuration mode; privileged user

[Guide]

stp can avoid network-loopback, but will occupy CUP. Users can enable or disable stp add cording to reality.

[Command Execution Echo]

- Set successfully.
Enable/disable stp successfully
- Set fail.
Enable/disable stp fail

[For example]

- disable stp globally
Raisecom(config)# **stp disable**
- enable stp globally
Raisecom(config)# **stp enable**
- Only stp is used in the port in ethernet layer 2 interface configuration mode
Raisecom(config-aggregator)# **stp disable**

[Relevant command]

Command	Description
show stp	Show the active status and configuration information of stp.
stp priority	Set system priority or port priority of stp.
stp hello-time	Set hello-time.

stp forward-delay	Set forward-delay
stp max-age	Set max-age
stp path-cost	set the path cost of stp.

3.196 stp forward-delay

[Function Introduction]

Set forward-delay, it is the delay time between changes of stp bridge port state.

stp forward-delay <4-30>

no stp forward-delay

[Parameter]

<4-30> the delay time of stp bridge port change, point is second.

[Default]

Forward-delay is 15 seconds in default.

[Mode]

Global configuration mode; privileged user

[Guide]

To avoid circulation, stp wait for a while before port change, the time is controlled by forward-delay. Users can adapt the value according to reality, when the network topology changes fast, decrease the value, and otherwise increase it. Use no stp forward-delay to restore default value

[Command Execution Echo]

- *Set successfully.*
- *Set fail.*

[For example]

Set up the "forward-delay" to 10

Raisecom(config)# stp forward-delay 10

[Relevant command]

Command	Description
show stp	show the active status and configuration information of stp
stp	enable/disable stp
stp priority	set the system priority or port priority of stp
stp forward-delay	Set forward-delay
stp hello-time	Set hello-time.
stp path-cost	set the path cost of stp

3.197 stp hello-time

[Function Introduction]

Set hello-time, it is the time slot of configuration information.

stp hello-time <1-10>

no stp hello-time

[Parameter]

<1-10> the time slot of sending configuration information, point is second.

[Default]

Hello-time is 2 seconds in default.

[Mode]

Global configuration exec; privileged user

[Guide]

The time slot of sending BPDU is 2 seconds in default. Users will adjust according to network. When the lost rate of configuration information is high, shorter time will enhance the robust performance of stp. Increasing value will decreasing the occupation of CPU. Use no stp hello-time to restore default value.

[Command Execution Echo]

- *Set successfully.*
- *Set fail.*

[For example]

- Set the value of hello-time 3 seconds
*Raisecom(config)# **stp hello-time 3***
- Restore the value of hello-time to 2 seconds.
*Raisecom(config)# **no stp hello-time***

[Relevant command]

Command	Description
show stp	Show the active status and configuration information of stp.
stp	Enable/disable stp
stp priority	Set the system priority or port priority of stp.
stp forward-delay	Set parameter forward-delay.
stp max-age	Set parameter max-age.
stp path-cost	Set path cost of stp.

3.198 stp max-age

[Function Introduction]

set the parameter max-age of stp,the max living time of bridge-configuration.

stp max-age <6-40>

no stp max-age

[parameter]

<6-40> the max living time of stp bridge configuration,point is second.

[default]

the value of max-ages is 20 seconds in default.

[mode]

global configuration mode; privileged user.

[guide]

the stp bridge configuration has living time ,when the configuration is overtime,stp will calculate st again..If the time is too short,calculation is frequency,if it is too long,stp will not adapt to the change of network topo.Use no stp max-age to restore default value.

[Command Execution Echo]

- set successfully
- set fail.

[for example]

Set max-age of stp 30 second.
*Raisecom(config)# **stp max-age 30***
Resume max-age of stp
*Raisecom(config)# **no stp max-age***

[relevant commmand]

Command	Description
show stp	Use the active status and configuration information of stp.
stp	enable/disable stp.
stp priority	set the system priority or port priority of stp.
stp forward-delay	Set parameter forward-delay of stp.
stp hello-time	set parameter hello-time of stp.
stp path-cost	set path cost of stp

3.199 stp path-cost

[Function Introduction]

Set the path cost of stp.

stp path-cost <1-65535>

no stp path-cost

[Parameter]

<1-65535> the path-cost of stp.

[Default]

The cost of port in default:

- 100 for 10Mbps
- 19 for 100Mbps
- 4 for 1000Mbps

[Mode]

Ethernet layer 2 interface configuration exec; privileged user

[Guide]

When STP calculates ST, root port and designated port must be selected, the lower cost of the port, and the more easily it is selected as root port or designated port.

[Command Execution Echo]

- *Set successfully.*
- *Set fail.*

[For example]

Set the cost of stp 30

Raisecom(config-aggregator)# stp path-cost 30

[Relevant command]

Command	Description
show stp	show the active status and configuration information of stp
stp	enable/disable stp
stp priority	set the system priority or port priority of stp
stp forward-delay	set the parameter forward-delay of stp
stp hello-time	Set the parameter hello-time of stp

3.200 stp priority

[Function Introduction]

Set the system priority or port priority in global configuration mode.

stp priority <1-65535>

no stp priority

[Parameter]

<1-65535> the priority of stp ranging from 1 to 65535

[Default]

The system priority of stp is 32768 in default.

[Mode]

Global configuration mode; privileged user

[Guide]

STP selects Root Bridge according system ID. The more minor system ID is, the more possible it is selected as Root Bridge. System ID comprises of 8 byte. The 2 highest network sequence bytes is priority of system, the next 6 bytes is MAC address. So system ID number is system priority. Use no stp priority to restore default system priority.

[Command Execution Echo]

- *Set successfully.*
- *Set fail.*

[For example]

Set the priority of stp or port 10.

*Raisecom(config)# **stp priority 10***

[Relevant command]

Command	Description
show stp	show the active status and configuration information of stp
stp	enable/disable stp
Stp hello-time	a parameter of stp
Stp forward-delay	a parameter of stp
Stp max-age	a parameter of stp
Stp path-cost	Set the path cost of stp

3.201 stp priority

[Function Introduction]

Set the port priority of stp in ethernet layer 2 interface configuration mode.

stp priority <1-255>

no stp priority

[Parameter]

<1-255> the port priority of stp.

[Default]

The priority of stp port is 128 in default.

[Mode]

Ethernet layer 2 interface configuration exec; privileged user

[Guide]

When STP calculate ST, root port and designated port must be selected, the lower priority of the port, the more easily it is selected as root port or designated port. Users can select given port as root port or designated port by setting port priority. Users can use no stp priority to restore default value in Ethernet layer 2 interface configuration mode.

[Command Execution Echo]

- *Set successfully.*
- *Set fail.*

[For example]

Set the priority of stp port 100

Raisecom(config-aggregator)# **stp priority 100**

[Relevant command]

Command	Description
show stp	Show the stp active state and configuration information
stp	Enable/disable stp
stp priority	Set the system priority or port priority of stp.
stp forward-delay	Set the forward-delay of stp.
stp hello-time	Set the hello-time of stp
stp path-cost	Set the path cost of stp

3.202 svl

[Function Introduction]

Enable/disable shared VLAN mode.

svl { enable | disable }

[Parameter]

- **enable** enable SVL function
- **disable** disable SVL function

[Default]

- SVL function is “disabled” in default.

[Mode]

Physical interface configuration exec of Ethernet; privileged user (priority 5)

[Guide]

Only users whose priority is 15 can use the command.

[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

[For example]

- Enable the SVL at Port 5
rc2126(config-port)# svl enable
- Disable the SVL at Port 5
rc2126(config-port)# svl disable

[Relevant command]

Command	Description
show svl	show the configuration information of shared VLAN function.

3.203 terminal history

[Function 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

[Mode]

Initial exec; common user, privileged user

[Guide]

Use the command to change the history command number input by console, making it clearer to show history command.

[Command Execution Echo]

Set successfully.

[For example]

Raisecom>terminal history 10

[Relevant command]

Command	Description
history	show the history command of the console

3.204 terminal time-out

[Function 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.

[Mode]

Initial exec; common user, privileged user

[Guide]

Use the command to change the configuration information when the console logout because of time-out.

[Command Execution Echo]

Set successfully.

[For example]

Raisecom> terminal time-out 1000

[Relevant command]

Command	Description
show terminal	Show the information of terminal.

3.205 timer flush

[Introduction]

Set the invalid period of the RIP Router received by every interface, viz, the waiting time of the Router from invalidation to being deleted. To restore to the default configuration using the command **no timer flush**.

timer flush *timeout*

no timer flush

[Parameter]

· *timeout* the time interval of the Router from invalidation to being deleted, the unit

is second. The data type is integer, the range is between 180~500 seconds.

[Default]

The default interval is 300 seconds

[Mode]

RIP protocol configuration mode; privileged user.

[Guide]

Using the command **timer flush** to set the invalid period of the RIP Router received by every interface, viz the waiting time of the Router from invalidation to being deleted. To restore to the default configuration using the command **no timer flush**.

[Command Execution Echo]

- set rip flush timer is success
- set rip flush timer is failure

[For example]

- Set the period to 200 seconds
Raisecom(config-router-rip)# **timer flush 200**
- Restore to the default value
Raisecom(config-router-rip)#**no timer flush**

[Relevant command]

Command	Description
router rip	Set the RIP protocol to be valid and enter the RIP protocol configuration mode
show ip protocol	Show the configuration information of the Router protocol

3.206 timer invalid

[Introduction]

The living period of the RIP Router received by every interface, viz, the waiting time of the Router from the receiving state to being set to be invalidation. To restore to the default configuration using the command **no timer invalid**.

timer invalid *timeout*

no timer invalid

[Parameter]

·*timeout* The time interval of the Router from the receiving state to being set to be invalidation. The unit is second. The data type is integer, its range is between 120~180 seconds.

[Default]

The default time interval is 180 seconds

[Mode]

RIP protocol configuration mode; privileged user.

[Guide]

Set the living period of the RIP Router received by every interface by using the command **timer invalid**, viz, the waiting time of the Router from the receiving state to being set to be invalidation. To restore to the default configuration using the command **no timer invalid**.

[Command Execution Echo]

- set rip invalid timer is success
- set rip invalidtimer is failure

[For example]

- Set the period to 150 seconds
Raisecom(config-router-rip)# **timer invalid 15**
- Restore to the default value
Raisecom(config-router-rip)#**no timer invalid**

[Relevant command]

Command	Description
router rip	Set the RIP protocol to be valid and enter the RIP protocol configuration mode
show ip protocol	Show the configuration information of the Router protocol

3.207 timer update

[Introduction]

Set the update period of every interface when sending RIP message. Restore to the default configuration by using the command **no ip rip update-timer**.

timer update *timeout*

no timer update

[Parameter]

·*timeout* Time interval for the sending of updating the message period, the unit is second, the data type is integer, its range is between 30~500 seconds.

[Default]

The default sending period is 30 seconds.

[Mode]

RIP protocol configuration mode; privileged user.

[Guide]

Set the update period of every interface when sending RIP message by using the command **timer update**. Adjust the frequency of the present interface sending period updating message. Restore to the default configuration by using the command **no timer update**.

[Command Execution Echo]

- set rip update timer is success
- set rip update timer is failure

[For example]

- Set the period to 50 seconds
Raisecom(config-router-rip)# **timer update 50**
- Restore to the default value
Raisecom(config-router-rip)#**no timer update**

[Relevant command]

Command	Description
router rip	Set the RIP protocol to be valid and enter the RIP protocol configuration mode
show ip protocol	Show the configuration information of the Router protocol

3.208 trans-eapol

[Function Introduction]

Enable or disable function to transfer EAOOL diagram.

trans-eapol *port-number*

no trans-eapol

[Parameter]

port-number The port number transferred by EAPOL diagram ,range from 1 to 26.

[Default]

Disable the function

[Mode]

Global configuration mode, privileged user (priority 15)

[Guide]

The port number referred by the command is uplink port.

[Command Execution Echo]

- Set transmission EAPOL packet on the specified port failed.
- Set transmission EAPOL packet on the specified port successfully.

[For example]

- Enable the function to transfer EAPOL diagram in port 3
Raisecom (config)# **trans-eapol 3**
- Disable the function to transfer EAPOL diagram.
Raisecom (config)# **no trans-eapol**

[Relevant command]

Command	Description
show running	show the running configuration information

3.209 uplink-port

[Function Introduction]

set uplink port,command no is used to delete port

uplink-port *port-number*

no uplink-port

[parameter]

port-number physical port number that ranges from 1 to 26.

[default]

there is no uplink port in default.

[mode]

global configuration mode; privileged user

[guide]

Only users whose priority is 15 can use the command.

[Command Execution Echo]

- The uplink port %d is not in VLAN %d ,please reset uplink port or VLAN!
- SUCCESS!
- No uplink port!
- Some vlan has been set rate-limit, please delete it first!

[for example]

- set port 26 as uplink port.
Raisecom(config)# **uplink-port 26**
- delete uplink port
Raisecom(config)# **no uplink-port**

[relevant commmand]

Command	Description
show uplink-port	show the port to uplink.
rate-limit vlan	set the bandwidth of VLAN

3.210 upload

[Function 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

[Default]

None

[Mode]

Privileged configuration exec, privileged user

[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 is sure to configure and switch system is connected to the server.

[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!*

[For 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 to download startup file from ftp server.*

[Relevant command]

Command	Description
download	Download configuration file or startup file of system.

3.211 user

[Function 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** Plain Text Password without encryption
- **md5** password with MD5 encryption
- **PASSWORD** password information.

[Default]

- The user's hostname is Raisecom added by the command; command hostname is used to change the hostname of user.
- The priority of user added by the command is command user privilege is used 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.

[Mode]

Privileged configuration exec, privileged user (Priority 15)

[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.

[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!*

[For 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***

[Relevant 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

3.212 User-access-list

[Introduction]

This command defines a list item of the access control list defined by the user. Using the command **no** to delete the item.

user-access-list <0-99> (**deny|permit**) MATCH-STRING MATCH-MASK OFFSET

[Parameter]

0-99: The serial number of the access control list

permit: Allow the message that satisfying the condition to pass through.

deny: Forbid the message that satisfying the condition to pass through.

MATCH-STRING: The match character string defined by the user. It must be made of a hexadecimal number; the number of characters must be even.

MATCH-MASK: Match mask, which is used to 'and' operation with the data package

OFFSET: offset, whose benchmark is at the beginning of the head of MAC frame. It defines the position of the character from where to do the 'and' operation. MATCH-MASK and OFFSET work in pairs. They will compare the MATCH-STRING defined by the user with the character string from the message, and find the matching message for corresponding operation.

[Default]

None

[Mode]

Global configuration mode; privileged user

[Guide]

This command defines a list item of the access control list defined by the user. When the data message satisfies this rule, use parameter *permit* / *deny* to decide whether the Switch will transmit or discard the message. This command only set the filtering rules of data. It always works with physical port or VLAN to form the total matching rule. It is set when configuring the filter.

[Command Execution Echo]

- Length of match data and mask is not equal!
- Length of match data must be EVEN and less 129!
- The match data overrun the frame!
- The match data is INVALID!
- SUCCESS!
- The operation fail!

[For example]

- user-access-list 50 1234 ffff 20

[Relevant command]

Command	Description
no user-access-list {{0-99}} any	Delete the specified list item of the access control list defined by the user
show user-access-list {{0-99}} any	Show the specified list item of the access control list defined by the user

3.213 user login

[Function Introduction]

set the authentication mode of login.

user login { local-user | radius-user | all }

[parameter]

- **local-user** use local configuration file to authenticate user.
- **radius-user** user RADIUS server to authenticate user.
- **all** use local configuration file to authenticate user,if it is not available,RADIUS server is used to authenticate user.

[default]

local configuration file is used in default.

[mode]

privileged configuration mode, privileged user. (priority 15).

[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.

[Command Execution Echo]

- Set User Login Method failed.
- Set User Login Method successfully.

[for example]

- Set all as the authentication type of login
Raisecom# **user login all**
- set local-user as the authentication type of login.
Raisecom# **user login local-user**

[relevant command]

Command	Description
radius-authserver host	set the IP address of RADIUS server.
radius-authserver key	Set the shared key between user and server when RADIUS authentication is used.

3.214 user privilege

[Function Introduction]

Use the command to set the priority of users.

user USERNAME privilege <1-15>

[Parameter]

- **USERNAME** user name
- **<1-15>** user priority

[Default]

The default priority of users is 15.

[Mode]

Privileged configuration exec, privileged user (Users of priority 15 can perform the command)

[Guide]

When the priority of some user is restricted, this command is used to forbidden him to execute some command. When the command of priority is below 5, the user will become common user from privileged user. In order to avoid failure of executing all the commands because of user's setting low priority, users can not change the priority of login user, and then at least one user's priority is sure to be 15.

[Command Execution Echo]

- *Set successfully.*
- *Can not change user privilege!*
- *You have no enough right to change user information!*

[For example]

Set privilege of user abc is 4
Raisecom# **user abc privilege 4**

[Relevant command]

Command	Description
user	Add user and set his password.
show user	Show the information of user

3.215 vlan

[Function Introduction]

Create VLAN or enter static VLAN mode.

vlan <1-4094>

no vlan {all | <2-4094>}

[Parameter]

- <1-4094> VLAN ID
- **all** All the static VLAN except default VLAN(VLAN ID is 1).
- <2-4094> VLAN ID

[Default]

In default, VLAN 1 is available in system, all the ports is available in default VLAN 1, their port VLAN ID is 1.

[Mode]

Global configuration exec; privileged user

[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.

[For example]

- Enter configuration mode of static VLAN 4094.
Raisecom(config)# vlan 4094
- Delete VLAN 2 form system.
Raisecom(config)#no vlan 2

[Relevant command]

Command	Description
name	The name static VLAN.
state	Set activation state of static VLAN.
shutdown	Shut down/startup configuration of static VLAN
pvid	Set the port attribute of port VLAN ID.
vlan-access	Set the port attribute of VLAN access.
show vlan static	Show configuration information of static VLAN.
show vlan current	Show all the configuration of current active VLAN.

3.216 vlan-access

[Function Introduction]

Set the access attribute of VLAN port.

vlan-access {all | {1-4094}} {tagged | untagged | forbidden}

no vlan-access {all | {1-4094}}

[Parameter]

- **all** all VLAN
- {1-4094} list of VLAN ID
- **tagged** access type of tagged vlan, VLAN frames must have tag information when it is sent from the port.
- **untagged** access type of untagged vlan, VLAN frames need not have tag

information when it is sent from the port.

- **forbidden** access type of forbidden, GVRP protocol is forbidden to register and configure attribute of VLAN.

[Default]

In default, all the ports is available in default VLAN (VLAN ID is 1).

[Mode]

Ethernet physical interface configuration exec; privileged user

[Guide]

when the device of switch port connected to network can not acknowledge 802.1Q frame, access mode of untagged can be set to it's PVID, when the device of switch port connected to network can acknowledge 802.1Q frame, then access mode of tagged can be set. The user can set attribute of forbidden to disable

GVRP protocol to register VLAN attribute in the port when it is not permitted.

[Command Execution Echo]

- *Static vlan VID not exist.*
- *Set successfully.*
- *Set failed.*

[For example]

- Add port to VLAN 2 in the form of untagged.
Raisecom(config-port)# **vlan-access 2 untagged**
- Delete static VLAN attribute of all ports.
Raisecom(config-port)# **no vlan-access all**
- Delete port access attribute for VLAN 2、3、6、7、8.
Raisecom(config-port)# **no vlan-access 2,3,6-8**

[Relevant command]

Command	Description
vlan	enter the configuration mode of static VLAN
name	set the name of static VLAN
state	Set the action state of static VLAN
shutdown vlan	shutdown/startup static VLAN
pvid	set the port of port VLAN ID
show vlan static	show configuration information of static VLAN
show vlan current	show all the configuration information of current active VLAN

3.217 write

[Function Introduction]

The command is used to save configuration information of current system.

[Parameter]

None

[Mode]

Privileged configuration exec, privileged user

[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.

[Command Execution Echo]

- *Save current configuration successfully!*

- *Save current configuration Fail!*

[For example]

Raisecom#write

[Relevant 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