

www.raisecom.com

ISCOM2126EA-MA Command Notebook

24-08-2009

Legal Notices

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

Warranty.

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

Restricted Rights Legend.

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

Copyright Notices.

Copyright ©2007 Raisecom. All rights reserved.

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

Trademark Notices

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

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

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

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

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

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

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

Microsoft Corporation.

Contact Information

Technical Assistance Center

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

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

Tel: +86-10-82883305

Fax: +86-10-82883056

World Wide Web

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

<http://www.raisecom.com>

Feedback

Comments and questions about how the ... system software works are welcomed. Please review the FAQ in the related manual, and if your question is not covered, send email by using the following web page:

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

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

export@raisecom.com

We hope to hear from you!

Chapter 1 System Commands ----- 17

1.1	clear.....	17
1.2	clear device statistics.....	17
1.3	console-cli.....	18
1.4	debug.....	19
1.5	dir.....	21
1.6	download	22
1.7	driver.....	24
1.8	enable.....	25
1.9	enable login	26
1.10	enable password	27
1.11	erase.....	28
1.12	exit.....	29
1.13	help.....	30
1.14	history	31
1.15	interface port.....	32
1.16	interface range.....	33
1.17	list	33
1.18	logout.....	35
1.19	password	35
1.20	ping.....	36
1.21	quit.....	38
1.22	radius accounting-server	39
1.23	radius accounting-server key	40
1.24	reboot	41
1.25	show device statistics	42
1.26	show radius-server	44
1.27	show running-config	45
1.28	show startup-config.....	46
1.29	show user	48
1.30	show version.....	49
1.31	terminal history	50
1.32	terminal time-out.....	51
1.33	user.....	52
1.34	user login	53
1.35	user name privilege	55
1.36	write	56

Chapter 2 Mirror Commands ----- 58

2.1	mirror	58
2.2	mirror block-non-mirror	59
2.3	mirror divider.....	60
2.4	mirror filter	61
2.5	mirror monitor-port.....	63
2.6	mirror source-port-list.....	64

2.7	mirror source-port-list ingress egress	65
2.8	show mirror	67
Chapter 3	Bandwidth Management Commands -----	70
3.1	clear double-tagging-vlan statistics	70
3.2	clear rate-limit statistics vlan	71
3.3	rate-limit double-tagging-vlan	72
3.4	rate-limit egress	74
3.5	rate-limit flow-control	75
3.6	rate-limit ingress	76
3.7	rate-limit vlan	78
3.8	show rate-limit	79
3.9	show rate-limit vlan	80
Chapter 4	Commands of MAC Address Management -----	83
4.1	clear mac-address-table	83
4.2	mac-address-table aging-time	84
4.3	mac-address-table learning	85
4.4	mac-address-table static multicast	86
4.5	mac-address-table static unicast	88
4.6	mac-address-table threshold	89
4.7	search mac-address	90
4.8	show mac aging-time	91
4.9	show mac-address-table multicast	92
4.10	show mac-address-table static	94
4.11	show mac-address-table threshold	95
Chapter 5	Physical Interface Management Commands -----	98
5.1	description	98
5.2	duplex	99
5.3	dynamic statistics time	100
5.4	flowcontrol {receive send}	101
5.5	show interface port	103
5.6	show system mtu	104
5.7	shutdown	105
5.8	speed	106
5.9	system mtu	107
Chapter 6	Commands of Storm-control -----	110
6.1	show storm-control	110
6.2	storm-control	111
Chapter 7	Transparent Transmission and Forward Commands -----	113
7.1	clear relay statistics	113
7.2	no relay shutdown	114
7.3	relay	114
7.4	relay cos	116
7.5	relay destination-address	117
7.6	relay drop-threshold	118

7.7	relay port.....	119
7.8	relay shutdown-threshold.....	120
7.9	show relay	121
7.10	show relay statistics.....	122
Chapter 8	Layer-3 Interface Commands -----	125
8.1	description	125
8.2	interface ip	126
8.3	ip address	126
8.4	show interface ip.....	128
8.5	show interface ip description	129
8.6	show interface ip statistics	130
Chapter 9	Trunk Group Commands -----	133
9.1	show trunk	133
9.2	trunk.....	134
9.3	trunk group	135
9.4	trunk loading-sharing mode	136
9.5	trunk loading-sharing ticket-generation-algorithm.....	138
Chapter 10	STP Commands -----	141
10.1	instance vlan.....	141
10.2	name.....	142
10.3	show spanning tree	143
10.4	show spanning-tree port-list/line/client.....	147
10.5	show spanning-tree region-operation	149
10.6	spanning-tree.....	151
10.7	spanning-tree clear statistics	152
10.8	spanning-tree edged-port	153
10.9	spanning-tree extern-path-cost.....	154
10.10	spanning-tree forward-delay	155
10.11	spanning-tree hello-time	157
10.12	spanning-tree inter-path-cost.....	158
10.13	spanning-tree link-type	159
10.14	spanning-tree max-age.....	160
10.15	spanning-tree mcheck	162
10.16	spanning-tree mode.....	163
10.17	spanning-tree region-configuration	164
10.18	spanning-tree rootguard	165
Chapter 11	DHCP Commands -----	169
11.1	ip address dhcp vlanid	169
11.2	ip dhcp client.....	171
11.3	ip dhcp client renew	173
11.4	ip dhcp information option attach-string	175
11.5	ip dhcp information option circuit-id	176
11.6	ip dhcp information option remote-id.....	178
11.7	ip dhcp snooping	179

11.8	ip dhcp snooping information option	181
11.9	ip dhcp snooping port-list.....	182
11.10	ip dhcp snooping trust.....	183
11.11	show ip dhcp client	185
11.12	show ip dhcp information option	188
11.13	show ip dhcp snooping	189
11.14	show ip dhcp snooping binding.....	190
Chapter 12 IGMP Commands		193
12.1	clear mvr port statistics	193
12.2	ip igmp filter vlan.....	194
12.3	ip igmp max-groups	195
12.4	ip igmp max-groups action.....	196
12.5	ip igmp querier.....	198
12.6	ip igmp querier query-interval	199
12.7	ip igmp snooping immediate-leave	200
12.8	ip igmp snooping mrouter	201
12.9	ip igmp snooping timeout.....	203
12.10	ip igmp snooping vlan-list	204
12.11	mvr immediate	205
12.12	mvr mode.....	207
12.13	mvr proxy.....	208
12.14	mvr proxy last-member-query	210
12.15	mvr proxy query-max-response-time	211
12.16	mvr proxy source-ip	213
12.17	mvr proxy suppression.....	214
12.18	mvr timeout.....	216
12.19	mvr type.....	217
12.20	mvr vlan	219
12.21	mvr vlan group.....	220
12.22	permit deny	222
12.23	range	223
12.24	show ip igmp filter	225
12.25	show ip igmp filter port.....	226
12.26	show ip igmp filter vlan	227
12.27	show ip igmp profile	229
12.28	show ip igmp snooping	230
12.29	show mvr	232
12.30	show mvr member	233
12.31	show mvr port	234
Chapter 13 RMON Commands		238
13.1	clear rmon.....	238
13.2	rmon alarm	238
13.3	rmon event.....	240
13.4	rmon history	242

13.5	rmon statistic	244
13.6	show rmon	245
Chapter 14 ARP Management Commands -----		255
14.1	arp	255
14.2	clear arp.....	256
14.3	show arp	257
Chapter 15 SNMP Commands -----		260
15.1	show snmp access	260
15.2	show snmp community	261
15.3	show snmp config	262
15.4	show snmp group	263
15.5	show snmp host.....	265
15.6	show snmp statistics.....	265
15.7	show snmp trap remote	267
15.8	show snmp user	268
15.9	show snmp view	270
15.10	snmp trap remote	271
15.11	snmp-server access.....	272
15.12	snmp-server community	275
15.13	snmp-server contact	277
15.14	snmp-server enable traps	278
15.15	snmp-server group	279
15.16	snmp-server host.....	281
15.17	snmp-server location	283
15.18	snmp-server user.....	284
15.19	snmp-server view	286
Chapter 16 Cluster Management Commands -----		290
16.1	cluster	290
16.2	cluster-autoactive	291
16.3	cluster-autoactive commander-mac.....	292
16.4	member	293
16.5	member auto-build.....	296
16.6	rcommand.....	299
16.7	rndp	300
16.8	rtdp	301
16.9	rtdp max-hop	303
16.10	show cluster member.....	304
16.11	show rndp	306
16.12	show rndp neighbor	307
16.13	show rtdp	308
16.14	show rtdp device-list	309
Chapter 17 System Log Commands -----		313
17.1	logging console.....	313
17.2	logging file	314

17.3	logging host	316
17.4	logging on	317
17.5	logging time-stamp	318
17.6	show logging.....	320
Chapter 18 Schedule Commands -----		323
18.1	cmd-str schedule-list.....	323
18.2	schedule-list.....	326
18.3	show schedule-list	328
Chapter 19 Trouble Shooting Commands -----		330
19.1	driver.....	330
19.2	show buffer	332
19.3	show diags.....	333
19.4	show memory	333
19.5	show tech-support	335
Chapter 20 Commands of Storm-control -----		337
20.1	creat vlan	337
20.2	name.....	338
20.3	show interface port switchport	338
20.4	show vlan.....	340
20.5	state.....	342
20.6	switchport access egress-allowed vlan.....	343
20.7	switchport access vlan.....	345
20.8	switchport mode	346
20.9	switchport trunk allowed vlan.....	348
20.10	switchport trunk native vlan	350
20.11	switchport trunk untagged vlan	351
20.12	vlan	353
Chapter 21 QinQ and VLAN Configuration Commands -----		356
21.1	mls double-tagging tpid.....	356
21.2	show interface vlan-mapping add-outer.....	357
21.3	show interface vlan-mapping translate	358
21.4	show switchport qinq	360
21.5	switchport qinq dot1q-tunnel.....	361
21.6	switchport vlan-mapping add-outer.....	362
21.7	switchport vlan-mapping translate	364
Chapter 22 ACL and Network Security Commands -----		367
22.1	access-list-map.....	367
22.2	clear filter statistics	368
22.3	filter.....	369
22.4	filter {enable disable}	371
22.5	ip-access-list.....	372
22.6	mac-access-list.....	373
22.7	match arp.....	375
22.8	match ip	376

22.9	match ip icmp	380
22.10	match ip igmp	381
22.11	match ip tcp	383
22.12	match ip udp	385
22.13	match user-define	387
22.14	match(ACLMAP layer 2)	389
22.15	show access-list	391
22.16	show access-list-map	392
22.17	show filter	392
Chapter 23 Commands of Storm-control -----		395
23.1	class-map(config)	395
23.2	class-map(config-pmap)	396
23.3	clear service-policy statistics	398
23.4	match.....	399
23.5	mls qos mapping cos.....	400
23.6	mls qos mapping dscp.....	401
23.7	mls qos port-priority	402
23.8	mls qos queue scheduler sp	403
23.9	mls qos queue scheduler wrr.....	404
23.10	mls qos queue wrr	405
23.11	mls qos trust port-priority	406
23.12	mls qos {aggregate-policer class-policer single-policer }	407
23.13	police	409
23.14	policy-map	410
23.15	redirect-to port	411
23.16	service-policy.....	412
23.17	set.....	413
23.18	show class-map.....	414
23.19	show mls qos.....	415
23.20	show mls qos mapping cos.....	416
23.21	show mls qos mapping dscp.....	417
23.22	show mls qos mapping localpriority	417
23.23	show mls qos policer	418
23.24	show mls qos port.....	419
23.25	show mls qos queue	420
23.26	show policy-map	422
23.27	show service-policy statistics.....	424
23.28	trust cos.....	425
23.29	trust dscp	426
Chapter 24 Dynamic ARP Inspection Commands-----		429
24.1	debug dai.....	429
24.2	ip arp-inspection	430
24.3	ip arp-inspection trust	432
24.4	show ip arp-inspection	433

Chapter 25	Keepalive Commands	435
25.1	show keepalive	435
25.2	snmp-server keepalive-trap	436
25.3	snmp-server keepalive-trap interval.....	437
Chapter 26	Unicast Router Commands	440
26.1	ip default-gateway	440
26.2	ip route.....	441
26.3	ip route aging-time	442
26.4	ip routing.....	444
26.5	show ip protocol.....	444
26.6	show ip route	446
Chapter 27	OAM Commands	451
27.1	clear oam event	451
27.2	clear oam statistics	451
27.3	oam enable	452
27.4	oam peer event trap.....	453
27.5	oam remote-loopback	454
27.6	show oam	455
27.7	show oam loopback.....	457
27.8	show oam peer	458
27.9	show oam peer event	460
27.10	show oam statistics.....	462
27.11	show oam trap	464
Chapter 28	Extended OAM Commands	468
28.1	clear extended-oam statistics	468
28.2	description	469
28.3	download	470
28.4	download remote	472
28.5	duplex.....	477
28.6	erase.....	478
28.7	extended-oam notification.....	479
28.8	fault-pass	480
28.9	flowcontrol	482
28.10	hostname.....	483
28.11	inside-loopback.....	484
28.12	interface client	485
28.13	ip address	486
28.14	ip default-gateway	488
28.15	line-speed auto	489
28.16	rate-limit.....	490
28.17	reboot	492
28.18	remote-device	493
28.19	show cable-diagnostics.....	494
28.20	show extended-oam statistics.....	494

28.21	show extended-oam status	496
28.22	show inside-loopback	497
28.23	show interface port	498
28.24	show interface port detail.....	499
28.25	show interface port statistics.....	502
28.26	show oam capability	504
28.27	show remote-device information	505
28.28	show sfp	507
28.29	show snmp trap remote	508
28.30	shutdown	509
28.31	snmp trap remote	510
28.32	snmp-server community	511
28.33	speed.....	512
28.34	switch-mode double-tagged-vlan	513
28.35	switch-mode transparent	515
28.36	system mtu	516
28.37	test cable-diagnostics	517
28.38	upload.....	518
28.39	upload remote.....	522
28.40	write	527
Chapter 29 Digital Diagnostic Commands-----		530
29.1	show interface port transceiver	530
29.2	snmp trap transceiver	533
Chapter 30 802.1x Commands-----		535
30.1	clear dot1x statistics	535
30.2	dot1x auth-control	536
30.3	dot1x reauthentication	537
30.4	dot1x timer quiet-period	538
30.5	dot1x timer reauth-period.....	540
30.6	dot1x timer server-timeout	541
30.7	dot1x timer supp-timeout	543
30.8	dot1x timer tx-period	544
30.9	show dot1x	546
30.10	show dot1x statistics.....	547
30.11	show radius-server	548
Chapter 31 IP Source Guard Commands -----		551
31.1	ip source binding	551
31.2	ip verify source	552
31.3	ip verify source trust.....	554
31.4	show ip verify source	555
Chapter 32 Auto-configuration and load commands -----		558
32.1	service config.....	558
32.2	service config filename	559
32.3	service config filename rule	561

32.4	service config overwrite	563
32.5	service config tftp-server.....	564
32.6	service config trap	565
32.7	service config version	566
32.8	show service config	568
32.9	show service config filename rule.....	569
Chapter 33 Commands of Ethernet Ring-----		573
33.1	clear ethernet ring statistics	573
33.2	ethernet ring	574
33.3	ethernet ring description	575
33.4	ethernet ring hello-time	576
33.5	ethernet ring holdtime	578
33.6	ethernet ring port	579
33.7	ethernet ring priority.....	580
33.8	ethernet ring protocol-vlan	581
33.9	ethernet ring restore-delay.....	583
33.10	show ethernet ring	584
33.11	show ethernet ring port.....	585
33.12	show ethernet ring port statistic	587
Chapter 34 Traceroute Commands -----		590
34.1	traceroute	590
34.2	traceroute concurrent number	592
Chapter 35 TACACS+ Commands-----		595
35.1	enable login	595
35.2	show tacacs-server	596
35.3	tacacs-server	597
35.4	tacacs-server key	598
35.5	user login	599
Chapter 36 SLA Commands-----		603
36.1	show sla configuration	603
36.2	show sla result.....	606
36.3	sla cfm-echo configuration.....	608
36.4	sla cfm-jitter configuration.....	610
36.5	sla icmp-echo configuration	611
36.6	sla icmp-jitter configuration	612
36.7	sla schedule.....	614
Chapter 37 Physical Interface Commands -----		617
37.1	show cable-diagnostics.....	617
37.2	test cable-diagnostics	618
Chapter 38 NTP Configuration Commands -----		621
38.1	debug ntp.....	621
38.2	ntp peer	622
38.3	ntp refclock-master	623
38.4	ntp server.....	625

38.5	show ntp associations.....	626
38.6	show ntp status.....	628
Chapter 39 Telnet Commands -----		631
39.1	show telnet-server	631
39.2	telnet.....	632
39.3	telnet-server.....	633
Chapter 40 PPPoE Commands -----		636
40.1	pppoeagent.....	636
40.2	pppoeagent circuit-id	637
40.3	pppoeagent circuit-id attach-string.....	638
40.4	pppoeagent remote-id.....	639
40.5	pppoeagent remote-id format	640
40.6	pppoeagent trust.....	641
40.7	pppoeagent vendor-specific-tag overwrite	642
40.8	show pppoeagent	644
40.9	show pppoeagent statistic	645
Chapter 41 Y.1731 Commands-----		648
41.1	clear ethernet cfm errors.....	648
41.2	clear ethernet cfm remote.....	648
41.3	clear ethernet cfm traceroute cache	649
41.4	clear performance-monitor statistics	650
41.5	ethernet cfm.....	651
41.6	ethernet cfm domain	652
41.7	ethernet cfm errors archive-hold-time	653
41.8	ethernet cfm mip level.....	654
41.9	ethernet cfm port	655
41.10	ethernet cfm remote mep age-time.....	656
41.11	ethernet cfm traceroute cache	657
41.12	ethernet cfm traceroute cache hold-time	658
41.13	ethernet cfm traceroute cache size.....	658
41.14	ping.....	659
41.15	service	660
41.16	service cc enable.....	662
41.17	service cc interval	663
41.18	service cvlan.....	664
41.19	service mep	665
41.20	service performance-monitor delay object	666
41.21	service performance-monitor delay threshold.....	667
41.22	service performance-monitor delay-variation object	669
41.23	service performance-monitor delay-variation threshold	670
41.24	service performance-monitor enable	671
41.25	service performance-monitor frame-loss-ratio threshold.....	672
41.26	service performance-monitor peer	673
41.27	service priority	675

41.28	service remote mep	675
41.29	service remote mep learning	676
41.30	service remote mep mac	677
41.31	service vlan-list	678
41.32	show ethernet cfm	680
41.33	show ethernet cfm domain.....	681
41.34	show ethernet cfm errors	681
41.35	show ethernet cfm local-mp.....	682
41.36	show ethernet cfm mep	683
41.37	show ethernet cfm performance-monitor	683
41.38	show ethernet cfm performance-monitor information.....	690
41.39	show ethernet cfm performance-monitor total frame-loss-ratio.....	691
41.40	show ethernet cfm remote	692
41.41	show ethernet cfm traceroute	693
41.42	snmp-server trap cfm.....	694
41.43	snmp-server trap performance-monitor	695
41.44	traceroute	696
Chapter 42 Commands of Storm-control -----		700
42.1	generate ssh-key	700
42.2	show ssh2 public-key authentication	701
42.3	show ssh2 session	701
42.4	ssh2 server	702
42.5	ssh2 server authentication public-key.....	703
42.6	ssh2 server authentication {password rsa-key }.....	704
42.7	ssh2 server authentication-retries.....	705
42.8	ssh2 server authentication-timeout.....	706
42.9	ssh2 server port.....	707
42.10	ssh2 server session.....	708

Chapter 1 System Commands

1.1 clear

[Function]

Clear all the information on the screen.

[Command Format]

clear

[Command Modes]

User EXEC, Privileged EXEC, Global configuration mode, VLAN configuration mode, interface/range configuration mode, router protocol configuration mode; common user, and Privileged EXEC; remote management mode; remote interface mode; user diagnostic mode.

[Command Executing Instruction]

Clear the shown information on the screen and the later information to be shown from the 1st line.

[Example]

Clear the shown information on the screen:

Raisecom> **clear**

1.2 clear device statistics

[Function]

Clear device statistics

[Command Format]

Clear device statistics {receive | send}

[Parameter]

Receive send messages

Send receive messages

[Command Modes]

Global configuration mode, privileged user

[Command Executing Instruction]

Use the command to clear switch send/receiving messages statistics

[Explanation of command execution echo]

None

[Example]

Clear CPU receiving messages statistics

Raisecom#**clear device statistics receive**

[Related commands]

Commands	Description
show device statistics	show CPU sending/receiving packets statistic

1.3 console-cli

[Function]

Enable/disable console port command control on the switch

[Command Format]

Console-cli {enable | disable}

[Parameter]

Enable enable console port command control

Disable disable console port command control

[Default]

Console port allows command control

[Command Modes]

Global configuration mode

[Command Executing Instruction]

Use the command to enable/disable console port command control. The command only allows control on telnet terminal, if console port is disabled to command control, console port input will be disabled, but output can still be kept.

[Explanation of command execution echo]

Set successfully

This command cannot be executed in the console

[Related commands]

Command		Description
telnet-server	max-session	Configure switch maximum telnet connection number
<i>max-session-num</i>		

1.4 debug

[Function]

Set debug command enable modular switch, no form of the command used to disable the switch.

[Command Format]

[no] debug (*all* / *system* / *ospf* / *rip* / *gvrp* / *igmp-snooping* / *mvr* / *cli* / *driver* / *dhcp* / *snmp* / *stp* / *lACP* / *rcmp* / *rndp* / *rtdp* / *radius* / *dot1x* / *qos* / *rmon* / *sntp* / *telnet* / *arp* / *ip* / *config*)

[Parameter]

all: debug all functions

arp: arp debug

cli: cli debug

config: system config information (can be write into system flash)

dhcp: dhcp debug

driver: driver debug

gvrp: gvrp debug

igmp-snooping: igmp-snooping debug

ip: ip debug

lACP: lacp debug

mvr: mvr debug

ospf: ospf debug

qos: qos debug

radius: radius debug

rip: rip debug

rmon: rmon debug

rdp: rdp debug

rtcp: rtcp debug

snmp: snmp debug

sntp: sntp debug

stp: stp debug

system: system debug

telnet: telnet debug

[Default]

Config modular is enabled.

System modular is enabled.

Others debug functionalities are disabled.

[Command Modes]

Privileged EXEC and Privileged EXEC

[Command Executing Instruction]

Use this command to enable one or all modulars debug functionalities.

All indicates all modulars, config modular indicates the modular that had already memorized in system flash file.

[Example]

Enable debug function of all modulars:

```
Raisecom#debug all
```

[Related commands]

Commands	Description
logging	Configure system log.

1.5 dir

[Function]

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

[Command Format]

dir

[Command Modes]

Privileged EXEC; Privileged EXEC.

[Example]

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

```
Raisecom#dir
```

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

```
size           date           time           name
-----
32    Dec-31-2000    00:00:14    durable.
32    Dec-31-2000    00:00:14    durable
```

[Related commands]

Commands	Description
write	Save the current system config

erase	Delete the designated file in falsh
download	Download system config file or start-up file
upload	Upload system config file or start-up file

1.6 download

[Function]

Use **download** to download system config file or start-up file to FPGA file to flash file system (available to RC5x1 series device only).

[Command Format]

download {*bootstrap/system-boot/startup-config / fpga*} {*tftp / ftp*}

[Parameter]

bootstrap: system bootstrap file

system-boot: boot file

startup-config: config file

fpga: FPGA file

tftp: download by tftp protocol

ftp: download by ftp protocol

[Command Modes]

Privileged EXEC and Privileged EXEC

[Command Executing Instruction]

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

[Explanation of command execution echo]

Read error.

Errors occurred when read the server.

Invalid input tftp protocol port

Errors occurred when input tftp protocol port.

Invalid input file name

Errors occurred when input a wrong file name

User name is empty.

FTP user name is empty.

User password is empty!

FTP user password is empty

[Example]

Use FTP protocol to download boot file from FTP server:

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 **tftp** to download boot file from tftp server:

Raisecom#download startup-config tftp

Please input server IP Address:1.0.0.1

Please input TFTP port(default 69):

Please input TFTP Server File Name:start_config.conf

[Related commands]

Commands	Description
Upload	Upload start-up file or boot file.

1.7 driver

[Function]

Configure the switch of device receiving some messages

[Command Format]

```
driver {receive-packet|send-packet}  
{ethertype-classify  
  {stp|garp|gmrp|gvrp|igmpsnoop|lacp|eapol|loopdetect|rcmp|rcmpdata  
  |rntp|rtcp|arp|ip|relay|others|oam|relay-stp}} {discard|syslog}  
{enable|disable} [port-list port-list]
```

[Parameter]

None

[Command Modes]

Privileged EXEC, privileged user

[Command Executing Instruction]

Use the command to control switch receiving or sending messages. If there is not-designated sort, it means all the messages. If it has been designated, the command controls only the designated sort and type messages. The supported sorts can be only Ethernet type.

Ethernet types include:

Stp (0x0042)

Garp (0x0043)

Gmrp (0x2042)

Gvrp (0x2142)

Igmpsnoop(0x0242)

Lacp(0x8809)

Eapol(0x888e)

Loop(0x0898)

Rcmp(0x0899)

Rcmpdata(0x0897)

Rndp(0x1a78)

Arp(0x0806)

Ip(0x0800)

Relay

Others

Oam

Relay-stp

[Explanation of command execution echo]

None

[Example]

Syslog all the received messages:

Raisecom#**driver receive-packet syslog enable**

[Related commands]

Commands	Description
show device statistics	Show CPU receiving/sending statistic and setting
clear device statistics	Clear CPU sending/receiving packets statistic

1.8 enable

[Function]

Enter privileged EXEC mode.

[Command Format]

enable

[Parameter]

None

[Command Modes]

Initialized mode; normal user

[Executing Command Instruction]

Use the command to enter privileged EXEC mode from initialized mode

[Explanation of command execution echo]

None

[Example]

Use **enter** to enter privileged EXEC mode

Raisecom>**enable**

Password:

[Related commands]

Command	Description
enable password	Change the password of entering privileged EXEC mode
disable	Quit form privileged EXEC mode and enter initialized mode

1.9 enable login

[Function]

Configure the password to enter privileged EXEC mode, the one saved on the switch or on Radius server.

[Command Format]

Enable login { local-user | radius-user }

[Parameter]

Local-user the password saved on the switch

Radius-user the password saved on radius server

[Command Modes]

Privileged configuration mode; privileged user

[Executing Command Instruction]

When you use local user 'enable', default password is 'raisecom'.

When you use the user on radius server, system enable user name is

'iscom_admin'. So to login, it is needed to add iscom_admin on radius server.
The maximum length of the password is 16 characters.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Configure local saved 'enable' password:

Raisecom#**enable login local-user**

[Related commands]

Command	Description
enable password	Enter the password to enter privileged EXEC mode
enable	Enter privileged EXEC mode

1.10 enable password

[Function]

Use **enable password** to set the password for access Global configuration mode.

no enable password recover password to default value.

[Command Format]

enable password

no enable password

[Default]

Default password is "raisecom" from User EXEC to Privileged EXEC.

[Command Modes]

Privileged EXEC and privileged user

[Command Executing Instruction]

Use this command to change the user password for entering Global

configuration mode.

[Explanation of command execution echo]

Set successfully

Password not same

You have no enough right to change enable password!

Password too long(must no more than 16 chars).

[Example]

Change password for entering Global configuration mode:

Raisecom#**enable password**

[Related commands]

Commands	Description
enable	Access privileged mode from normal mode.
disable	Exit privileged mode to normal mode.

1.11 erase

[Command Executing Instruction]

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

[Command Format]

erase *[FILENAME]*

[Parameter]

FILENAME: file disgnated in the file system.

[Default]

Delete the current startup_config.conf

[Command Modes]

Privileged EXEC and privileged user

[Command Executing Instruction]

Use **erase** to delete the designated file in flash file system. Delete startup-config.conf file in the system if no file is designated before executing this command.

[Explanation of command execution echo]

Erase current specified file successfully!

Command executed successfully.

Erase current specified file unsuccessfully

Command executed unsuccessfully.

[Example]

Delete 'aaa' file in flash file system:

Raisecom#**erase aaa**

[Related commands]

Commands	Description
Write	Save the current system config file.

1.12 **exit**

[Function]

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

[Command Format]

exit

[Command Modes]

User EXEC, Privileged EXEC, global configuration mode, VLAN configuration mode, interface/range configuration mode, routing protocol configuration mode, normal user, and privileged user; remote management mode; remote interface mode; user diagnostic mode.

[Command Executing Instruction]

Use **exit** in user EXEC and Privileged EXEC mode to exit login.

Use this command in interface/range configuration mode, routing protocol configuration mode to return to previous mode.

[Example]

Return to previous mode or exit login:

Raisecom#**exit**

[Related commands]

Commands	Description
quit	Return to parent mode or exit login.

1.13 help

[Function]

Use **help** to show system help information

[Command Format]

help

[Parameter]

None

[Command Modes]

Initialized mode, privileged mode, global mode, VLAN configuration mode, interface/interface range mode, routing protocol configuration mode; normal user, privileged user

[Executing Command Instruction]

Use the command to show command line help information

[Explanation of command execution echo]

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

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

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show me?').

[Example]

Raisecom#**help**

[Related commands]

None

1.14 history

[Function]

Show commands input before

[Command Format]

history

[Parameter]

None

[Default]

20 commands can be saved

[Command Modes]

Initialized mode, privileged mode, global mode, VLAN configuration mode, interface/interface range mode, routing protocol configuration mode; normal user, privileged user

[Executing Command Instruction]

Use the command to show the input commands before

[Explanation of command execution echo]

ter time-out 65535

enable

chin

enable

help

eng

[Example]

Raisecom#**history**

[Related commands]

Command	Description
terminal history	Change the commands numbers that is to be remembered

1.15 interface port

[Function]

Enter physical port mode

[Command Format]

Interface port *port_number*

[Parameter]

Port_number physical port number, range is 1-26

[Default]

By default, all the physical ports are not configured

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Use **interface port** to enter physical port configuration mode, you can configure physical port related attribution in this mode.

[Example]

Enter physical port 4 configuration mode:

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

[Related commands]

Command	Description
show interface port	Show physical interface information

1.16 interface range

[Function]

Enter physical port range configuration mode

[Command Format]

Interface range {*port_list* / **all**}

[Parameter]

Range physical port range configuration mode

Port-list physical port number, range is 1-26, use ',' and '-' for multiple port input;

All all the ports

[Default]

By default, all the physical ports are not configured

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Use **interface range** to enter physical port range configuration mode

[Example]

Enter physical port 4-10 configuration mode:

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

[Related commands]

Command	Description
show interface port	Show physical port information

1.17 list

[Function]

Use this command to show all commands in one mode.

[Command Format]

list

[Command Modes]

User EXEC, Privileged EXEC, Global configuration mode, VLAN configuration exec, interface/range configuration mode, routing protocol configuration mode; normal user and Privileged EXEC; remote management mode; remote interface mode; user diagnostic mode.

[Command Executing Instruction]

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

[Explanation of command execution echo]

chinese

clear

enable

english

exit

help

history

list

quit

terminal history <1-20>

terminal time-out <0-65535>

[Example]

Use this command to show all commands in one mode:

Raisecom>**list**

1.18 logout

[Function]

Use **logout** to exit login

[Command Format]

logout

[Parameter]

None

[Command Modes]

Privileged EXEC mode; privileged user

[Executing Command Instruction]

When you finished configuring the system, use the command to exit login state, other user on this control panel needs re-login to configure the switch.

[Explanation of command execution echo]

None

[Example]

Raisecom#**logout**

[Related commands]

None

1.19 password

[Function]

Use **password** to change the login password for current user.

[Command Format]

password

[Default]

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

[Command Modes]

Privileged EXEC, privileged user.

[Command Executing Instruction]

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

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully!

Password not same!

Radius user can't change password!

Password is too long (must less than 16 chars)

[Example]

Change the login password for current user:

Raisecom#**password**

Please input password:xxxx

Please input again:xxxx

[Related commands]

Commands	Description
user privilege	Set user popedom.

1.20 ping

[Function]

Start ping test, press CTRL + C to stop ping

[Command Format]

ping *A.B.C.D* [count *count*] [size *size*] [waittime *waittime*]

[Parameter]

A.B.C.D the destination IP address

Count ping packets number, range is 1-65535

Size ping packet byte number, range is 0-4096(ICMP head is not included)

Waittime ping packet waiting time, range is 1-60s

[Default]

By default, ping packet number is 1, ping packet size is 0 (IP head and ICMP head information is not included), timeout threshold is 3s.

[Command Modes]

Privileged user (priority level 15)

[Command Executing Instruction]

Only user with priority 15 can use the command.

[Explanation of command execution echo]

Type CTRL+C to abort.

Sending 1, <>-byte ICMP Echos to A.B.C.D , timeout is <> seconds:

!

A.B.C.D is alive

Type CTRL+C to abort.

Sending <>, <>-byte ICMP Echos to A.B.C.D , timeout is<> seconds:

!!!!!!!!!!!!!!

---- PING Statistics----

<> packets transmitted,

<> packets received, Success rate is <> percent(<>/<>)

round-trip (ms) min/avg/max = <>/<>/<>

Type CTRL+C to abort.

Sending <>, <>-byte ICMP Echos to A.B.C.D , timeout is <> seconds:

UUUUU

no answer from A.B.C.D

Ping unsuccessfully£, The number of concurrent have reached max value.

IP Address can not be in class D or class E!

[Example]

Ping IP address is 20.0.0.2 (let's suppose the address can pass ping test), other parameters are default value:

```
Raisecom#ping 20.0.0.2
Type CTRL+C to abort.
Sending 1, 8-byte ICMP Echos to 20.0.0.2 , timeout is 3 seconds:
!
20.0.0.2 is alive
```

Ping IP address is 20.0.0.2 (let's suppose the address can pass ping test), packets number is 10, timeout threshold is 5s, packet size is 20 bytes:

```
Raisecom# ping 20.0.0.2 count 10 size 20 waittime 5
Type CTRL+C to abort.
Sending 10, 28-byte ICMP Echos to 20.0.0.2 , timeout is 5 seconds:
!!!!!!!!!!
---- PING Statistics----
10 packets transmitted,
10 packets received, Success rate is 100 percent(10/10)
round-trip (ms)   min/avg/max = 0/1/16
```

ping IP address is 30.0.0.2 (let's suppose the address can not pass ping test), other parameters are as default:

```
Raisecom#ping 30.0.0.2
Type CTRL+C to abort.
Sending 1, 8-byte ICMP Echos to 30.0.0.2 , timeout is 3 seconds:
U
no answer from 30.0.0.2
```

[Related commands]

None

1.21 quit

[Function]

Use the command to return to previous mode or logout.

[Command Format]

quit

[Command Modes]

User EXEC, Privileged EXEC, Global configuration mode, vlan configuration mode, interface/range configuration mode, router protocol configuration mode; normal user, privileged user ; remote management mode; remote interface mode; user diagnostic mode.

[Command Executing Instruction]

Use the command in privileged EXEC and user EXEC to quit login state.

Use the command in vlan configuration mode, interface/range configuration mode, router protocol configuration mode to return to previous mode.

[Example]

Return to previous mode or quit login state:

Raisecom>**quit**

[Related commands]

Commands	Description
exit	Return to previous mode or quit login state.

1.22 radius accounting-server

[Function]

Configure Radius server IP address and UDP port ID.

[Command Format]

Radius accounting-server *A.B.C.D* [*acct-port*]

[Parameter]

A.B.C.D Radius accounting server IP address;

Acct-port Radius accounting server UDP port ID

[Default]

Default IP address is 0.0.0.0, port ID is 1813

[Command Modes]

Privileged EXEC mode, privileged user

[Command Executing Instruction]

Use the command to configure Radius server IP address and UDP port ID

[Explanation of command execution echo]

Set successfully

Could not config radius accounting info when there is active radius user login

[Example]

Configure Radius accounting server IP address to 20.20.20.20, port ID is still the same

Raisecom#**radius accounting-server 20.20.20.20**

Configure Radius accounting server IP address to 20.20.20.20, port ID to 6000

Raisecom#**radius accounting-server 20.20.20.20 6000**

[Related commands]

Command	Description
show radius-server	Show Radius accounting related configuration

1.23 radius accounting-server key

[Function]

Configure the shared key to communicate with Radius accounting server

[Command Format]

Radius accounting-server key WORD

[Default]

By default the value is empty

[Command Modes]

Privileged EXEC mode, privileged user

[Command Executing Instruction]

Use the command to configure Radius server IP address and UDP port ID

[Explanation of command execution echo]

Set successfully

Could not config radius accounting info when there is active radius user login

[Example]

Configure the shared key to hello

Raisecom#**radius accounting-server key** hello

[Related commands]

Command	Description
show radius-server	Show Radius accounting related configuration

1.24 reboot

[Function]

Use **reboot** to reboot switch.

[Command Format]

reboot

[Command Modes]

Privileged EXEC; privileged user

[Command Executing Instruction]

'Yes' should be entered to confirm the operation when the command is used to reboot switch.

[Example]

Raisecom#**reboot**

Please input 'yes' to confirm:yes

Rebooting ...

1.25 show device statistics

[Function]

Show device sending/receiving messages statistics

[Command Format]

Show driver statistics {receive | send} [port *portnum*] [detail]

[Parameter]

Receive send messages

Send receive messages

Portnum port number

Detail show all the receiving/sending messages statistics

[Command Modes]

Privileged EXEC, privileged user

[Command Executing Instruction]

Use the command to show switch sending/receiving messages statistics and control information. Only Ethernet is the supported sort. If there is no designated port, it will be shown switch receiving/sending messages statistics; and if there is, it will be shown the statistics of the port. Without the parameter detail, the types that has 0 packets will not be shown, while 'detail' is used, all the types statistics will be shown.

[Explanation of command execution echo]

Type	Action	Total
------	--------	-------

[Example]

Show switch receiving packets sorts statistics

Raisecom#**show device statistics receive**

Type	Action	Total

SlowProtocol	----	5
Loopdetect	----	18
Rndp	----	1
Rtdp	----	4
Arp	----	1
IP	----	3

show switch port 9 sending messages Ethernet sorts statistics

Raisecom#**show device statistics send port 9 detail**

Type	Action	Total

STP	----	0
Garp	----	0
Gmrp	----	0
Gvrp	----	0
IgmpSnoop	----	0
SlowProtocol	----	541
EAPOL	----	
Loopdetect	----	0
Rcmp control	----	0
Rcmp data	----	0
Rndp	----	37
Rtdp	----	0
Arp	----	0

IP	----	0
Relay	-----	0
others	----	0
oam	-----	0
relay-stp	-----	0

[Related commands]

Commands	Description
<code>clear device statistics</code>	Clear CPU sending/receiving packets statistic

1.26 show radius-server

[Function]

Show Radius related configuration

[Command Format]

Show radius-server

[Parameter]

None

[Default]

None

[Command Modes]

Privileged EXEC mode, privileged user

[Command Executing Instruction]

Use the command to show Radius authentication, accounting related configuration

[Explanation of command execution echo]

Authentication server IP: *A.B.C.D* port: ***
Authentication server key: xxxxxxxx
Accounting server IP: *A.B.C.D* port: ***
Accounting server key: xxxxxxxx

Accounting login: *Enable*
Accounting fail policy: online

update interval: *12* minutes

[Related commands]

None

1.27 `show running-config`

[Function]

Use **show running-config** to show the configuration information of current system.

[Command Format]

show running-config

[Command Modes]

Privileged EXEC, privileged user

[Command Executing Instruction]

Show the configuration information of current system. '!' stands for explanation. Use command **write** to write the configuration information to flash memory.

[Example]

Show the configuration information of current system:

Raisecom# **show running-config**

System current configuration:

!command in view_mode

terminal time-out 65535

!

!command in enable_mode

!

!command in vlan configuration mode

!

!command in port_mode

!

!command in aggregator mode

!

!command in ip interface mode

!

!command in rip_mode

!

!command in ospf_mode

!

!command in config_mode

!

[Related commands]

Commands	Description
show startup-config	Show system startup information
download	Download system configuration file or startup file.
upload	Upload system configuration file or startup file.

1.28 show startup-config

[Function]

Use **show startup-config** command to show startup configuration information that is saved in the system.

[Command Format]

show startup-config

[Command Modes]

Privileged EXEC; privileged user.

[Command Executing Instruction]

Use this command to show startup configuration information that is saved in flash system file; use **write** command to save information for the device or to refresh information by download, or use **erase** command to delete information. Also can save information by uploading.

[Example]

Show startup configuration information that is saved in system:

Raisecom#**show startup-config**

```
!command in view_mode

!command in enable_mode

!command in vlan configuration mode

!command in port_mode

!command in aggregator mode

!command in ip interface mode

!command in rip_mode

!command in ospf_mode

!command in config_mode

snmp-server host 20.0.0.1 v2 public udp-port 163snmp
```

snmp-server host 20.0.0.2 v1 public

!

!NEVER change the NOTATION

!end

[Related commands]

Commands	Description
show startup-config	Show system startup config information.
download	Download system configuration file or startup file.
upload	Upload system config file or start file.
write	Save current system configuration.
erase	Delete designated file in the system.

1.29 show user

[Function]

Use **show user** to show the user information stored in system.

[Command Format]

show user

[Command Modes]

Privileged EXEC; privileged user

[Command Executing Instruction]

Use the command to inspect how many users can login the system. The information of users is stored in usertable.conf. Users can use **erase** to delete the file to restore default user status.

[Example]

Show the user information stored in system:

Raisecom#**show user**

User name priority Server

<i>Raisecom</i>	<i>15</i>	<i>local</i>
<i>Abc</i>	<i>15</i>	<i>10.0.0.1</i>

[Related commands]

Commands	Description
user	Set up the user information.
user privilege	Set the privilege of user.

1. 30 `show version`

[Function]

Use **show version** to show system version.

[Command Modes]

privileged configuration mode, privileged user.

[Command Executing Instruction]

Use the command to show the software and system hardware version.

[Explanation of command execution echo]

The information be shown after Bootstrap Version contains two cases:

1. UNKNOWN indicates Bootstrap main version is lower than 2.0.8;
2. Show version information in form of Bootstrap_2.0.8.ISCOM2826E.1.20060802 indicates Bootstrap version is higher than 2.0.8.

[Example]

Show system version information:

Raisecom#**show version**

RaiseCom Operating System Software

Copyright(c) 2003-2005 by Raisecom Science & Technology CO., LTD.

Product name: ISCOM2826E

*ROS Version 3.1.647.ISCOM2826E.28.20060803.(Compiled Aug 3 2006,
09:41:29)*

Bootstrap Version Bootstrap_2.0.8.ISCOM2826E.1.20060802

Hardware ISCOM2826. Version Rev.A

System MacAddress is :000e.5e11.4d0b

ISCOM2826 with

64M bytes DRAM

8 M bytes Flash Memory

Switch uptime is 0 days, 0 hours, 36 minutes

1.31 terminal history

[Function]

Change the history commands number that are to be remembered

[Command Format]

Terminal history *command_count*

[Parameter]

History terminal history command configuration information

Command_count history commands number input from terminal, range is
1-20

[Default]

20 commands can be saved

[Command Modes]

Initialized mode; normal user, privileged user

[Executing Command Instruction]

Use the command to change terminal input history commands number, so that history commands can be shown more clearly.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Configure local saved 'enable' password:

Raisecom#**terminal history 10**

[Related commands]

Command	Description
history	Show the history commands of the terminal

1.32 terminal time-out

[Function]

Use the command to change time-out length when logout

[Command Format]

Terminal time-out *timeout*

[Parameter]

Time-out the configuration when the terminal quit because of timeout

Timeout timeout length when terminal is squared, range is 0-65535

[Default]

600s

[Command Modes]

Initialized mode; normal user, privileged user

[Executing Command Instruction]

Use the command to change time-out length when logout

[Explanation of command execution echo]

Set successfully

[Example]

Configure quit time to 1000s:

Raisecom#**terminal time-out 1000**

[Related commands]

Command	Description
show terminal	Show terminal information

1.33 user

[Function]

Add user and set the password of the user.

Use the command of **no user** to delete user.

[Command Format]

user *USERNAME* **password** {*no-encryption* / *md5*} *PASSWORD*

no user *USERNAME*

[Parameter]

USERNAME: username

password: password

md5: password with MD5 encryption

PASSWORD: password information.

[Default]

The default priority for adding a user is 15.

Use **user privilege** command to change the priority of user.

The user's default enable password is 123 added by the command, **enable password** is used to change password.

[Command Modes]

Privileged EXEC, privileged user (Priority 15)

[Command Executing Instruction]

There is at least one user whose priority is 15 in system user database.

Only users whose priority is 15 can use the command.

[Explanation of command execution echo]

You have no enough right to change user information!

This echo shows when privileged user whose priority is not 15 tries to create a new user. Only 15-priority users can perform this command.

Set successfully!

Set unsuccessfully!

[Example]

Add a user whose ID is abc and password is 123:

Raisecom# **user name** *abc* **password** *123*

Delete a user whose ID is abc:

Raisecom# **no user** *abc*

[Related commands]

Commands	Description
hostname	Change hostname specified by special user.
user name <i>USERNAME</i> privilege	Change the priority of user
enable password	Change the password of user enable
password	Change the password of current user

1.34 user login

[Function]

Set the login mode for authentication.

[Command Format]

user login { *local-user* / *radius-user* / *local-radius* / *radius-local* }

[Parameter]

local-user: Use local configuration file to authenticate user.

radius-user: User RADIUS server to authenticate user.

local-radius: use local configuration file to check login user, do not need to login RADIUS server to get authentication once more.

radius-local: should pass RADIUS server authentication, do not need to login local configuration file to get the authentication once more.

[Default]

Local configuration file is used by default.

[Command Modes]

Privileged EXEC, privileged user (priority 15)

[Command Executing Instruction]

Based on RADIUS authentication, user is “ENABLE” and password is 123, hostname is Raisecom, tip is Enter keyboard by default, default priority is 15.

[Explanation of command execution echo]

Set User Login Method unsuccessfully.

Set User Login Method successfully.

[Example]

Set local-user as the authentication type of login:

Raisecom# **user login local-user**

[Related commands]

Commands	Description
radius host	Set RADIUS authentication IP server address.
radius-key	Set the shared key for RADIUS authentication server and client PC.

1.35 user name privilege

[Function]

Use **user name privilege** command to set the user priority for particular user.

[Command Format]

user name USERNAME privilege <1-15>

[Parameter]

USERNAME: user name;

<1-15>: user privilege.

[Default]

Default user priority is 15.

[Command Modes]

Privileged configure mode; privileged user (Only the user with priority 15 can apply this command).

[Command Executing Instruction]

Use this command when it's needed to limit the user priority for particular user, if the user priority is less than 5, it will change to normal user. Users are disabled to change the priority of the users who have already login.

[Explanation of command execution echo]

Set successfully.

can not change user privilege !

You have no enough right to change user information !

[Example]

Set the user priority of user abc to 4:

Raisecom# **user name abc privilege 4**

[Related commands]

Commands	Description
user	Add user and set user password.
show user	Show user information.

1.36 write

[Function]

The command is used to save configuration information of current system.

[Command Format]

write [*schedule-list list-no*]

[Parameter]

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

list-no: schedule list range is<0-99>.

[Command Modes]

Privileged EXEC, privileged user

[Command Executing Instruction]

Use the command to save configuration information of current system, then the saved system command will be executed automatically after reset the system, a new configuration of the switch is not needed.

[Explanation of command execution echo]

Save current configuration successfully!

Save current configuration Fail!

[Example]

Current configuration information saved by system:

Raisecom#**write**

[Related commands]

Commands	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



Chapter 2 Mirror Commands

2.1 mirror

[Function]

Enable/disable the mirror function.

[Command Format]

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

[Parameter]

enable: enable mirroring function

disable: disable mirroring function

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

list-no: schedule list number range from <0-99>

[Default]

disable

[Command Modes]

Global configuration mode, Privileged user (priority 15)

[Command Executing Instruction]

Only users whose priority is 15 can perform the command.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully!

[Example]

Enable the mirroring function:

Raisecom(config)# **mirror** *enable*

Disable the mirroring function:

Raisecom(config)# **mirror** *disable*

[Related commands]

Commands	Description
show mirror	Display the mirror function status.

2.2 mirror block-non-mirror

[Function]

Enable or disable block non-mirror flow control function.

[Command Format]

mirror block-non-mirror {*enable* | *disable*}

[Parameter]

block-non-mirror: block the traffic from non-mirror port to the monitor port.

enable: active the function.

disable: stop the function.

[Default]

Block-non-mirror port traffic function disable.

[Command Modes]

Global configuration mode; privileged user (priority 15)

[Command Executing Instruction]

Only users whose priority is 15 can perform the command.

[Explanation of command execution echo]

Set successfully !

Set unsuccessfully !

[Example]

Enable the mirror block-non-mirror function:

```
Raisecom (config)# mirror block-non-mirror enable
```

Disable the mirror block-non-mirror function:

```
Raisecom (config)# mirror block-non-mirror disable
```

[Related commands]

Commands	Description
show mirror	Show the setting of mirror function.

2.3 mirror divider

[Function]

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

[Command Format]

```
mirror {ingress / egress} divider <1-1023>
```

```
no mirror {ingress / egress} divider
```

[Parameter]

ingress: ingress mirror divider;

egress: egress mirror divider;

divider: copy the reciprocal rate packet of the number of divider ,from source port to the monitor port

1 —1023: number of mirror divider

[Default]

The dividers for ingress mirror and egress divider are 1

[Command Modes]

Global configuration mode, Privileged user (priority 15)

[Command Executing Instruction]

Only users whose priority is 15 can perform the command.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully !

[Example]

Set the ingress divider to 30:

```
Raisecom (config)# mirror ingress divider 30
```

Set the egress divider to 50:

```
Raisecom (config)# mirror egress divider 50
```

Delete the mirror divider:

```
Raisecom (config)# no mirror ingress divider
```

```
Raisecom (config)# no mirror egress divider
```

[Related commands]

Commands	Description
show mirror	Show the setting of mirror function.

2.4 mirror filter

[Function]

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

[Command Format]

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

```
no mirror {ingress | egress} filter
```

[Parameter]

ingress: ingress mirror filtering rule;

egress: egress mirror filtering rule;

destination: target MAC address;

source: source MAC address;

HHHH.HHHH.HHHH: MAC address

[Default]

All the packets on the mirror ports are mirrored

[Command Modes]

Global configuration mode; privileged user (priority 15)

[Command Executing Instruction]

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

[Explanation of command execution echo]

Set successfully

Set unsuccessfully !

[Example]

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

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

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

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

Recover the filter rule to the default setting:

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

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

[Related commands]

Commands	Description
----------	-------------

show mirror	Show the settings of mirror function.
--------------------	---------------------------------------

2.5 mirror monitor-port

[Function]

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

[Command Format]

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]

By default condition, set port 1 as monitor port.

[Command Modes]

Global configuration mode, Privileged user

[Command Executing Instruction]

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

[Explanation of command execution echo]

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

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

Set successfully !

[Example]

Set port 5 is monitor port of mirror function:

Raisecom(config)# **mirror monitor-port 5**

Delete mirror port:

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

[Related commands]

Commands	Description
no mirror all	Delete all the mirror setting.
show mirror	Show all the mirror setting.

2.6 mirror source-port-list

[Function]

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

[Command Format]

mirror *source-port-list both port-list*

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

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

no mirror *source-port-list*

no mirror *all*

[Parameter]

source-port-list: source mirror port;

port-list: the number of physical port, range from 1 to 26, use “,” and “-” for multi port input;

ingress: mirror ingress packets;

egress: mirror egress packets;

both: mirror both ingress and mirror egress packets;

all: all the mirror configuration.

[Default]

disable

[Command Modes]

Global configuration mode, Privileged user

[Command Executing Instruction]

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

[Explanation of command execution echo]

The port list is wrong!

Error occurred when enter multi ports using “-“ and “,”.

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

The port X is already a monitoring port.

Set successfully !

[Example]

Set physical port of 1 to 5 is mirror port and mirror rule is ingress:

Raisecom(config)# **mirror source-port-list ingress 1-5**

Delete mirror source port:

Raisecom(config)# **no mirror source-port-list**

Delete all mirror setting:

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

[Related commands]

Commands	Description
show mirror	Show all the mirror information.

2.7 mirror source-port-list ingress egress

[Function]

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

[Command Format]

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

[Parameter]

source-port-list: source mirror port;

port-list: physical port number, range from 1-26, use ',' and '-' to input multi ports ;

ingress: ingress mirror divider;

egress: egress mirror divider;

both: mirror both ingress and mirror egress packets;

all: all the mirror configuration

[Default]

No source mirror port is set by default.

[Command Modes]

Global configuration mode, Privileged user

[Command Executing Instruction]

Only users whose priority is 15 can perform the command.

[Explanation of command execution echo]

The port list is wrong!

Error occurred when input multi ports using “-“ and “,”.

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

The port X is already a monitoring port.

Set successfully !

[Example]

Set physical port of 1 to 5 is mirror port and mirror rule is ingress:

Raisecom(config)# **mirror source-port-list ingress 1-5**

Delete source mirror of port:

Raisecom(config)# **no mirror source-port-list**

Delete all mirror setting:

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

[Related commands]

Commands	Description
show mirror	Show the setting of mirror function.

2.8 show mirror

[Function]

Show the mirror situation for all the settings.

[Command Format]

show mirror

[Parameter]

mirror: mirror function

[Command Modes]

Privileged EXEC; privileged user

[Explanation of command execution echo]

Mirror: Disable

Monitor port: 1

-----the ingress mirror rule-----

Mirrored ports: 3,4

-----the egress mirror rule-----

Mirrored ports: 3,4

[Example]

Show the mirror rule:

Raisecom# **show mirror**

[Related commands]

Commands	Description
mirror <i>{enable / disable}</i>	Mirror function enable/disable.
mirror monitor-port	Set the mirror monitor port.
mirror source-port-list	Set the source mirror port.



Chapter 3 Bandwidth Management

Commands

3.1 clear double-tagging-vlan statistics

[Function]

Clear VLAN rate-limit packets loss information

[Command Format]

clear double-tagging-vlan statistics **outer** {**any** | *spvlanid*} **inner** {**any** | *cvlanid*}

[Parameter]

Outer outer VLAN

Spvlanid VLANID <1-4094>;

Cvlanid VLANID <1-4094>;

Any any VLAN

Inner inner VLAN

[Default]

None

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Use the command to clear designated outer VLAN, inner VLAN double TAG rate-limit packets loss statistics

[Explanation of command execution echo]

Set successfully

This is the echo of successful configuration;

Set unsuccessfully

Configuration failure echo

[Example]

Clear inner vlan5, outer vlan8 rate-limit packets loss statistics

Raisecom(config)# **clear double-tagging-vlan statistics outer 8 inner 5**

[Related commands]

Commands	Description
Show rate-limit vlan	Show all VLAN rate-limit state
Rate-limit double-tagging-vlan	Configure double TAG VLAN rate-limit packets loss

3.2 clear rate-limit statistics vlan

[Function]

Clear VLAN rate-limit packets loss statistics

[Command Format]

clear rate-limit statistics vlan [vlanid]

[Parameter]

vlanid VLANID <1-4094>

[Default]

None

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Use the command to clear all the single TAG VLAN rate-limit packets loss statistics, or clear only that stat. of the designated VLAN

[Explanation of command execution echo]

Set successfully

This is the echo of successful configuration;

Set unsuccessfully

Configuration failure echo

[Example]

Clear all VLAN rate-limit packets loss statistics:

Raisecom(config)# **clear rate-limit statistics vlan**

[Related commands]

Commands	Description
Show rate-limit vlan	Show all VLAN rate-limit state
Rate-limit vlan	Configure double TAG VLAN rate-limit packets loss

3.3 rate-limit double-tagging-vlan

[Function]

Set bandwidth for QinQ VLAN, command in **no** form for cancel operation.

[Command Format]

rate-limit double-tagging-vlan outer {<1-4094>|any} inner {<1-4094>|any} rate burst [schedule-list list-no]

no rate-limit double-tagging-vlan outer {<1-4094>|any} inner {<1-4094>|any} [schedule-list list-no]

[Parameter]

outer: outer VLAN;

<1-4094>: VLANID;

any: any VLAN

inner: inter VLAN

rate: rate (from 1 to 1048576kbps)

burst: burst rate(from 1 to 512KBps)

schedule-list: set the start time, over time, period interval of schedule

list-no: list range 0-99.

[Default]

No QinQ VLAN bandwidth limit

[Command Modes]

Global configuration mode; Privileged user

[Command Executing Instruction]

The rate should near the n^{th} power of 2 (n should be whole number).

[Explanation of command execution echo]

Set successfully

Set unsuccessfully!

[Example]

Set outer VLAN 4 bandwidth limit to be 4Mbps, burst value to be 64Kbps:

```
Raisecom(config)#rate-limit double-tagging-vlan outer 4 inner any  
4196 64
```

Set outer VLAN 8 inner 6 bandwidth limit to be 4Mbps, burst value to be 64Kbps:

```
Raisecom(config)#rate-limit double-tagging-vlan outer 8 inner 6 4196  
64
```

Delete outer VLAN 4 bandwidth limit:

```
Raisecom(config)#no rate-limit double-tagging-vlan outer 4 inner any
```

[Related commands]

Commands	Description
rate-limit vlan	Set VLAN bandwidth limit.
show rate-limit vlan	Show rate limit of all VLAN.

3.4 rate-limit egress

[Function]

Configure the bandwidth limit of local device port, use **no** to delete it

[Command Format]

rate-limit port-list *port-list* **egress** *rate* [*egress-burst*] [**schedule-list** *list-no*]

rate-limit port-list *port-list* **both** *rate* [**schedule-list** *list-no*]

rate-limit line *line-id* **egress** *rate*

rate-limit client *client-id* **egress** *rate*

rate-limit line *line-id* [**client** *client-id*] **egress** *rate*

rate-limit client *client-id* **both** *rate*

rate-limit line { *line-id* } [**client** *client-id*] **both** *rate*

no rate-limit line { *line-id* } [**client** *client-id*] **both**

no rate-limit client *client-id* **both**

no rate-limit line *line-id* **egress**

no rate-limit client *client-id* **egress**

no rate-limit line *line-id* [**client** *client-id*] **egress** *rate*

no rate-limit port-list *port-list* {*ingress* | *egress* | *both*}

[Parameter]

Port-list physical port;

Port-list physical port number, range is 1-26, use ‘,’ and ‘-’ for multiple ports input;

Egress port direction is egress;

Rate configure rate value, unit is kbps, range is 1-1048576;

Burst configure burst value, unit is kbps, range is 1-512;

Schedule-list configure the start time, ending time and interval of schedule task;

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

Line-id line port number;

Client-id client port number;

[Default]

By default, physical port rate-limit is not configured

[Command Modes]

Global configuration mode; privileged user

[Explanation of command execution echo]

Set successfully

Actual egress rate of FE (or GE) port: XXX Kbps

Actual egress burst of FE (or GE) port: XXX Kbps

This is the echo of successful configuration;

Set unsuccessfully

When you configure the device sub-card, and the sub-card does not exist;

[Example]

Configure the device user port 1 client bandwidth to 5Mbps:

Raisecom(config)#rate-limit client 1 egress 5000

Delete the device user port 1 client bandwidth configuration

Raisecom(config)#no rate-limit client 1 egress

Configure port 5 client rate to 10Mbps, burst 64Kbps

Raisecom(config)#rate-limit port-list 5 egress 10240 64

Delete port 5 rate-limit

Raisecom(config)#no rate-limit port-list 5 egress

[Related commands]

Commands	Description
Show rate-limit	Show port rate-limit configuration

3.5 rate-limit flow-control

[Function]

Enable flow control when rate is too high.

[Command Format]

rate-limit flow-control

[Default]

Drop mode

[Command Modes]

Port configuration mode

[Command Executing Instruction]

This command is to set mode when port message rate is over threshold under port configuration mode.

[Explanation of command execution echo]

Set successfully

Set Unsuccessfully

[Example]

Enable flow control mode under port 2 configuration mode:

Raisecom(config-port)# **rate-limit flow-control**

[Related commands]

Commands	Description
show interface port <i>port_id</i> rate-limit	Show current configuration of assigned port ingress rate.
no rate-limit flow-control	Disable flow control mode when rate over threshold and change to drop mode.

3.6 rate-limit ingress

[Function]

Configure the bandwidth limit of local device port, use **no** to delete it

[Command Format]

rate-limit port-list *port-list* **ingress** *rate* [*ingress-burst*] [**schedule-list** *list-no*]

rate-limit port-list *port-list* **both** *rate* [**schedule-list** *list-no*]

rate-limit line *line-id* **ingress** *rate*

rate-limit client *client-id* **ingress** *rate*

rate-limit line *line-id* [**client** *client-id*] **ingress** *rate*

rate-limit client *client-id* **both** *rate*
rate-limit line { *line-id* } [**client** *client-id*] **both** *rate*
no rate-limit line { *line-id* } [**client** *client-id*] **both**
no rate-limit client *client-id* **both**
no rate-limit line *line-id* **ingress**
no rate-limit client *client-id* **ingress**
no rate-limit line *line-id* [**client** *client-id*] **ingress** *rate*
no rate-limit port-list *port-list* {ingress | egress | both}

[Parameter]

Port-list physical port;

Port-list physical port number, range is 1-26, use ',' and '-' for multiple ports input;

Ingress port direction is egress;

Rate configure rate value, unit is kbps, range is 1-1048576;

Burst configure burst value, unit is kbps, range is 1-512;

Schedule-list configure the start time, ending time and interval of schedule task;

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

Line-id line port number;

Client-id client port number;

[Default]

By default, physical port rate-limit is not configured

[Command Modes]

Global configuration mode; privileged user

[Explanation of command execution echo]

Set successfully

Actual egress rate of FE (or GE) port: XXX Kbps

Actual egress burst of FE (or GE) port: XXX Kbps

This is the echo of successful configuration;

Set unsuccessfully

When you configure the device sub-card, and the sub-card does not exist;

[Example]

Configure the device user port 1 client bandwidth to 5Mbps:

Raisecom(config)#rate-limit client 1 ingress 5000

Delete the device user port 1 client bandwidth configuration

Raisecom(config)#no rate-limit client 1 ingress

Configure port 5 client rate to 10Mbps, burst 64Kbps

Raisecom(config)#rate-limit port-list 5 ingress 10240 64

Delete port 5 rate-limit

Raisecom(config)#no rate-limit port-list 5 ingress

[Related commands]

Commands	Description
Show rate-limit	Show port rate-limit configuration

3.7 rate-limit vlan

[Function]

Set VLAN bandwidth limit, command in **no** form for cancel operation.

[Command Format]

rate-limit vlan <1-4094> *rate burst [schedule-list list-no]*

no rate-limit vlan <1-4094> [*schedule-list list-no*]

[Parameter]

VLAN: VLAN;

<1-4094>: VLANID;

rate: rate (from 1 to 1048576kbps)

burst: burst rate(from 1 to 512KBps)

schedule-list: set the start time, over time, period interval of schedule

list-no: list range 0-99

[Default]

No VLAN bandwidth limit

[Command Modes]

Privileged EXEC; Global configuration mode

[Command Executing Instruction]

The rate should near the n^{th} power of 2 (n should be whole number).

[Explanation of command execution echo]

Set successfully

Set unsuccessfully!

[Example]

Set VLAN 5 bandwidth limit to be 5Mbps, burst value to be 32Kbps:

Raisecom(config)#**rate-limit vlan 5 5120 32**

Delete VLAN 5 bandwidth limit:

Raisecom(config)#**no rate-limit vlan 5**

[Related commands]

Commands	Description
rate-limit double-tagging-vlan	Set bandwidth limit of QinQ VLAN.
show rate-limit vlan	Show all VLAN bandwidth limit setting.

3.8 show rate-limit

[Function]

Show bandwidth limit setting.

[Command Format]

show rate-limit port-list [{*port-list*}]

[Parameter]

rate-limit: rate limit;

port-list: physical port number;

port-list: physical port number, range: 1-26; use “,” and “-” to input multi ports.

[Command Modes]

Privileged EXEC, Privileged user

[Explanation of command execution echo]

I-Rate: Ingress Rate

I-Burst: Ingress Burst

E-Rate: Egress Rate

E-Burst: Egress Burst

Port I-Rate(Kbps) I-Burst(kBps) E-Rate(Kbps) E-Burst(kBps)

[Example]

Show bandwidth limit information:

Raisecom# **show rate-limit port-list**

[Related commands]

Commands	Description
rate-limit port-list	Show bandwidth limit of the port.
no rate-limit port-list	Delete bandwidth limit of the port.

3.9 show rate-limit vlan

[Function]

Show configuration of VLAN bandwidth.

[Command Format]

show rate-limit vlan

[Parameter]

rate-limit: bandwidth limit;

vlan: VLAN.

[Command Modes]

Privileged EXEC, privileged user

[Explanation of command execution echo]

CVLAN: Customer VLAN(inner VLAN)

SPVLAN:Service provider VLAN(outer VLAN)

Type	CVLAN	SPVLAN	Rate(Kbps)
------	-------	--------	------------

Burst(KBps)			
-------------	--	--	--

[Example]

Show rate limit information:

Raisecom#**show rate-limit vlan**

[Related commands]

Commands	Description
rate-limit vlan	Set bandwidth limit for VLAN.
rate-limit double-tagging-vlan	Set bandwidth limit for QinQ VLAN.

Chapter 4 Commands of MAC Address Management

4.1 clear mac-address-table

[Function]

Clear the specified MAC address in MAC address table.

[Command Format]

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

[Parameter]

all: Clear dynamic/static MAC address.

dynamic: Clear dynamic MAC address only.

static: Clear dynamic static MAC address only.

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

list-no: specify the certain schedule list <0-99>.

[Command Modes]

Global configuration mode

[Example]

Delete all dynamic MAC addresses:

Raisecom(config)#**clear mac-address-table** *dynamic*

[Related commands]

Commands	Description
mac-address-table static	Configure static MAC-address .

4.2 mac-address-table aging-time

[Function]

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

[Command Format]

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

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

[Parameter]

aging-time: aging time;

0: MAC address aging disable;

time: aging time, unit is second, range from 3-765;

schedule-list: set the starting time, ending time, time interval of periodical task.

list-no: range from <0-99>.

[Default]

Aging time is 300 second.

[Command Modes]

Global configuration mode

[Explanation of command execution echo]

Set successfully

Set unsuccessfully!

[Example]

Set aging time of MAC address is 500 seconds:

Raisecom(config)# **mac-address-table aging-time 500**

Set MAC address aging disable:

Raisecom(config)# **mac-address-table aging-time 0**

Recover default value of MAC address aging time:

Raisecom(config)# **no mac-address-table** *aging-time*

[Related commands]

Commands	Description
show mac aging-time	Show MAC address aging time.

4.3 mac-address-table learning

[Function]

Enable and disable MAC address learning function of physical port.

[Command Format]

mac-address-table learning (*enable/disable*) **line** *line-list* [**client** *client-list*]

mac-address-table learning (*enable / disable*) **client** *client-list*

[Parameter]

enable: enable learning function;

disable: disable learning function;

line-list: line port list;

client-list: client port list;

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

list-no: specify the certain schedule list <0-99>.

[Default]

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

[Command Modes]

Global configuration mode

[Explanation of command execution echo]

Set successfully

Set port XX unsuccessfully!

The input port list is wrong!

[Example]

Enable MAC address learning function of line port 5, 10:

Raisecom(config)#**mac-address-table learning disable line 5, 10**

[Related commands]

Commands	Description
show interface port	Show one or all ports state.

4.4 mac-address-table static multicast

[Function]

Use the command to add a layer-2 port as multicast group member, **no** command can cancel the configuration.

[Command Format]

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

[Parameter]

mac-address: specify static group MAC address, in format of 0100.5eHH.HHHH;

vlan: VLAN

vlanid: VLAN ID (optional), range from 1 to 4094;

port: physical port;

portlist: specify static router port number being configured, range: 1~26.

[Command Modes]

Global configuration mode; privileged user

[Command Executing Instruction]

Use the command to add a layer-2 port as multicast group member, **no** command can cancel the configuration.

[Explanation of command execution echo]

VLAN X does not exist or not active.

Port is not in vlan.

IGMP snooping on VLAN is disable!

Join port in a assigned group on assigned VLAN successfully

Join port in a assigned group on assigned VLAN unsuccessfully

Disable join port in a assigned group on assigned VLAN successfully

Disable join port in a assigned group on assigned VLAN unsuccessfully

Fail to disable join port in a specified group on specified VLAN, the reason maybe MAC address not exist or port not exist.

[Example]

The below example shows how to add ports 1-5 into group 0100.5e02.0203:

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

The below example shows how to cancel adding ports 1-5 into group 0100.5e02.0203:

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

[Related commands]

Commands	Description
----------	-------------

show mac-address-table static Show static address of some one or all (ports or VLAN).

4.5 mac-address-table static unicast

[Function]

Set the static MAC address, no command to delete.

[Command Format]

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

[Parameter]

static: static address

HHHH.HHHH.HHHH: MAC address, hexadecimal number, each four characters to be point separate;

vlan: VLAN;

vlan_id: VLAN ID, range from 1-4094;

port: physical ports;

port-number: physical port, range from 1-26.

[Default]

No static MAC address.

[Command Modes]

Global configuration mode

[Explanation of command execution echo]

Set successfully

VLAN X does not exist or not active!

Port X is not in vlan Y!

Join port X in a assigned group Y on assigned VLAN Z unsuccessfully!

Warning! This MAC address has already existed.

[Example]

Set the static MAC address for port 3 which is associated with VLAN 1:

```
Raisecom(config)#mac-address-table static unicast 1234.abcd.0000  
vlan 1 port 3
```

Delete the static MAC address for port 3 which is associated with VLAN 1:

```
Raisecom(config)#no mac-address-table static unicast  
1234.abcd.0000 vlan 1 port 3
```

[Related commands]

Commands	Description
show mac-address-table static	Show the static address information for one or all (ports or VLAN).

4.6 mac-address-table threshold

[Function]

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

[Command Format]

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

[Parameter]

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

0-4095: upper bond.

[Default]

Do not set the threshold

[Command Modes]

Physical ports/range configuration mode; privileged user

[Executing Command Instruction]

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

[Explanation of command execution echo]

Set port X unsuccessfully

Set successfully

[Example]

Set the threshold for port 1 learning MAC address to 100:

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

Cancel the threshold for port 1 learning MAC address:

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

[Related commands]

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

4. 7 search mac-address

[Function]

Search a specified MAC address in the MAC address table.

[Command Format]

search mac-address HHHH.HHHH.HHHH

[Parameter]

HHHH.HHHH.HHHH: MAC address, hexiadcimal digit string, dotted for every four characters.

[Command Modes]

Global configuration mode

[Explanation of command execution echo]

If the mac address is found out, show following information:

MAC address Port number VLAN identifier symbol

[Example]

Search mac address 1234.1234.1234:

Raisecom#**search mac-address 1234.1234.1234**

[Related commands]

Commands	Description
mac-address-table 12-address	Set all MAC addresses or those addresses comply to certain condition in the switch.

4.8 show mac aging-time

[Function]

Show MAC address aging time.

[Command Format]

show mac aging-time

[Parameter]

aging-time: MAC address aging time.

[Command Modes]

Privileged EXEC; privileged user.

[Command Executing Instruction]

Only the privileged user with priority not less than 5 can use this command.

[Explanation of command execution echo]

Aging time: X seconds

Set unsuccessfully !

[Example]

Show current aging time:

Raisecom# **show mac aging-time**

[Related commands]

Commands	Description
mac-address-table aging-time	Set MAC address aging time.
no mac-address-table aging-time	Recover MAC address aging time to default value.

4.9 show mac-address-table multicast

[Function]

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.

[Command Modes]

Privileged EXEC; privileged user

[Command Executing Instruction]

show mac-address-table multicast shows all VLAN layer 2 multicast router information in the switch.

show mac-address-table multicast vlan *vlan-id* shows referred VLAN layer 2 multicast router information in the switch.

show mac-address-table multicast count shows all VLAN layer 2

multicast count information in the switch.

show mac-address-table multicast vlan *vlan-id* count shows referred VLAN layer 2 multicast port count information in the switch.

If VLAN is not referred, show all VLAN layer 2 multicast router information.

[Example]

Show all VLAN layer 2 multicast router information:

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

Multicast filter mode: Forward-all

<i>Vlan</i>	<i>Group Address</i>	<i>Ports[Static](Hardware)</i>
-------------	----------------------	--------------------------------

2	0100.5E08.0808	1-61-6
---	----------------	---------------

Show layer 2 multicast router information of VLAN 2:

Raisecom#**show mac-address-table multicast vlan 2**

Multicast filter mode: Forward-all

<i>Vlan</i>	<i>Group Address</i>	<i>Ports[Static](Hardware)</i>
-------------	----------------------	--------------------------------

2	0100.5E08.0808	1-61-6
---	----------------	---------------

Show all VLAN layer 2 multicast router count information:

Raisecom#**show mac-address-table multicast count**

Multicast filter mode: Forward-all

Multicast address entries for all Vlan: 1

Show layer 2 multicast router counter information of VLAN 2:

Raisecom#**show mac-address-table multicast vlan 2 count**

Multicast filter mode: Forward-all

Multicast address entries for all Vlans: 1

[Related commands]

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

4.10 show mac-address-table static

[Function]

Show static MAC address information.

[Command Format]

show mac-address-table static

show mac-address-table static vlan vlan_id

[Parameter]

vlan: VLAN;

vlan_id: VLAN ID, range is 1-4094.

[Command Modes]

privileged user

[Explanation of command execution echo]

Information of static mac address in switch:

port No. VLAN ID static MAC Addr

[Example]

Show static MAC address.

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

Show the static MAC address table of physical port 5:

Raisecom#**show mac-address-table static port 5**

Show the static MAC address information of vlan 2:

Raisecom#**show mac-address-table static vlan 2**

[Related commands]

Commands	Description
mac-address-table static	Set static MAC address. Use no to delete.

4.11 show mac-address-table threshold

[Function]

Show restriction of port learning MAC address amount.

[Command Format]

show mac-address-table port-list {1-maxport}

[Command Modes]

Privileged configuration mode, privileged user

[Command Executing Instruction]

This command shows restriction of port learning MAC address amount.

[Explanation of command execution echo]

port macthresholdvlan macthreshold

1 N/A N/A

[Example]

Show restriction of port learning MAC address amount:

Raisecom#**show mac-address-table threshold port-list all**

[Related commands]

Commands	Description
mac-address-table threshold	Set amount of dynamically MAC address learned from port.
no mac-address-table threshold	Recover port VLAN MAC address amount threshold to default setting.

Chapter 5 Physical Interface Management

Commands

5.1 description

[Function]

Modify the description of MAC interface or IP interface.

[Command Format]

[no] description WORD

[Parameter]

WORD: specify MAC interface description, 255 characters for length at most, the characters should not be separated by space.

[Command Modes]

Physical ports configuration mode; IP interface mode

[Executing Command Instruction]

Add physical port and IP interface description.

[Explanation of command execution echo]

Set description successfully.

Set description unsuccessfully

The description is too long.

[Example]

Set physical port description information:

Raisecom(config-port)# **description** *this-is-a-interface*

[Related commands]

Commands	Description
show interface port detail	Show the detail information of remote port.

5.2 duplex

[Function]

Use **duplex** command to set duplex mode of the physical ports.

[Command Format]

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

[Parameter]

full: full duplex;

half: half-duplex;

schedule-list: starting time, ending time and time interval of dispatching task;

list-no: list range from <0-99>.

[Default]

Duplex mode for electrical interface and 1000M optical interface is Auto-negotiation and full duplex for 100M optical interface.

[Command format]

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

[Executing Command Instruction]

Only the user with priority 15 can use this command. Different type of port can configure different type of duplex mode. 100M/1000M optical interface should not configure half-duplex; duplex mode configuration is unavailable if sub-card does not exist.

[Explanation of command execution echo]

Set successfully

Port X set unsuccessfully

Port x only supports 100M/FD!

Port x only supports 1000M/FD or auto-negotiation!

Port x is unavailable!

[Example]

Configure the Ethernet port 4 as half-duplex:

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

[Related commands]

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

5.3 dynamic statistics time

[Function]

Configure port dynamic statistics refresh frequency, use **no** to restore port dynamic stat. refresh frequency to default value

[Command format]

Dynamic statistics time *time*

No dynamic statistics time

[Parameter]

time: port dynamic statistics refresh, range is 2-60;

[Default]

By default, port dynamic statistic refresh frequency is 2s

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Use the command to configure dynamic statistics refresh frequency, default refresh frequency is 2s

[Explanation of command execution echo]

Set successfully

[Example]

Set port dynamic statistics refresh frequency is 10s:

Raisecom(config)# **dynamic statistics time 10**

[Related commands]

Command	Description
no dynamic statistics time	Restore port dynamic refresh frequency to default value
show interface port-list { <i>all</i> <i>port-list</i> } statistics dynamic	Show port-list dynamic statistics
show interface line-list <i>line-list</i> statistics dynamic	Show line-list statistics
show interface client-list <i>client-list</i> statistics dynamic	Show client-list statistics

5.4 flowcontrol {receive|send}

[Function]

Enable or disable the flow control function at the physical port.

[Command Format]

flowcontrol {*receive* | *send*} {*on* | *off*} [*schedule-list list-no*]

[Parameter]

receive: flow control at the receiving direction;

sent: flow control at the sending direction;

on: Enable flow control function;

off: Disable flow control function;

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

list-no: schedule list number range from <0-99>.

[Default]

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

[Command Modes]

Physical ports/range configuration mode; privileged user

[Executing Command Instruction]

Only users with priority 15 can use this command, flow control configuration is unsuccessful when sub-card is unavailable.

[Explanation of command execution echo]

Set successfully

Port X set unsuccessfully

Port x is unavailable!

[Example]

Enable the flow control function at the RX direction:

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

Disable the flow control function at the TX direction:

Raisecom(config-port)# **flowcontrol** send off

[Related commands]

Commands	Description
show inter port port-list	Show the port configuration information.

5.5 show interface port

[Function]

Show port information of remote device.

[Command Format]

show interface port

[Parameter]

port-list: port list.

[Command Modes]

Remote configuration mode; privileged user

[Executing Command Instruction]

Show remote device interface information, including port management status, operation status, speed and duplex and flow control enable/disable, in remote configuration mode. Remote device interface information will not be shown if remote device is disconnect or OAM link is not established.

[Explanation of command execution echo]

Raisecom(config-remote)#**show interface port**

Local Port: 12

<i>Port</i>	<i>Admin</i>	<i>Operate</i>	<i>Speed/Duplex</i>	<i>Flowcontrol</i>
-------------	--------------	----------------	---------------------	--------------------

Flowcontrol Set

<i>line 1</i>	<i>enable</i>	<i>up(100M/full)</i>	<i>100M/full</i>	<i>off</i>	<i>disable</i>
<i>client 1</i>	<i>disable</i>	<i>down</i>	<i>auto</i>	<i>off</i>	<i>disable</i>
<i>client 2</i>	<i>disable</i>	<i>down</i>	<i>auto</i>	<i>off</i>	<i>disable</i>
<i>client 3</i>	<i>disable</i>	<i>down</i>	<i>auto</i>	<i>off</i>	<i>disable</i>

client 4 enable up(100M/full) auto off disable

[Example]

Raisecom(config-port)# **show interface port**

[Related commands]

Commands	Description
shutdown	Enable/disable remotoe client port.
duplex {full half}	Configuring duplex for remote device.
speed (auto/10/100/1000)	Configuring speed for remote device.
flowcontrol {on/off}	Enable/disable remote client port flow control.
show interface port detail	Show detail information of remote device port.

5.6 show system mtu

[Function]

Show system maximal transmission unit.

[Command Format]

show system mtu

[Command Modes]

Privileged configuration mode

[Executing Command Instruction]

Use this command to show configuration of system maximal transmission unit.

[Explanation of command execution echo]

System MTU size:

[Example]

Show system mtu:

Raisecom(config)# **show system mtu**

[Related commands]

Commands	Description
system mtu <i>mtuLength</i>	Configure system maximal transmission unit.
no system mtu	Recover default value for system maximal transmission unit.

5.7 shutdown

[Function]

Shutdown the physical port, use **no** command to open the port.

[Command format]

shutdown [*schedule-list list-no*]

no shutdown [*schedule-list list-no*]

[Parameter]

schedule-list: set the starting time, ending time and time period of schedule list.

list-no: schedule list <0-99>.

[Default]

no shutdown

[Command Modes]

Ethernet physical interface/range configuration mode; privileged user

[Executing Command Instruction]

Only the user with priority 15 can use this command. Open/shutdown port will fail when sub-card does not exist.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

Port x is unavailable!

[Example]

Shutdown physical port 5:

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

Open physical port 5:

Raisecom(config-port)# **no shutdown**

[Related commands]

Commands	Description
show interface port	Show the state of some or all interface ports.

5.8 speed

[Function]

Use this command to set rate of physical port.

[Command format]

speed { *auto* | *10* | *100* | *1000* } [*schedule-list list-no*]

[Parameter]

auto: speed auto-negotiation;

10: speed is 10Mbps;

100: speed is 100Mbps;

1000: the speed the 1000Mbps;

schedule-list: set the starting time, ending time and time period of schedule list;

list-no: schedule list <0-99>.

[Default]

Electrical interface and 1000M optical interface speed is auto-negotiation and 100M optical interface is speed at 100M by default.

[Command Modes]

Ethernet physical interface/range configuration mode; privileged user

[Executing Command Instruction]

Only the user with priority 15 can use this command. Different type of port can configure different speed. 100M electrical interface should not configure 1000M speed; 100M optical interface can only configure 100M speed; 1000M optical interface can configure 1000M or auto-negotiation; relevant configuration is unavailable when sub-card does not exist.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

Port x only supports 100M/FD!

Port x only supports 1000M/FD or auto-negotiation!

Port x does not support 1000M!

Port x is unavailable!

[Example]

Set physical port 4 speed at 10Mbps:

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

[Related commands]

Commands	Description
show interface port	Show the state of some or all interface ports.

5.9 system mtu

[Function]

Configure maximal transmission unit of system.

[Command Format]

system mtu *mtuLength*

[Parameter]

mtuLength: configuring range of system maximal transmission unit.

[Default]

By default, system maximal transmission unit is default value.

[Command Modes]

Global configuration mode

[Executing Command Instruction]

Use this command to set a specified value for system maximal transmission unit. When the configured value is bigger than default value, system mtu takes the maximal configured value; when the configured value is smaller than default value, system mtu takes the smallest configured value. For some special types just support fixed value, the actual effective value is not smaller than minimum fixed value supported by device configured value.

[Explanation of command execution echo]

Actual max frame length: XXX

Set unsuccessfully

[Example]

Configure system mtu to be 6000:

Raisecom(config)# **system mtu 6000**

[Related commands]

Commands	Description
no system mtu	Recover system mtu to default value.
show system mtu	Show system mtu.

Chapter 6 Commands of Storm-control

6.1 show storm-control

[Function]

Show the setting for storm-control.

[Command Format]

storm-control

[Parameter]

storm-control: storm control function

[Command Modes]

Privileged EXEC; privileged user

[Explanation of command execution echo]

Broadcast: Enable

Multicast: Enable

Unicast destination lookup unsuccessfully (DLF): Enable

Threshold: 1024 pps

[Example]

show the storm-control rule:

Raisecom# **show storm-control**

[Related commands]

Commands	Description
storm-control	Set the rule of storm-control.
no storm-control	Delete the rule of storm-control.

6.2 storm-control

[Function]

Enable or disable port storm control function.

[Command Format]

storm-control *broadcast* {*enable* | *disable*} [*schedule-list* *list-no*]

[Parameter]

broadcast: broadcast packet;

multicast: multicast packetl;

dlf: target searching failure packet;

all: broadcast packet, multicast packet and dlf;

enable: enable storm control function;

disable: disable storm control function;

schedule-list: Set the starting time, ending time and time interval of the schedule;

list-no: schedule list range is <0-99>.

[Default]

storm control function enable

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

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

[Explanation of command execution echo]

Set successfully

Set unsuccessfully !

[Example]

Enable broadcast storm-control function:

Raisecom(config)# **storm-control** *broadcast enable*

Disable all the storm-control function:

Raisecom(config)# **storm-control** *all disable*

[Related commands]

Commands	Description
show storm-control	Show storm control function configuration for all packets or one type of packet.

Chapter 7 Transparent Transmission and Forward Commands

7.1 clear relay statistics

[Function]

Clear transparent transmission statistics

[Command Format]

Clear relay statistics [**port-list** *port-list*]

[Parameter]

Port-list

[Default]

None

[Command Modes]

Global configuration mode

[Executing Command Instruction]

Use the command to recount each port transparent transmission messages statistics from 0

[Explanation of command execution echo]

Set successfully

[Example]

Clear transparent transmission messages statistics:

Raisecom (config)# **clear relay statistics**

[Related commands]

Commands	Description
show relay [port-list]	Show current configuration information.

port-list

7.2 no relay shutdown

[Function]

Enable port

[Command Format]

No relay shutdown

[Parameter]

None

[Default]

Enable port in default state

[Command Modes]

Port mode

[Executing Command Instruction]

When port is shutdown because of transparent transmission function, use **no relay shutdown** to enable the port

[Explanation of command execution echo]

Set successfully

[Example]

Enable port 10, which is shut down by transparent transmission function:

Raisecom (config-port)# **no relay shutdown**

[Related commands]

Commands	Description
show relay [port-list]	Show current configuration information.

7.3 relay

[Function]

Start the function for forwarding layer-2 message pellucidly. Use **no** command to deny the function.

[Command Format]

relay {*bpdu* | *dot1x* | *lacp*| *gmrp* | *gvrp* | *all*} **port-list** *port-list*
[**schedule-list** *list-no*]

no relay {*bpdu* | *dot1x* | *lacp*| *gmrp* | *gvrp* | *all*} **port-list** [{*1-26*}]
[**schedule-list** *list-no*]

[Parameter]

message type: bpdu | dot1x | lacp | gmrp | gvrp;

port-list: physical port;

port-list: physical list, range is 1-26, use “,” and “-“ for multiple port input;

all: all the layer-2 message;

schedule-list: Set the starting time, ending time and time interval of the schedule;

list-no: schedule list range is <0-99>.

[Default]

disable

[Command Modes]

Global configuration mode; privileged user (priority 15)

[Executing Command Instruction]

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

[Explanation of command execution echo]

Failed to set forwarding ports

Set forwarding ports successfully

[Example]

Start the transparent transmission for EAPOL message at port 3:

Raisecom (config)# **relay dot1x port-list 3**

Deny transparent transmission for EAPOL message:

Raisecom (config)# **no relay dot1x port-list 3**

[Related commands]

Commands	Description
show relay port-list	Show current configuration information.

7.4 relay cos

[Function]

Configure the COS value of transparent transmission message TAG;

[Command Format]

Relay cos *cos--ID*

No relay cos

[Parameter]

cos-id cos value, range is <1-7>

[Default]

Default value is 5

[Command Modes]

Global configuration mode

[Executing Command Instruction]

Use the command to configure COS value.

[Explanation of command execution echo]

Set successfully

[Example]

Configure COS value to 7:

Raisecom (config)# **relay cos 7**

Restore COS to default value:

Raisecom (config)# **no relay cos**

[Related commands]

Commands	Description
show relay [port-list <i>port-list]</i>	Show current configuration information.

7.5 relay destination-address

[Function]

Configure transparent transmission messages destination MAC address;

[Command Format]

Relay destination-address *mac-address*

No relay destination-address

[Parameter]

Mac-address designate the message multicast MAC address

[Default]

The destination MAC address default value is: 0x010E-5E00-0003

[Command Modes]

Global mode

[Executing Command Instruction]

Use the command to configure transparent transmission destination MAC address, it must be a multicast address, and can take 0x0180-c200 and 0x010e-5E00 as the head, but default value 0x010e-5E00-0003 is available

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

Set unsuccessfully. The destination MAC address is wrong.

[Example]

Configure the destination MAC to 0180.C100.0002

```
Raisecom (config-port)# relay destination-address 0180.c100.0002
```

Restore the transparent transmission messages destination MAC to default value:

```
Raisecom (config-port)# no relay port
```

[Related commands]

Commands	Description
show relay [port-list <i>port-list</i>]	Show current configuration information.

7.6 relay drop-threshold

[Function]

Configure the message threshold of port dropping packets

[Command Format]

Relay drop-threshold {stp | dot1x | lacp} *drop-threshold-value*

No relay drop-threshold {stp | dot1x | lacp}

[Parameter]

Stp | dot1x | lacp transparent transmission protocol type

drop-threshold-value packets loss threshold, <1-4096>, unit is messages/second

[Default]

Default value is 0, which means no threshold

[Command Modes]

Port mode

[Executing Command Instruction]

Use the command to set dropping packets threshold, that is, when the port receiving messages rate is larger than the shutting down threshold, the

port will be shut down. Only when transparent transmission function is enabled, can dropping packets function takes effect

[Explanation of command execution echo]

Set successfully

[Example]

In port 10, configure STP messages dropping packets threshold to 2000:

Raisecom (config)# **relay drop-threshold stp** 2000

Restore the threshold value to default value 0:

Raisecom (config)# **no relay drop-threshold stp**

[Related commands]

Commands	Description
show relay [port-list <i>port-list]</i>	Show current configuration information.

7.7 relay port

[Function]

Configure transparent transmission message designated egress port

[Command Format]

Relay port *port-ID*

No relay port

[Parameter]

port-ID designate egress port <1-MAX_PORT>

[Default]

By default, there is no designated egress port

[Command Modes]

Interface mode

[Executing Command Instruction]

Use the command to designate egress port for transparent transmission messages, that is, local port ingress encapsulation transparent transmission messages can be sent out from only the designated port. It is the same to the opposite process.

[Explanation of command execution echo]

Set successfully

Port X set unsuccessfully. Egress port can't be the ingress port of PDUs

[Example]

Designate egress port 21 on port 23:

Raisecom (config-port)# **relay port 21**

Delete designated VLAN:

Raisecom (config-port)# **no relay port**

[Related commands]

Commands	Description
show relay [port-list <i>port-list]</i>	Show current configuration information.

7.8 relay shutdown-threshold

[Function]

Configure the message threshold of shutting down port

[Command Format]

Relay shutdown-threshold {stp | dot1x | lacp} *shutdown-threshold-value*

Shutdown-threshold-value port shutting down threshold, <1-4096>, unit is: messages/second

[Parameter]

Stp | dot1x | lacp transparent transmission protocol type

Shutdown-threshold-value port shutting down threshold, <1-4096>, unit

is messages/second

[Default]

Default transparent transmission protocol port shutting down value is 0, which means no threshold

[Command Modes]

Port mode

[Executing Command Instruction]

Use the command to set port shutting down threshold, that is, when the port receiving messages rate is larger than the shutting down threshold, the port will be shut down. When port is disabled because of transparent transmission, use **no relay shutdown** to enable the port. Only when transparent transmission function is enabled, can port shutdown function takes effect

[Explanation of command execution echo]

Set successfully

[Example]

In port 10, configure STP messages shutting down threshold to 2000:

Raisecom (config-port)# **relay shutdown-threshold stp** 2000

Restore the threshold value to default value 0:

Raisecom (config-port)# **no relay shutdown-threshold stp**

[Related commands]

Commands	Description
show relay [port-list <i>port-list]</i>	Show current configuration information.

7.9 show relay

[Function]

Show the setting of transparent transmission port.

show relay

[Parameter]

relay: port transparent transmission for layer-2 packets.

[Command Modes]

Privileged EXEC; privileged user.

[Explanation of command execution echo]

Type	line ports

BPDU	--
Dot1x	--
LACP	--

[Example]

Show transparent transmission port:

Raisecom# **show relay**

[Related commands]

Commands	Description
relay protocol-type line [<i>client</i>]	Set transparent transmission line port.
relay protocol-type client	Set transparent transmission client port.

7.10 show relay statistics

[Function]

Show transparent transmission message statistics

[Command Format]

Show relay statistics [**port-list** *port-list*]

[Parameter]

Port-list

[Default]

None

[Command Modes]

All

[Executing Command Instruction]

None

[Explanation of command execution echo]

Port	Protocol	Encapsulation Counter	Decapsulation Counter	Drop Counter

--				
1	stp	245	0	0
	dot1x	0	0	0
	lacp	0	0	0
2	stp	0	0	0
	dot1x	0	0	0
	lacp	0	0	0

[Example]

Show transparent transmission configuraiton

Raisecom # **show relay statistics**

[Related commands]

Commands	Description
Relay {stp dot1x lacp all}	Enable transparent transmission type

Chapter 8 Layer-3 Interface Commands

8.1 description

[Function]

Modify layer-3 interface description

[Command Format]

[no] description WORD

[Parameter]

WORD- the description of designated layer-3 interface, maximum length is 64 characters, it can not be divided with space

[Default]

Default description is **ip interface IfNum**

[Command Modes]

IP interface mode

[Executing Command Instruction]

User can add designated layer 3 description in interface configuration mode

[Explanation of command execution echo]

Set description successfully

Set description unsuccessfully

The description is too long

[Example]

Configure layer-3 interface description

```
raisecom(config-ip)# description this-is-a-interface
```

[Related commands]

Commands	Description
Show interface ip description	Show device layer-3 interface description

8.2 interface ip

[Function]

To enter IP interface mode.

[Command Format]

interface ip <0-IfNum>

[Parameter]

<0-IfNum>: IP interface number.

[Default]

All the system IP interfaces have no address

[Command Modes]

Global configuration mode; Privileged EXEC.

[Executing Command Instruction]

Use **interface ip** command to enter IP configuration mode, it is available to configure management address for Ethernet switch.

[Example]

To enter the configuration mode for IP interface 4:

```
raisecom(config)# interface ip 4
```

[Related commands]

Commands	Description
ip address	Set the IP address for current interface.
show interface ip	Show the layer-3 interface

8.3 ip address

[Function]

Set IP address of current interface.

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

[Command Format]

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

no ip address *ip-address*

[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]

No IP address is configured for the current interface by default.

[Command Modes]

Ethernet layer-3 interface configuration mode and Privileged user

[Executing Command Instruction]

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

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

Too many VLAN Set in the interface.

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

Can't add ip interface for cluster member.

Invalid network mask.

Can not assign ip address for vlan X ...

Invalid IP address or network mask.

VLAN X already associated with interface Y.

A.B.C.D overlaps with interface X.

[Example]

Set current interface IP address to 192.168.1.2, associated VLAN ID is 2:

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

Erase interface IP address:

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

[Related commands]

Commands	Description
show ip route	Show the route.
show interface ip	Show layer-3 interface.

8.4 show interface ip

[Function]

Show layer 3 in privileged EXEC mode.

[Command Format]

show interface ip

[Command Modes]

Privileged EXEC, privileged user

[Executing Command Instruction]

Show layer 3 configuration in Privileged EXEC mode by this command.

[Explanation of command execution echo]

Raisecom#**show interface ip**

<i>Index</i>	<i>Ip Address</i>	<i>NetMask</i>	<i>Vid</i>	<i>Status</i>
--------------	-------------------	----------------	------------	---------------

0 20.0.0.1 255.0.0.0 1 active

[Example]

Raisecom#**show interface ip**

[Related commands]

Commands	Description
ip address	Set the IP address

8.5 show interface ip description

[Function]

In privileged EXEC mode show layer-3 interface description

Show interface ip description

[Parameter]

None

[Default]

None

[Command Modes]

Privileged EXEC mode; privileged user

[Executing Command Instruction]

Use the command to show layer-3 interface configuration description in privileged EXEC mode

[Explanation of command execution echo]

Raisecom#show interface ip description

Index Description

0 this-is-an-interface

1 ip interface 1

2 ip interface 2

3 ip interface 3

4 ip interface 4

...

[Example]

Raisecom#**show interface ip description**

[Related commands]

Commands	Description
Description	Show device layer-3 interface description

8.6 show interface ip statistics

[Function]

In privileged EXEC mode show layer-3 interface statistics information

Show interface ip *ifNum* statistics

[Parameter]

ifNum: IP interface number, range is [0-MAX-IP-PORT]

[Default]

None

[Command Modes]

Privileged EXEC mode; privileged user

[Executing Command Instruction]

User can add designated layer 3 description in interface configuration mode

[Explanation of command execution echo]

Set description successfully

Set description unsuccessfully

The description is too long

[Example]

Configure layer-3 interface description

raisecom(config-ip)# **description** *this-is-a-interface*

[Related commands]

Commands	Description
Show interface ip description	Show device layer-3 interface description



Chapter 9 Trunk Group Commands

9.1 show trunk

[Function]

Show trunk information, trunk mode and member port of current trunk group and current enabled member port.

[Command Format]

show trunk

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

This command is used to display the load-sharing mode of all aggregated links, ticket algorithm using mac address, all current aggregation group, group members and current effective member port. The current effective member port is the group member that has “UP” status.

[Explanation of command execution echo]

Trunk: Enable

Loading sharing mode: SXORDMAC

Loading sharing ticket algorithm: --

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

[Example]

Display current trunk related information:

Raisecom# **show trunk**

[Related commands]

Commands	Description
trunk	Enable/disable trunk function.
trunk-group	Create an aggregation group.
trunk-loading-sharing mode	Set the load-sharing mode of all aggregated ports

9.2 trunk

[Function]

Enable or disable trunk function.

[Command Format]

trunk {*enable*|*disable*}

[Parameter]

enable: enable trunk function

disable: disable trunk function

[Default]

enable

[Command Modes]

Global configuration mode; Privileged user.

[Executing Command Instruction]

Use this command to enable or disable trunk function.

[Explanation of command execution echo]

Set success

Set unsuccessfully !

[Example]

Enable trunk function for the link:

Raisecom(config)# **trunk enable**

Disable trunk function for the link:

Raisecom(config)# **trunk disable**

[Related commands]

Commands	Description
show trunk	Show trunk status, trunk load-sharing mode, all the trunk members of the trunk group and all the current enabled port member.

9.3 trunk group

[Function]

Add a trunk group, **no** command is used to delete the operation.

[Command Format]

trunk group *trunk-group-id portlist*

no trunk group *trunk -group-id*

[Parameter]

trunk-group-id: trunk group ID, range is 1—6.

portlist: port number for the group, format can be 1-3, 5 etc. 8 ports as the maximum.

[Command Modes]

Global configuration mode, privileged user

[Executing Command Instruction]

Use this command to create a link trunk. Combine appointed *portlist* aggregation to a single aggregation port. Each aggregation port includes 8 ports with the same speed as the maximum.

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

[Explanation of command execution echo]

Set successfully

Set unsuccessfully !

Permit 8 members at most!

Some member ports are overlapped with those of other trunk group!

Trunk group 3 is not exist!

[Example]

Create aggregation group 3, including prt 1, 4, 5, 6, 8:

Raisecom(config)#**trunk group 3 1,4-6,8**

Delete aggregation group 3:

Raisecom(config)#**no trunk group 3**

[Related commands]

Commands	Description
show trunk	Show trunk status, trunk load-sharing mode, all the trunk members of the trunk group and all the currently enabled port member.

9.4 trunk loading-sharing mode

[Function]

Set loading-sharing mode for the trunk group, **no** command can delete operation.

[Command Format]

trunk loading-sharing mode {*smac* | *dmac* | *sxordmac* | *sip* | *dip* | *sxordip*}

no trunk loading-sharing mode

[Parameter]

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

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

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

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

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

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

[Default]

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

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

Users can select different loading shared mode based on the usage of the aggregation links.

For example, if the link is used to connect layer-3 switch in order to provide router support for access layer, users should select loading shared mode based on source MAC address, since the data flow of trunk group are of the same destination MAC but different source MAC.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully !

[Example]

Select the forward port based on source IP address for trunk load-sharing mode:

Raisecom(config)#**trunk loading-sharing mode sip**

Recover trunk load-sharing mode to default setting:

Raisecom(config)#**no trunk loading-sharing mode**

[Related commands]

Commands	Description
show trunk	Show trunk status, trunk load-sharing mode, all the trunk members of the trunk group and all the currently enabled port member.

9.5 trunk loading-sharing ticket-generation-algorithm

[Function]

Set loading-sharing ticket algorithm of the trunk.

[Command Format]

[no] trunk loading-sharing ticket-generation-algorithm{*crc*|*direct-map*}

[Parameter]

crc: CRC value of MAC address;

direct-map: direct mapping value.

[Command Modes]

Global configuration mode

[Executing Command Instruction]

This command is used to set load-sharing ticket algorithm.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully !

[Example]

Set load-sharing ticket algorithm based on CRC:

Raisecom# **trunk loading-sharing ticket-generation-algorithm *crc***

[Related commands]

Commands	Description
show trunk	Show trunk information.

Chapter 10 STP Commands

10.1 instance vlan

[Function]

Configure the mapping relationship between instance and vlan

[Command Format]

instance *instance-id* **vlan** *vlanlist*

no instance *instance-id* [**vlan** *vlanlist*]

[Parameter]

Instance-id instance number, range is 0 to a value before 4094

[Command Modes]

Region configuration mode; privileged user

[Executing Command Instruction]

Use the command to configure the mapping relationship between monitoring region instance and VLAN. When you exit the monitoring region, the configuration will be written into the operation region. In region configuration mode, use **show spanning-tree region-configuration** to show the configuration results. When you use **instance** *instance-id* **vlan** *vlanlist*, if the corresponding instance does not exist, then it will be created, and if it exist, the input VLAN will be added to the instance. In the command **no instance** *instance-id* [**vlan** *vlanlist*], if the instance does not exist, there will be echo notice, otherwise the later input VLAN will be deleted from the instance, if it is not instance 0 and no VLAN is included in the instance, then the instance will be deleted; if the VLAN list option is not input, then it will be deleted.

[Explanation of command execution echo]

Set successfully

[Example]

Map VLAN 10,100-200 to instance 1:

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

```
Raisecom(config-region)#instance 1 vlan 10,100-200
```

Set successfully

Delete VLAN 100-150 from instance 1:

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

```
Raisecom(config-region)#no instance 1 vlan 100-150
```

Set successfully

Delete instance 1:

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

```
Raisecom(config-region)#no instance 1
```

Set successfully

[Related commands]

Commands	Description
Show spanning-tree region-configuration	Show spanning-tree region configuration

10.2 name

[Function]

Configure MST region name

[Command Format]

name *WORD*

no name

[Parameter]

WORD region name, the character string length can not be longer than 32

[Command Modes]

Region configuration mode; privileged user

[Executing Command Instruction]

Use the command to configure the name of monitoring region. When logging out monitoring region, the region name will be configured to operation region. In region configuration mode, use **show spanning-tree region-configuration** to show the configuration result.

[Explanation of command execution echo]

Set successfully

The length of region name can't be longer than 32

[Example]

Configure the region name to hello:

Raisecom(config)#spanning-tree region-configuration

Raisecom(config-region)#name hello

[Related commands]

Commands	Description
Show spanning-tree region-configuration	Show spanning-tree region configuration

10.3 show spanning tree

[Function]

Show the spanning-tree examples or appointed spanning-tree information.

[Command Format]

show spanning-tree

[Command Modes]

Privilege configuration mode; privileged user

[Executing Command Instruction]

Show the information of spanning tree, including example information

and port information under the example. Show the example information if there is appointed example No.; show information of all running example information (in order of example number) if there is no appointed example No.; related prompt information will show if the appointed example is invalid.

[Explanation of command execution echo]

Echo 1:

MSTP Admin State: Disable

Protocol Mode: MSTP

Echo 2:

No spanning-tree information available for instance instance-id

Echo 3:

MSTP Admin State: Enable

Protocol Mode: MSTP

MST ID: 0

BridgeId: Mac 000E.5E03.84D0 Priority 32768

Root: Mac 000E.5E03.84D0 Priority 32768 RootCost 0

RegionalRoot: Mac 000E.5E03.84D0 Priority 32768 InternalRootCost 0

Operational: HelloTime 2, ForwardDelay 15, MaxAge 20

Configured: HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3

MaxHops 20, Diameter 7

<i>PortId</i>	<i>PortState</i>	<i>PortRole</i>	<i>PathCost</i>	<i>PortPriority</i>	<i>LinkType</i>	<i>TrunkPort</i>
---------------	------------------	-----------------	-----------------	---------------------	-----------------	------------------

<i>1</i>	<i>discarding</i>	<i>disabled</i>	<i>200000</i>	<i>128</i>	<i>point-to-point</i>	<i>no</i>
----------	-------------------	-----------------	---------------	------------	-----------------------	-----------

.....

MST ID: 1

BridgeId: Mac 000E.5E03.84D0 Priority 32768

RegionalRoot: Mac 000E.5E03.84D0 Priority 32768 InternalRootCost 0

<i>PortId</i>	<i>PortState</i>	<i>PortRole</i>	<i>PathCost</i>	<i>PortPriority</i>	<i>LinkType</i>	<i>TrunkPort</i>
---------------	------------------	-----------------	-----------------	---------------------	-----------------	------------------

<i>1</i>	<i>discarding</i>	<i>disabled</i>	<i>200000</i>	<i>128</i>	<i>point-to-point</i>	<i>no</i>
----------	-------------------	-----------------	---------------	------------	-----------------------	-----------

.....
MST ID: 1

.....
Echo 4:

MSTP Admin State: Enable

Protocol Mode: MSTP

MST ID: 0

BridgeId: Mac 000E.5E03.84D0 Priority 32768

Root: Mac 000E.5E03.84D0 Priority 32768 RootCost 0

RegionalRoot: Mac 000E.5E03.84D0 Priority 32768 InternalRootCost 0

Operational: HelloTime 2, ForwardDelay 15, MaxAge 20

Configured: HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3

MaxHops 20, Diameter 7

Port 1

State:discarding Role:disabled Priority:128 Cost: 200000 TrunkPort:no

Root: Mac 000E.5E03.84D0 Priority 32768 RootCost 0

RegionalRoot: Mac 000E.5E03.84D0 Priority 32768 InternalRootCost 0

DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 2

.....

MST ID: 1

BridgeId: Mac 000E.5E03.84D0 Priority 32768

RegionalRoot: Mac 000E.5E03.84D0 Priority 32768 InternalRootCost 0

Port 1

State:discarding Role:disabled Priority:128 Cost: 200000 TrunkPort:no

RegionalRoot: Mac 000E.5E03.84D0 Priority 32768 InternalRootCost 0

DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

Port 2

.....

MST ID: 1

.....

[Related commands]

Commands	Description
spanning-tree	Enable/disable spanning tree.
spanning-tree bridge-diameter	Set network diameter.
spanning-tree priority	Set system priority or port priority.
spanning-tree path-cost	Set port path cost.

spanning-tree forward-delay	Set forward-delay of spanning-tree protocol.
spanning-tree hello-time	Set hello-time of spanning-tree.
spanning-tree max-age	Set max-age of spanning-tree.
spanning-tree max-hops	Set maximal hops of MST.
spanning-tree transit-limit	Set maximal trasimit packets per hello time.
spanning-tree link-type	Set link type of port.
spanning-tree mode	Set spanning-tree mode of the switch.

10.4 show spanning-tree port-list/line/client

[Function]

Show the port activity status and configuration of spanning tree.

[Command Format]

show spanning-tree [*instance instance-id*] **port-list** [*portlist*] [**detail**]

show spanning-tree line [*linelist*]

show spanning-tree client [*clientlist*]

[Parameter]

Instance-id

Portlis / linelist/ clientlst

Detail show spanning-tree instance detailed information

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

show the port activity status and configuration of spanning tree. Show port information under the example if there is appointed example number and don't show information under other examples; show port information under all examples if there is no appointed example number; show all port information participates in spanning tree calculation under the switch if there is no port list appointed, or just show the appointed port list.

[Explanation of command execution echo]

Echo 1:

PortEnable: admin: enable oper: disable

No spanning-tree information available on this port

Port ID:2

PortEnable: admin: enable oper: disable

No spanning-tree information available on this port

.....

Echo 2:

Port ID:1

PortEnable: admin: enable oper: enable

EdgedPort: admin: auto oper: no

LinkType: admin: auto oper: point-to-point

Partner MSTP Mode: mstp

Bpdus send: 0 (TCN<0> Config<0> RST<0> MST<0>)

Bpdus received:0 (TCN<0> Config<0> RST<0> MST<0>)

Instance PortState PortRole PortCost(admin/oper) PortPriority

0 discarding disabled 200000/200000 128

1 discarding disabled 200000/200000 128

Echo 3:

Port ID:1

PortEnable: admin: enable oper: enable

EdgedPort: admin: auto oper: no

LinkType: admin: auto oper: point-to-point

Partner MSTP Mode: mstp

Bpdus send: 0 (TCN<0> Config<0> RST<0> MST<0>)

Bpdus received:0 (TCN<0> Config<0> RST<0> MST<0>)

This port In mst0 Info:

State:discarding Role:disabled Priority:128 Cost: 200000

Root: Mac 000E.5E03.84D0 Priority 32768 RootCost 0

RegionalRoot: Mac 000E.5E03.84D0 Priority 32768 InternalRootCost 0

DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

This port In mst1 Info:

State:discarding Role:disabled Priority:128 Cost: 200000

RegionalRoot: Mac 000E.5E03.84D0 Priority 32768 InternalRootCost 0

DesignatedBridge: Mac 0000.0000.0000 Priority 0 DesignatedPort 0

.....

Port ID 2

.....

[Related commands]

Commands	Description
spanning-tree	Enable/disable spanning tree.
spanning-tree priority	Set system priority or port priority.
spanning-tree path-cost	Set port path cost.
spanning-tree link-type	Set link type of switch port.
spanning-tree edged-port	Set edged port type of switch.
spanning-tree clear statistics	Clear spanning tree statistics under port.

10.5 show spanning-tree region-operation

[Function]

In region configuration mode, show MST region configuration

[Command Format]

Show spanning-tree region-configuration

[Parameter]

None

[Command Modes]

Region configuration mode; privileged user

[Executing Command Instruction]

Show MST operation region information

[Explanation of command execution echo]

Operational:

Name: raisecom

Revision level: 0 Instances running: 2

Digest: 0x40D5ECA178C657835C83BBCB16723192

Instance Vlans Mapped

0 2-4094

1 1

[Example]

None

[Related commands]

Commands	Description
Name	Configure region name
Revision-level	Configure revision level

Instance vlan	Configure the mapping relationship between the instance and VLAN
---------------	--

10.6 spanning-tree

[Function]

Enable or disable spanning tree (802.1W Rapid Spanning Tree Protocol).

[Command Format]

spanning-tree {enable / disable}

[Parameter]

enable: Enable spanning tree;

disable: Disable spanning tree.

[Default]

Enable.

[Command mode]

Global configuration mode or Physical port configuration mode;
privileged user

[Executing Command Instruction]

STP can avoid loop in network, but will increase CPU overhead. Users can enable/disable STP according to actual need.

Before or after starting STP, it is available to use configuration command to configure STP parameters for device of the ports. Operating this command under global configuration mode is to enable/disable device STP; while operating this command under Ethernet port configuration mode is to enable/disable port STP. No matter port STP enable or disable, STP will stop all schedules of spanning tree when global STP disable; port STP will be effective only when global STP is enabled.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Globally disable spanning tree protocol:

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

Globally enable spanning tree protocol:

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

Under physical interface configuration mode, disable spanning tree protocol on the port:

```
Raisecom(config-port)# spanning-tree disable
```

[Related commands]

Commands	Description
show spanning-tree <i>[detail]</i>	Show active state and configuration information of spanning tree.
show spanning-tree port-list <i>[detail]</i>	Show port information of spanning tree.

10.7 spanning-tree clear statistics

[Function]

Clear RSTP statistical information.

[Command Format]

spanning-tree clear statistics

[Command Modes]

Physical interface/port range configuration mode; privileged user

[Executing Command Instruction]

Use this command to clear statistical information on designated port.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Clear spanning tree information of port 3:

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

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

[Related commands]

Commands	Description
show spanning-tree port-list <i>[detail]</i>	Show port information of spanning tree.

10.8 spanning-tree edged-port

[Function]

Set edged-port type of the port.

[Command Format]

spanning-tree edged-port

[no] spanning-tree edged-port

[Default]

All ports of bridge are configured as self-check edged port mode.

[Command Modes]

Physical port/ port range configuration mode; privileged user.

[Executing Command Instruction]

spanning-tree edged-port command is used to configure current Ethernet port to be edged-port.

no spanning-tree edged-port is used to recover the current Ethernet port to default status, that is non edged-port.

If current Ethernet port is connected to other switch, please use **no spanning-tree edged-port** command to specify it to non edged-port.

Use **spanning-tree edged-port** to specify the Ethernet port which directly connected to PC to be edged-port.

If you configure a port as edge port on an RSTP switch, the edge port immediately transitions to the forwarding state. So please enable it only on ports that connect to a single end station.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Set port 1 to be edged port:

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

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

Recover port 1 to be edged port self-check mode:

Raisecom(port)# **no spanning-tree edged-port**

[Related commands]

Commands	Description
show spanning-tree port-list [detail]	Show port information of spanning tree.

10.9 spanning-tree extern-path-cost

[Function]

Configure port outer path-cost

[Command Format]

spanning-tree extern-path-cost *pathcost*

no spanning-tree extern-path-cost

[Default]

By default, port outer path coast is 0

[Command Modes]

Physical port/ port range configuration mode; privileged user.

[Executing Command Instruction]

The voting process of span-tree lives on priority vector, outer path cost is a part of priority vector, which effects the voting of port role

[Explanation of command execution echo]

Set successfully.

[Example]

Set port extern-path-cost to be 10000

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

Raisecom(port)#**spanning-tree extern-path-cost 10000**

[Related commands]

Commands	Description
show spanning-tree	Show STP instance information

10.10 spanning-tree forward-delay

[Function]

Set the forward-delay of spanning tree.

The forward delay is the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state:

[Command Format]

spanning-tree forward-delay <4-30>

no spanning-tree forward-delay

[Parameter]

<4-30>: The time delay of spanning tree protocol bridge port status conversion, unit is second.

[Default]

15 seconds

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

The forward delay is the number of seconds a port waits before changing from its spanning-tree learning and listening states to the forwarding state. Use command **no spanning-tree forward-delay** can recover to default value.

Configuration of max-age will triggering forward-delay automation schedule to calculate a priority value for matching max-age. Configuration of network diameter and hello-time will trigger forward-delay automation schedule as well. If users don't want enable automation schedule, it is better to configure network diameter, hello-time or max-age before configure forward-delay.

[Explanation of command execution echo]

Set successfully.

*Set unsuccessfully. Forward-delay must satisfy the formula:
 $2 * (\text{forward-delay} - 1) \geq \text{max-age}$*

[Example]

Set the value of forward-delay to 10 seconds:

Raisecom(config)# **spanning-tree forward-delay 10**

[Related commands]

Commands	Description
show spanning-tree port-list <i>[detail]</i>	Show port information of spanning tree.
spanning-tree max-age	Set the max-age of spanning tree.
spanning-tree priority	Set the system priority or port priority of spanning tree.
spanning-tree bridge-diameter	Set network diameter of spanning tree protocol.

10.11 spanning-tree hello-time

[Function]

You can configure the interval between the generations of configuration messages by the root switch by changing the hello time.

[Command Format]

spanning-tree hello-time <1-10>

no spanning-tree hello-time

[Parameter]

<1-10>: The time interval of time-lapse sending bridge configuration information. Unit is second.

[Default]

2 seconds.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

You can configure the interval between the generations of configuration messages.

BPDU interval is 2 seconds by default. Decrease the interval to strong STP when loss ratio of configuration interface is high; increase this interval can reduce CPU occupation by STP. Reasonable hello-time will ensure connection of network and don't take up too much resource to find out network fault.

Forward-delay and max-age value will be calculated out by automation when configuring hello-time. Hello-time value will renew to default 2 seconds when configuration network diameter, in this case, if user want enable hello-time, it is suggested not configure network diameter after configuration hello-time. Or else the value configured forestall will be changed during configuration of network diameter. Use the command **no spanning-tree hello-time** to recover default value.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Set the hello-time of spanning tree to 3 seconds:

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

Set the hello-time of spanning to the default value that is 2 seconds:

```
Raisecom(config)# no spanning-tree hello-time
```

[Related commands]

Commands	Description
show spanning-tree port-list <i>[detail]</i>	Show port information of spanning tree.
spanning-tree forward-delay	Set the forward-delay of spanning tree.
spanning-tree max-age	Set the max-age of spanning tree.
spanning-tree bridge-diameter	Set network diameter of spanning tree protocol.

10.12 spanning-tree inter-path-cost

[Function]

Configure port inter path cost

[Command Format]

```
spanning-tree [instance instance-id] inter-path-cost pathcost
```

```
no spanning-tree [instance instance-id] inter-path-cost
```

[Parameter]

Instance-id range is 0-4095

Pathcost used to mark port inter-path-cost, range is 0-200000000

[Default]

By default, port inter-path-cost is 0

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

The voting process of span-tree lives on priority vector, outer path cost is a part of priority vector, which effects the voting of port role

[Explanation of command execution echo]

Set successfully.

Instance instance-id does not include port portid

[Example]

Set port 1 instance 1 inter-path-cost to 10000

Raisecom(config)#interface port 1

Raisecom(config)# **spanning-tree instance 1 inter-path-cost** 10000

[Related commands]

Commands	Description
show spanning-tree	Show port information of spanning tree.

10.13 spanning-tree link-type

[Function]

Set the RSTP link type of switch port.

[Command Format]

spanning-tree link-type {point-to-point | shared}

no spanning-tree link-type

[Parameter]

point-to-point: set the RSTP link type as point-to-point.

shared: set the type of link to shared.

[Default]

By default, switch set link type as point-to-point in full-duplex mode, as shared link in half-duplex mode.

[Command Modes]

Physical port/port range configuration mode; privileged user.

[Executing Command Instruction]

User can use this command to change the default setting of RSTP link type. Example: half-duplex port use point-to-point mode to connect the RSTP switch, if the port is set to point-to-point, then this port can change its state quickly.

Command **spanning-tree link-type** can change default setting of port link type, and command **no spanning-tree link-type** will recover auto-check of port link type.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Set link type of the port as shared link:

```
Raisecom(config)# spanning-tree link-type shared
```

Recover the port to auto-negotiation link type:

```
Raisecom(config)# no spanning-tree link-type
```

[Related commands]

Commands	Description
show spanning-tree port-list <i>[detail]</i>	Show port information of spanning tree.

10.14 spanning-tree max-age

[Function]

Set maximum aging time of spanning tree.

[Command Format]

spanning-tree max-age <6-40>

no spanning-tree max-age

[Parameter]

<6-40>: The maximum aging time of spanning tree configuration information, unit is second.

[Default]

The maximum age is 20 seconds.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

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

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Set the max-age of spanning tree to 30 seconds:

Raisecom(config)# **spanning-tree max-age 30**

Set the max-age of spanning tree to 20 seconds:

Raisecom(config)# **no spanning-tree max-age**

[Related commands]

Commands	Description
show spanning-tree port-list <i>[detail]</i>	Show port information of spanning tree.
spanning-tree forward-delay	Set forward-delay of spanning tree.
spanning-tree hello-time	Set the hello-time of spanning tree.
spanning-tree bridge-diameter	Set the diameter of spanning tree.

10.15 spanning-tree mcheck

[Function]

Force the port as RSTP mode.

[Command Format]

spanning-tree mcheck

[Command Modes]

Physical port/range configuration mode; privileged user.

[Executing Command Instruction]

When the network is stable, though the bridge which runs STP is disconnected, the port of running switch which runs RSTP still runs under the STP mode, under this situation, user can use **spanning-tree mcheck** command to set mCheck variable to force the port moving to RSTP mode. If the port is moved to RSTP mode, when the port get the new STP packet, port will back to STP mode again.

Only when the RSTP switch is working under global RSTP mode, user can use this command. If the RSTP switch is working under global STP mode, the command is not available.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Set port 3 works under STP mode, disconnecting with opposite end; and the bridge works under RSTP mode, so port 3 should works under RSTP mode:

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

Raisecom(port)#**spanning-tree mcheck**

[Related commands]

Commands	Description
show spanning-tree port-list	Show port information of spanning tree protocol.

10. 16 spanning-tree mode

[Function]

Set the switch in STP or RSTP mode.

[Command Format]

spanning-tree mode *{stp/rstp}*

no spanning-tree mode

[Parameter]

stp: STP mode.

rstp: RSTP mode.

[Default]

Spanning-tree running mode is MSTP mode by default.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

802.1w protocol defines two modes: stp mode and rstp compatible mode.

Under the STP mode, switch does not execute fast forwarding of designated port and fast changing from designated port to root port.

RSTP only send STP BPDU and topology changing notification. The received RST BPDU will be dropped.

Under RSTP mode switch sends MST BPDU. If the connected switch port is running STP protocol, port will change to STP compatible mode.

Use the command **no spanning-tree mode** to recover switch into default working mode.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Set switch info STP spanning tree mode:

Raisecom(config)# **spanning-tree mode stp**

[Related commands]

Commands	Description
show spanning-tree	Show the activity status of spanning tree and configuration information.

10.17 spanning-tree region-configuration

[Function]

Enter/exit region configuration mode

[Command Format]

spanning-tree region-configuration

to quit: **quit/exit/^z**

[Parameter]

None

[Default]

None

[Command Modes]

Domain configuration mode

[Executing Command Instruction]

Use **spanning-tree region-configuration** to enter region configuration mode, in this mode you can define region name, instance- VLAN relationship; when you quit form region configuration mode, region configuration takes effect. In region configuration mode you can use **show spanning-tree region-configuration** to show current configuration-region and operation-region. In other modes, use **show spanning-tree region-operation** to show operation region information.

[Example]

Enter region configuration mode:

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

Raisecom(config-region)#

[Related commands]

Commands	Description
Name <i>WORD</i>	Configure region name
Instance <i>instance-id</i> vlan <i>vlanlist</i>	Configure instance and vlan mapping relationship
Revision-level <i>level</i>	Configure MST revision
Show spanning-tree region-operation	Show spanning tree operation region configuration
Show spanning-tree region-configuration	Show spanning tree configuration region and operation region information

10.18 spanning-tree rootguard

[Function]

Configure rootguard attribution

[Command Format]

Spanning-tree rootguard {enable | disable}

[Parameter]

Enable enable rootguard function

Disable disable rootguard function

[Default]

By default, port rootguard function is disabled

[Command Modes]

Physical interface/port range configuration mode ; privileged user

[Executing Command Instruction]

When a bridge receives higher priority message, re-voting is need, which effects both network connectivity and CPU resource. To a network that has enabled MSTP, if someone sends out high priority BPDU message to attack the network, it may cause endless voting and effect network stability. To these ports that is near to the edge, you can enable rootguard function, and deny the messages with higher priority than bridge priority, then block the port for a time to prevent the attack source from effecting upper layer link.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully, root guard port must be designated port in all instance

[Example]

Enable port 1 rootguard function

Raisecom(config-port)# **spanning-tree rootguard enable**

Set successfully

[Related commands]

Commands	Description
----------	-------------

show spanning-tree	Show the activities status and configuration information of spanning tree.
show spanning-tree port	Show the port activities status and configuration information of spanning tree.



Chapter 11

DHCP Commands

11.1 ip address dhcp vlanid

[Function]

Enable DHCP Client function in IP interface (only interface 0), in the designated VLAN and DHCP server IP address, acquire automatically the IP address and the requested parameters, like gateway address, TFTP server name(option66), TFTP server address(option150), configuration filename (option67).

If DHCP server device does not support option150, then you can configure TFTP server address in option66, which is also supported by DHCP Client.

[Command Format]

Ip address dhcp *vlanlist* [**server-ip** *ip-address*] [**schedule-list** *list-no*]

No ip address dhcp

[Parameter]

Ip-address DHCP server IP address

Vlanlist the VLAN that IP address belongs to

Schedule-list set schedule task starting time, ending time, executing interval

[Default]

By default the interface does not acquire IP address through DHCP

[Command Modes]

IP interface configuration mode (only IP 0); privileged user

[Executing Command Instruction]

To use the command, the designated VLAN should have been created,

and the IP interface should belongs to the VLAN, or the interface can not acquire IP address successfully. IP 0 will acquire gateway information and take effect when acquiring IP address. When command line designates the IP address of DHCP Server, it will only acquire the IP address of the designated DHCP Server.

The IP address acquired by DHCP and manual configuration will cover each other.

When IP 0 has acquired IP address through DHCP, if you execute **ip address dhcp vlanlist [server-ip ip-address]**, while the designated VLAN or server-IP is different from the VLAN or server-IP used to acquire IP address, then the interface will release the acquired IP address and start a new application process.

If IP 0 has acquired IP address through DHCP, it will make IP address lease automatically.

What's else, the command can be executed only in IP 0, other interfaces are not supported.

[Explanation of command execution echo]

Acquiring IP address via DHCP

Acquiring IP address successfully

Acquiring IP address unsuccessfully

This interface has been allocated address via DHCP in that vlan with same server

Specified vlan already associated with other interface

Too many vlan set in all interfaces. The max total num is %d

Can not assign ip address for vla %d(cluster)

Invalid server address

%s overlaps with interface %d

Acquiring IP address unsuccessfully

Only interface 0 supports HDCP Client

Enable DHCP Client unsuccessfully. DHCP server or DHCP relay is enabled

Enable DHCP Server unsuccessfully. DHCP client or DHCP snooping is enabled

Enable DHCP relay unsuccessfully. DHCP client or DHCP snooping is enabled

IP address config process is running

[Example]

In IP 0, designated VLAN 1, apply IP address through DHCP

Raisecom(config-ip)#**ip address dhcp 1**

In IP 0, designate VLAN 1, designate DHCP Server 20.168.0.2 applying IP address through DHCP

Raisecom(config-ip)#**ip address dhcp 1 server-ip 20.168.0.2**

[Related commands]

Commands	Description
No address dhcp	In IP 0 release the IP address acquired from DHCP and other information
Ip dhcp client renew	DHCP client lease
Show ip dhcp client	Show DHCP client configuration and acquired information

11.2 ip dhcp client

[Function]

Configure DHCP Client hostname, class-id and client-id under IP interface 0.

[Command Format]

ip dhcp client {hostname *HOSTNAME* | class-id *CLASS-ID* | client-id *CLIENT-ID*} [schedule-list *list-no*]

[Parameter]

HOSTNAME: the hostname;

CLASS-ID: class-id name;

CLIENT-ID: client-id name;

schedule-list: set schedule task start time, finish time, and time interval of periodic operation;

list-no: schedule list number range is <0-99>.

[Default]

HOSTNAME: RaisecomFTTH

CLASS-ID: RaisecomFTTH -ROS_VERSION

CLIENT-ID: RaisecomFTTH -SYSMAC- IF0

Thereinto: ROS_VERSION is ROS platform version; SYSMAC is device MAC address.

[Command Modes]

IP interface configuration mode (for interface 0 only), Privileged user

[Executing Command Instruction]

This command is used for DHCP Client specifying hostname, class-id and client-id. The length of them should not over 32.

[Explanation of command execution echo]

1. Configuration is successfully:

Set successfully

2. Configuration is unsuccessfully:

Set unsuccessfully

3. The input name is too long:

The input name is too long

4. The command is operated not IP interface 0:

Only Interface 0 supports DHCP Client

[Example]

Configuring hostname IP interface 0 to be myhost:

Raisecom(config-ip)# **ip dhcp client hostname** *myhost*

[Related commands]

Commands	Description
no ip dhcp client <i>{hostname / class-id / client-id}</i>	Renew hostname, class-id and client-id to default value.
show ip dhcp client	Show configuration of DHCP Client and obtained information.

11.3 ip dhcp client renew

[Function]

DHCP Client extension. DHCP Client will make extension by automation if users don't operate by force.

[Command Format]

ip dhcp renew [**schedule-list** *list-no*]

[Parameter]

schedule-list: set schedule task start time, finish time, and time interval of periodic operation;

list-no: schedule list number range is <0-99>.

[Default]

Automation extension by DHCP Client is of the same effect as operated by force.

[Command Modes]

IP interface configuration mode (for interface 0 only), Privileged user

[Executing Command Instruction]

This command is valid only if IP interface 0 has obtained IP by DHCP.

[Explanation of command execution echo]

1. Executing this command after IP interface 0 obtained IP by DHCP:

DHCP Client is renewing.

2. IP interface 0 extension successfully/unsuccessfully:

Renew successfully

Renew unsuccessfully

3. The IP interface 0 has not obtained IP or is obtaining IP by DHCP now:

No support of renew operation in this state.

4. The system is running another DHCP Client operation:

Another DHCP Client process is running

5. The command is operated not IP interface 0:

Only Interface 0 supports DHCP Client

[Example]

Extending IP interface 0:

Raisecom(config-ip)# **ip dhcp client renew**

[Related commands]

Commands	Description
----------	-------------

ip address dhcp {1-4094} [server-ip ip-address]	Obtain IP address and other information by DHCP under IP interface 0.
no ip address dhcp	Release the IP obtained by DHCP and other information.
show ip dhcp client	Show configuration of DHCP Client and obtained information.

11.4 ip dhcp information option attach-string

[Function]

Set attached string for Option82 under global configuration mode.

[Command Format]

[no] ip dhcp information option attach-string

[Parameter]

string: value of attach-string

[Default]

By default, the global attach-string is an empty string.

[Command Modes]

Global configuration mode; Privileged user

[Executing Command Instruction]

This command can set sub-option circuit-id of Option82 to be transmitted as attach-string when device is in support of DHCP Snooping or DHCP Relay.

[Explanation of command execution echo]

Set successfully

Show the information for succeeding in configuring attach-string.

Set unsuccessfully

Show the information when fail to configure attach-string.

Attach-string is too long.

Show the information when the attach-string is over 32 bytes.

[Example]

Set attach-string in global configuration mode:

```
Raisecom(config)# ip dhcp information option attach-string raisecom
```

Recover attach-string in global configuration mode:

```
Raisecom(config)# no ip dhcp information option attach-string
```

[Related commands]

Commands	Description
[no]ip dhcp snooping information option	Enable/disable Option82 function by DHCP Snooping under global configuration mode.
[no]ip dhcp relay information option	Enable/disable Option82 function by DHCP Relay under global configuration mode.
show ip dhcp information option	Show configuration of DHCP Option module under privileged EXEC mode.

11.5 ip dhcp information option circuit-id

[Function]

This command is used to set sub-option circuit-id of Option 82 under port. There are three conditions when DHCP request information reaches the port:

Add sub-option circuit-id of Option82 and send it as configured string if Option82 function is enabled Snooping device;

Add Option82 to information that doesn't contain it and send circuit-id as device configured value if Option82 is enabled by Relay device;

According to strategies, information contains Option82 will be discarded or hold if Option82 is enabled by Relay device; or use the configured value to take the place of origin circuit-id in Option82.

[Command Format]

```
ip dhcp information option circuit-id CIRCUIT-ID
```


[no] ip dhcp information option circuit-id

[Parameter]

CIRCUIT-ID: string of circuit ID.

[Default]

The circuit-id string is empty under port mode

[Command Modes]

Port configuration mode, Privileged user

[Executing Command Instruction]

To set circuit ID under port mode by the command **ip dhcp information option circuit-id CIRCUIT-ID**. To delete circuit ID under port mode by the command **no ip dhcp information option circuit-id**.

[Explanation of command execution echo]

Set successfully

Show the information for succeeding in configuring circuit-id.

Set unsuccessfully

Show the information for failing to configure circuit-id.

Circuit-ID is too long.

Show the information when the string of circuit-id over 64 bytes.

[Example]

Set circuit-id string under port mode:

Raisecom(config-port)#**ip dhcp information option circuit-id raisecom**

Recover circuit-id string under port mode:

Raisecom(config-port)# **no ip dhcp information option circuit-id**

[Related commands]

Commands	Description
[no]ip dhcp snooping information option	Enable/disable Option82 function by DHCP Snooping under global configuration mode.
[no]ip dhcp relay information option	Enable/disable Option82 function by DHCP Relay under global configuration mode.
show ip dhcp information option	Show configuration of DHCP Option module under privileged EXEC mode.

11.6 ip dhcp information option remote-id

[Function]

Set mode for sub-option remote-id of Option82 under global configuration mode. Sub-option remote-id of Option82 will be transmitted in setting mode by this command.

[Command Format]

ip dhcp information option remote-id (*switch-mac* /*client-mac*/*switch-mac-string* /*client-mac-string*)

[Parameter]

switch-mac: transmit remote-id in switch MAC (binary system format) address mode;

client-mac: transmit remote-id in client MAC (binary system format) address mode;

switch-mac-string: transmit remote-id in switch MAC string mode;

client-mac-string: transmit remote-id in client MAC string mode.

[Default]

The remote-id is transmitted in binary system format as switch MAC address by default.

[Command Modes]

Global configuration mode, Privileged user

[Executing Command Instruction]

Set mode for sub-option remote-id of Option82 under global configuration mode. Sub-option remote-id of Option82 will be transmitted in setting mode by this command.

[Explanation of command execution echo]

Set successfully

Show the information for succeeding in configuring remote-id.

Set unsuccessfully

Show the information for failing to configure remote-id.

[Example]

Set mode for sub-option remote-id of Option82:

```
Raisecom(config)#ip    dhcp    information    option    remote-id  
switch-mac-string
```

[Related commands]

Commands	Description
[no]ip dhcp snooping information option	Enable/disable Option82 function by DHCP Snooping under global configuration mode.
[no]ip dhcp relay information option	Enable/disable Option82 function by DHCP Relay under global configuration mode.
show ip dhcp information option	Show configuration of DHCP Option module under privileged EXEC mode.

11.7 ip dhcp snooping

[Function]

Enable DHCP Snooping function in global configuration mode. **no ip dhcp snooping** command will stop the function.

[Command Format]

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

[Parameter]

schedule-list: set the start time, over time, period interval of schedule;

list-no: list range <0-99>.

[Default]

DHCP Snooping is disabled

[Command Modes]

Global configuration mode, Privileged EXEC

[Executing Command Instruction]

Enable DHCP Snooping function in global configuration mode. **no ip dhcp snooping** command will stop the function. DHCP Snooping and DHCP Server/Relay are mutually exclusive.

[Explanation of command execution echo]

Enable DHCP Snooping successfully

Enable DHCP Snooping unsuccessfully

Disable DHCP Snooping successfully

Disable DHCP Snooping unsuccessfully

[Example]

Enable DHCP Snooping function in global configuration mode:

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

Disable DHCP Snooping function in global configuration mode:

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

[Related commands]

Commands	Description
show ip dhcp snooping	Show configuration of DHCP Snooping.

11.8 ip dhcp snooping information option

[Function]

Enable and disable DHCP Snooping to support option 82.

[Command Format]

[no] ip dhcp snooping information option [*schedule-list list-no*]

[Parameter]

schedule-list: set the start time, over time, period interval of schedule;

list-no: list range <0-99>.

[Default]

Do not support option 82

[Command Modes]

Privileged EXEC, Global configuration mode

[Executing Command Instruction]

This function can be set in Global configuration mode or Interface configuration mode.

But it can take effect only if DHCP Snooping is enabled.

[Explanation of command execution echo]

Enable DHCP Snooping to support option 82 successfully

Enable DHCP Snooping to support option 82 unsuccessfully

Disable DHCP Snooping from supporting option 82 successfully

Disable DHCP Snooping from supporting option 82 unsuccessfully

[Example]

DHCP Snooping supports Option 82 enable:

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

DHCP Snooping supports Option 82 disable:

Raisecom(config)#**no ip dhcp snooping information option**

[Related commands]

Commands	Description
show ip dhcp snooping	Show configuration information of DHCP Snooping.

11.9 ip dhcp snooping port-list

[Function]

Enable DHCP Snooping function in interface mode. **no ip dhcp snooping port-list** command can disable this function.

[Command Format]

[no] ip dhcp snooping port-list { *all* | *port-list* } [*schedule-list list-no*]

[Parameter]

all: all physical port;

port-list: physical port list ;

schedule-list: set the start time, over time, period interval of schedule;

list-no: list range <0-99>.

[Default]

DHCP Snooping function is enabled.

[Command Modes]

Privileged EXEC, Global configuration mode

[Executing Command Instruction]

ip dhcp snooping port-list command can enable DHCP Snooping function on specify port. **no ip dhcp snooping port-list** command can stop this function.

By default, DHCP Snooping service is enabled on all the interfaces. But it can take effect only if DHCP Snooping is enabled.

[Explanation of command execution echo]

Enable DHCP Snooping successfully

Enable DHCP Snooping unsuccessfully

Disable DHCP Snooping successfully

Disable DHCP Snooping unsuccessfully

[Example]

Enable DHCP Snooping function for specified port:

Raisecom(config)#**ip dhcp snooping port-list 1-10,20**

Disable DHCP Snooping function for specified port:

Raisecom(config)#**no ip dhcp snooping port-list 1-10,20**

[Related commands]

Commands	Description
show ip dhcp snooping	Show configuration information of DHCP Snooping.

11.10 ip dhcp snooping trust

[Function]

DHCP snooping is a DHCP security feature that provides security by filtering distrusted DHCP messages and by building and maintaining a DHCP snooping binding table. An distrusted message is a message that is received from outside the network or firewall and that can cause traffic attacks within your network.

The DHCP snooping binding table contains the MAC address, IP address,

lease time, binding type, VLAN number, and interface information that corresponds to the local distrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An distrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

DHCP snooping acts like a firewall between distrusted hosts and DHCP servers. It also gives you a way to differentiate between distrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

[Command Format]

[no] ip dhcp snooping trust [*schedule-list list-no*]

[Parameter]

schedule-list: set the start time, over time, period interval of schedule;

list-no: list range <0-99>.

[Default]

Untrust

[Command Modes]

Privileged EXEC; Interface configuration mode

[Executing Command Instruction]

Port trust can take effect only if DHCP Snooping in Global configuration mode.

[Explanation of command execution echo]

Set port as DHCP Snooping trusted port successfully

Set port as DHCP Snooping trusted port unsuccessfully

Set port as DHCP Snooping untrusted port successfully

Set port as DHCP Snooping untrusted port unsuccessfully

[Example]

Set port 3 to be DHCP Snooping trusted port:

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

Raisecom(config-port)#**ip dhcp snooping trust**

Set port 3 to be DHCP Snooping untrusted port:

Raisecom(config-port)#**no ip dhcp snooping trust**

[Related commands]

Commands	Description
ip dhcp snooping information option	Enable DHCP Snooping to support option 82
show ip dhcp snooping	Show configuration of DHCP Snooping

11.11 show ip dhcp client

[Function]

Show DHCP Client configuration information and obtained information.

[Command Format]

show ip dhcp client

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

Show DHCP Client configuration and obtained information. The configuration information contains hostname, class-id and client-id and obtained information includes IP address, subnet mask, default gateway, rent client length, start time and expire time, server address, TFTP server

name, TFTP server address and configuration file name.

[Example]

Show DHCP Client configuration information and obtained information:

Raisecom#**show ip dhcp client**

<i>Hostname:</i>	<i>RaisecomFTTH</i>
<i>Class-ID:</i>	<i>RaisecomFTTH -3.5.856</i>
<i>Client-ID:</i>	<i>RaisecomFTTH -000e5e48e596-IF0</i>
<i>Assigned IP Addr:</i>	<i>10.0.0.5</i>
<i>Subnet mask:</i>	<i>255.0.0.0</i>
<i>Default Gateway:</i>	<i>10.0.0.1</i>
<i>Client lease Starts:</i>	<i>Jan-01-2007 08:00:41</i>
<i>Client lease Ends:</i>	<i>Jan-11-2007 11:00:41</i>
<i>Client lease duration:</i>	<i>874800(sec)</i>
<i>DHCP Server:</i>	<i>10.100.0.1</i>
<i>Tftp server name:</i>	<i>TftpServer</i>
<i>Tftp server IP Addr:</i>	<i>10.168.0.205</i>
<i>Startup_config filename:</i>	<i>2109.conf</i>

Note: a) Show below result if IP interface 0 has not startup DHCP Client:

<i>Hostname:</i>	<i>RaisecomFTTH</i>
<i>Class-ID:</i>	<i>RaisecomFTTH -3.5.856</i>
<i>Client-ID:</i>	<i>RaisecomFTTH -000e5e48e596-IF0</i>
<i>DHCP Client is disabled.</i>	

b) Show below result if IP interface 0 is obtaining IP by DHCP Client (the process is not finish yet):

Hostname: RaisecomFTTH

Class-ID: RaisecomFTTH -3.5.856

Client-ID: RaisecomFTTH -000e5e48e596-IF0

DHCP Client is requesting for a lease.

c) Show below result if IP interface 0 fails to apply IP address by DHCP Client:

Hostname: RaisecomFTTH

Class-ID: RaisecomFTTH -3.5.856

Client-ID: RaisecomFTTH -000e5e48e596-IF0

No lease information is available.

d) The contents in blue above are items not supported by DHCP Server. The DHCP Client show 0.0.0.0 in IP address format; and show nothing in string format.

e) if DHCP Server is not in support of option 150 (TFTP server address) and only in support of option 60 (TFTP server name), it is available to configure option 66 as TFTP server address, DHCP Client can also obtain the informatio and show it.

[Related commands]

Commands	Description
ip address dhcp {1-4094} [server-ip ip-address]	Obtain IP address and other information by DHCP under IP interface 0.
no ip address dhcp	Release the IP obtained by DHCP and other information.
ip dhcp client renew	DHCP Client extension.

ip dhcp client { hostname <i>HOSTNAME</i> class-id <i>CLASS-ID</i> client-id <i>CLIENT-ID</i> }	Configure hostname, class-id and client-id to default value.
no ip dhcp client {hostname class-id client-id}	Renew hostname, class-id and client-id to default value.

11.12 show ip dhcp information option

[Function]

Show configuration of DHCP Option module.

[Command Format]

show ip dhcp information option

[Command Modes]

Privileged EXEC, Privileged user

[Explanation of command execution echo]

To show configuration of DHCP Option module:

DHCP Option Config Information

Attach-String: *raisecom rai*

Remote-ID Mode: *switch-mac-string*

Port: *10* *Circuit ID:* *raisecom*

[Example]

Raisecom#**show ip dhcp information option**

[Related commands]

Commands	Description
ip dhcp information attach-string <i>STRING</i>	Set attach-string of Option82 under global configuration mode.
no ip dhcp information option attach-string	Recover default value of attach-string of Option82 under global configuration mode.
ip dhcp information option circuit-id	Set sub-option circuit-id of Option82 under

<i>CIRCUIT-ID</i>	port.
no ip dhcp information option circuit-id	Recover default value for sub-option circuit-id of Option82 under port.
ip dhcp information option remote-id (<i>switch-mac /client-mac</i> <i>/switch-mac-string /client-mac-string</i>)	Set sub-option remote-id mode of Option82 under global configuration mode.

11.13 show ip dhcp snooping

[Function]

Show relative information including the enable state, option 82 and port trust etc.

[Command Format]

show ip dhcp snooping

[Command Modes]

Privileged EXEC, Privileged user

[Example]

Show related configuration information of DHCP Snooping:

Raisecom#**show ip dhcp snooping**

DHCP Snooping: Enabled

Option 82: Enabled

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

<i>1</i>	<i>enabled</i>	<i>yes</i>
----------	----------------	------------

<i>2</i>	<i>enabled</i>	<i>no</i>
----------	----------------	-----------

<i>3</i>	<i>disabled</i>	<i>yes</i>
----------	-----------------	------------

<i>4</i>	<i>enabled</i>	<i>yes</i>
----------	----------------	------------

<i>...</i>	<i>...</i>	<i>...</i>
------------	------------	------------

[Related commands]

Commands	Description
ip dhcp snooping	Enable DHCP Snooping in global configuration mode
ip dhcp snooping port-list	Enable DHCP Snooping in port configuration mode
ip dhcp snooping information option	Enable DHCP Snooping to support option 82
ip dhcp snooping trust	Set trust port for DHCP Snooping

11.14 show ip dhcp snooping binding

[Function]

Use the command to show DHCP Snooping binding table information, the current binding number and history largest binding number. The binding table information includes binding IP address, binding MAC address, binding VLAN and binding ports.

[Command Format]

show ip dhcp snooping binding

[Command Modes]

None

[Example]

Show DHCP Snooping binding table information:

Raisecom#**show ip dhcp snooping binding**

Ip Address	Mac Address	Lease(sec)	Type
VLAN Port			

20.168.0.3	000E.5E00.91E0	1650	dhcp-snooping
1 17			

Current Binding: 1

History Max Binding: 1

Characters	Description
Ip Address	Binding IP address

Mac Address	Binding MAC address
Lease(sec)	Binding table lease left time
Type	Binding type
VLAN	Binding VLAN
Port	Binding port

[Related commands]

Commands	Description
ip dhcp snooping	Enable DHCP Snooping in global configuration mode
ip dhcp snooping port-list	Enable DHCP Snooping in port configuration mode



Chapter 12

IGMP Commands

12.1 clear mvr port statistics

[Function]

Clear MVR port statistics

[Command Format]

Clear mvr port [*portid*] **statistics**

[Parameter]

[*portid*]

[Default]

None

[Command Modes]

Global configuration mode; Privileged user

[Executing Command Instruction]

Use the command to clear MVR port statistics. All the statistics information and REPLACE recorded information will be cleared in the designated port.

[Explanation of command execution echo]

Clear statistics successfully

Clear statistics unsuccessfully

[Example]

Clear MVR port 8 statistics:

Raisecom(config)# **clear mvr port 8 statistics**

[Related commands]

Commands	Description
Show mvr port [<i>portid</i>] statistics	Show MVR statistics based on port

12.2 ip igmp filter vlan

[Function]

Use the defined filter rule on designated VLAN

[Command Format]

ip igmp filter *profile-number* **vlan** *vlanid*

no ip igmp filter vlan *vlanid*

[Parameter]

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

vlanid: vlan ID

[Default]

None

[Command Modes]

Physical port configuration mode; Privileged EXEC.

[Executing Command Instruction]

Use the command to apply the defined filter rule on designated VLAN. The applied filter rule should have been created, of it may cause configuration failure. Use **no ip igmp filter vlan** *vlanlist* to delete the configured filter rule under VLAN.

[Explanation of command execution echo]

Set IGMP filter profile on specify vlan successfully

Set IGMP filter profile on specify vlan unsuccessfully

The IGMP profile does not exist

Delete IGMP filter profile on specify vlan unsuccessfully

[Example]

Apply filter profile on specified VLAN

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

Delete the profile:

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

[Related commands]

Commands	Description
Ip igmp max-group vlan vlanlist	Set maximum group number on designated VLAN
Ip igmp max-group action vlanlist	Set max group action on designated VLAN
Show ip igmp filter vlan [vlanid]	Show VLAN configured filter information

12.3 ip igmp max-groups

[Function]

Set the maximum number for multicast groups.

[Command Format]

ip igmp max-groups *group-number*

no ip igmp max-groups

[Parameter]

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

[Default]

No limitation on max-groups number.

[Command Modes]

Physical port configuration mode; Privileged EXEC.

[Executing Command Instruction]

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

[Explanation of command execution echo]

Set the IGMP max group number on the port successfully

Set the IGMP max group number on the port unsuccessfully

Unlimited the IGMP max group number on the port successfully

Unlimited the IGMP max group number on the port unsuccessfully

[Example]

Set the max-groups of the port permitted to be 10:

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

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

[Related commands]

Commands	Description
show ip igmp filter port	Show the IGMP profile which applied on the port

12.4 ip igmp max-groups action

[Function]

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

[Command Format]

ip igmp max-groups action {deny | replace}

no ip igmp max-groups action

[Parameter]

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

replace: when number of multicast group members exceed max-groups number, original groups member will be replaced. The replace action happens only if the maximum groups is 1.

[Default]

Deny

[Command Modes]

Physical port configuration mode; Privileged EXEC.

[Executing Command Instruction]

Actions to be taken when multicast group number exceeds max-groups number. If there is no limitation on maximum multicast group number, no action will be taken. This limitation is applied for MVR and IGMP snooping.

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

[Explanation of command execution echo]

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

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

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

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

[Example]

Set the maximum multicast group number as 10, action is deny:

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

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

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

[Related commands]

Commands	Description
show ip igmp filter port	Show IGMP profile information which applied on the ports.

12.5 ip igmp querier

[Function]

Enable or disable query function

[Command Format]

ip igmp querier {enable | disable}

no ip igmp max-groups vlan *vlanlist*

[Parameter]

None

[Default]

Default action is **disable**

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Use the command to enable/disable switch query function. **ip igmp querier** is able to enable/disable the function alone, and it can also be under MVR proxy function's control. When you enable MVR proxy function, if query function is enabled at the same time, then when MVR proxy is stopped, query function will be disabled at the same time.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Raisecom(config)#**ip igmp querier enable**

Raisecom(config-port)# **ip igmp querier disable**

[Related commands]

Commands	Description
Mvr proxy	Enable MVR proxy function
Ip igmp querier query-interval <10-65535>	Set query sending interval
MVR proxy query-max-response-time seconds	Set query max-response time

12.6 ip igmp querier query-interval

[Function]

Configure query sending interval

[Command Format]

ip igmp querier query-interval *time*

no ip igmp querier query-interval

[Parameter]

Time –query time interval, unit is second, range is <10-65535>

[Default]

60 seconds

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Set query sending interval. When the command is executed, query will send out general QUERY message in designated interval

[Explanation of command execution echo]

Set query interval successfully

Set query interval unsuccessfully

[Example]

Set query interval to 120s:

Raisecom(config)#**ip igmp querier query-interval 120**

Restore the query time to default value:

Raisecom(config)#**no ip igmp querier query-interval**

[Related commands]

Commands	Description
Mvr proxy	Enable mvr proxy function
Mvr proxy source-ip A.B.C.D	Set query and proxy source IP address
Mvr proxy query-max-response-time seconds	Set query maximum response time
Ip igmp querier {enable disable}	Enable or disable query function
Show mvr proxy	Show proxy configuration

12.7 ip igmp snooping immediate-leave

[Function]

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

[Command Format]

ip igmp snooping immediate-leave

[no] ip igmp snooping immediate-leave

[Default]

IGMP Snooping immediate-leave function is disabled by default.

[Command Modes]

VLAN configuration mode; Privileged EXEC.

[Executing Command Instruction]

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

[Explanation of command execution echo]

Enable IGMP immediate-Leave processing on the VLAN 1 successfully

Enable IGMP Immediate-Leave processing on the VLAN 1 unsuccessfully

Disable IGMP Immediate-Leave processing on the VLAN 1 successfully

Disable IGMP Immediate-Leave processing on the VLAN 1 unsuccessfully

[Example]

Start the IGMP snooping immediate-leave on VLAN1:

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

Stop the IGMP snooping immediate-leave on VLAN1:

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

[Related commands]

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

12.8 ip igmp snooping mrouter

[Function]

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

[Command Format]

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

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

[Command Modes]

Global configuration mode; Privileged EXEC.

[Executing Command Instruction]

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

[Explanation of command execution echo]

Set multicast router port successfully

Set multicast router port unsuccessfully

Set multicast router port successfully

Set multicast router port unsuccessfully

[Example]

Set the IGMP Snooping router port on VLAN 1 manually:

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

Erase the IGMP Snooping router port on VLAN 1 manually:

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

[Related commands]

Commands	Description
----------	-------------

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

12.9 ip igmp snooping timeout

[Function]

Use this command to configure time of IGMP snooping timeout. Use **no ip igmp-snooping timeout** to recover default configuration.

[Command Format]

ip igmp-snooping timeout *timeout*

[no] ip igmp-snooping timeout

[Parameter]

timeout: time of IP IGMP Snooping timeout, integer number range from 30 to 3600(second).

[Default]

Default value of timeout is 300 seconds.

[Command Modes]

Global configuration mode and Privileged EXEC

[Executing Command Instruction]

This command configure valid time of multicast router in IGMP Snooping, multicast route is deleted when timer is overtime. Use **no ip igmp-snooping timeout** to recover default configuration.

[Explanation of command execution echo]

set igmp snooping aging successfully

set igmp snooping aging unsuccessfully

set default igmp snooping aging successfully

set default igmp snooping aging unsuccessfully

[Example]

Set time of IGMP snooping timeout is 3000 seconds:

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

Set time of IGMP snooping timeout is default value:

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

[Related commands]

Commands	Description
show ip igmp snooping	Show IGMP Snooping config information

12.10 ip igmp snooping vlan-list

[Function]

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

[Command Format]

ip igmp snooping vlan-list *vlanlist*

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

[Parameter]

vlanlist: VLAN list, range from 1-4094, format is {1-4094}, Example 2-100,120.

[Default]

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

[Command Modes]

Global configuration mode; Privileged EXEC.

[Executing Command Instruction]

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

[Explanation of command execution echo]

Enable IGMP snooping on VLAN 1 —10 successfully

Enable IGMP snooping on VLAN 1 —10 unsuccessfully

Disable IGMP snooping on VLAN 1 —10 successfully

Disable IGMP snooping on VLAN 1 —10 unsuccessfully

[Example]

Start the IGMP Snooping function on VLAN 1-10 and 12,15:

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

Stop the IGMP Snooping function on VLAN 1-10 and 12:

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

[Related commands]

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

12.11mvr immediate

[Function]

Start the immediate leave function on the port.

[Command Format]

[no] mvr immediate [schedule-list list-no]

[Default]

All the immediate leave function is disabled.

[Command Modes]

Physical port configuration mode; privileged user

[Executing Command Instruction]

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

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

[Explanation of command execution echo]

Enable the Immediate Leave feature of MVR on a port successfully

Enable the Immediate Leave feature of MVR on a port unsuccessfully

Disable the Immediate Leave feature of MVR on a port successfully

Disable the Immediate Leave feature of MVR on a port unsuccessfully.

[Example]

Start the immediate leave function on port 1:

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

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

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

[Related commands]

Commands	Description
show mvr port <i>[portid]</i>	Show MVR port information.

12.12 mvr mode

[Function]

Configure MVR operation mode.

[Command Format]

mvr mode {*dynamic* / *compatible*}

[Parameter]

dynamic: the dynamic mode allows the source ports to be added to multicast group dynamically;

compatible: does not allow dynamic membership joins on source ports.

[Default]

Default mode is **compatible**

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

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

Under the **dynamic** mode, source port join the multicast group

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

[Explanation of command execution echo]

Set MVR mode dynamic successfully

Set MVR mode compatible successfully

Set MVR mode dynamic unsuccessfully

Set MVR mode compatible unsuccessfully

[Example]

Set the MVR mode to dynamic mode:

Raisecom(config)#**mvr mode** *dynamic*

Set the MVR mode to compatible mode:

Raisecom(config)#**mvr mode** *compatible*

[Related commands]

Commands	Description
show mvr	Show MVR configuration information

12.13 mvr proxy

[Function]

Enable/disable MVR proxy function

[Command Format]

Mvr proxy

No mvr proxy

[Parameter]

None

[Default]

Disable

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Use the command to enable MVR proxy function. When it is enabled, MVR message compression function and MVR querier can be started at the same time, and stop at the same time as well. The switch will respond query message from uplink router, and send query message periodically. MVR message compression function and MVR querier function can be enabled and disabled at the same time.

MVR message compression function can be enabled or disabled alone, without the limitation of MVR proxy. If MVR message compression function and MVR querier function are both enabled, MVR proxy will be loaded; if only one of them is enabled, then only MVR proxy suppression or MVR proxy querie will be loaded alone, MVR proxy will not be loaded

[Explanation of command execution echo]

Enable MVR proxy successfully

Enable mvr proxy unsuccessfully

Disable mvr proxy successfully

Disable mvr proxy unsuccessfully

[Example]

Enable MVR proxy

Raisecom(config)#**mvr proxy**

Disable MVR proxy

Raisecom(config)#**no mvr proxy**

[Related commands]

Commands	Description
Mvr proxy suppression	Enable IGMP message suppression function
Ip igmp querier {enable disable}	Enable/disable query function
Show mvr proxy	Show proxy configuration

12.14 mvr proxy last-member-query

[Function]

Set last member query interval

[Command Format]

Mvr proxy last-member-query *time*

No mvr proxy last-member-query

[Parameter]

Time- the last member query time (second), range is <1-25>

[Default]

1s

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Set last member sending query interval. When the last group user leaves, or when the group is out of time, a specified group query will be sent. If there

is no report message received in last-member-query time, the group will be deleted

[Explanation of command execution echo]

Set last time query time successfully

Set last time query time unsuccessfully

[Example]

Set last-member-query time to 10s

Raisecom(config)#**mvr proxy last-member-query 10**

Restore the time to default value

Raisecom(config)#**no mvr proxy last-member-query**

[Related commands]

Commands	Description
Mvr proxy	Enable mvr proxy function
Mvr proxy source-ip A.B.C.D	Set query sending interval
Ip igmp querier query-interval <10-65535>	Set query sending interval
Mvr proxy query-max-response-time	Set query maximum response time
Ip igmp querier {enable disable}	Enable or disable query function
Show mvr proxy	Show proxy configuration

12.15 mvr proxy query-max-response-time

[Function]

Set query maximum response time

[Command Format]

Mvr proxy query-max-response-time *time*

No mvr proxy query-max-response-time

[Parameter]

Time- the maximum response time (second), range is <1-25>

[Default]

10s

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Set query maximum response time

[Explanation of command execution echo]

Set query max response time successfully

Set query max response time unsuccessfully

[Example]

Set query max response time to 20s

Raisecom(config)#**mvr proxy query-max-response-time 20**

Restore response time to default value

Raisecom(config)#**no mvr proxy query-max-response-time**

[Related commands]

Commands	Description
Mvr proxy	Enable mvr proxy function
Mvr proxy source-ip A.B.C.D	Set query sending interval
Ip igmp querier query-interval <10-65535>	Set query sending interval
Mvr proxy last-member-query	Set last member query interval
Ip igmp querier {enable disable}	Enable or disable query function
Show mvr proxy	Show proxy configuration

12.16 mvr proxy source-ip

[Function]

Configure query and proxy source IP address

[Command Format]

Mvr proxy source-ip A.B.C.D

No mvr proxy source-ip

[Parameter]

A.B.C.D – source IP address

[Default]

Use IP interface 0 IP address, if there is no configuration in IP interface 0, use 0.0.0.0

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Designate the source IP address of mvr proxy packets. If not configured, use IP interface 0 IP address, if there is no configuration in IP 0, use 0.0.0.0

According to RFC1166 and CISCO device, the limit to configure IP is shown below:

A 0.0.0.0	Reserved
1.0.0.0 to 126.0.0.0	Available
127.0.0.0	Reserved
B 128.0.0.0 to 191.254.0.0	Available
191.255.0.0	Reserved
C 192.0.0.0	Reserved

192.0.1.0 to 223.255.254

Available

223.255.255.0

Reserved

[Explanation of command execution echo]

Set source ip address successfully

Set source ip address unsuccessfully

Delete source ip address successfully

Delete source ip address unsuccessfully

[Example]

Set query and proxy source IP address

Raisecom(config)#**mvr proxy source-ip** 192.168.0.1

Delete querier and proxy source IP address

Raisecom(config)#**no mvr proxy source-ip**

[Related commands]

Commands	Description
Mvr proxy	Enable mvr proxy function
Mvr proxy source-ip A.B.C.D	Set query sending interval
Ip igmp querier query-interval <10-65535>	Set query sending interval
Mvr proxy last-member-query	Set last member query interval
Ip igmp querier {enable disable}	Enable or disable query function
Show mvr proxy	Show proxy configuration

12.17 mvr proxy suppression

[Function]

Enable/disable IGMP message suppression function

[Command Format]

Mvr proxy suppression

No mvr proxy suppression

[Parameter]

None

[Default]

Disable

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Use the command to enable/disable IGMP message suppression function. The function can be enabled or disabled dependently, and it can be controlled by MVR proxy function as well, when MVR proxy function is enabled, if MVR message suppression function is not enabled while IGMP message suppression function is enabled, then when stopped, IGMP message suppression will be disabled as well

[Explanation of command execution echo]

Enable IGMP message suppression successfully

Enable IGMP message suppression unsuccessfully

Disable IGMP message suppression successfully

Disable IGMP messge suppression unsuccessfully

[Example]

Enable MVR proxy

Raisecom(config)#**mvr proxy suppression**

Disable MVR proxy

Raisecom(config)#**no mvr proxy suppression**

[Related commands]

Commands	Description
----------	-------------

Mvr proxy	Enable mvr proxy function
Show mvr proxy	Show proxy configuration

12.18 mvr timeout

[Function]

Configure time of MVR timeout.

[Command Format]

mvr timeout *timeout*

no mvr timeout

[Parameter]

timeout: maximum overtime for MVR multicast address, range from 60~36000(second), default is 600 seconds.

[Default]

Default is 600 seconds.

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

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

[Explanation of command execution echo]

Set MVR timeout successfully

Set MVR timeout unsuccessfully

Set default MVR timeout successfully

Set default MVR timeout unsuccessfully

[Example]

Set the timeout to 180 seconds:

Raisecom(config)#**mvr timeout 180**

Recover to default setting:

Raisecom(config)#**no mvr timeout**

[Related commands]

Commands	Description
show mvr	Show MVR configuration information

12.19 **mvr type**

[Function]

Configure MVR port type.

[Command Format]

mvr type {*source* / *receiver*}

no mvr type

[Parameter]

source: specify the port as the source port, which is the port connected to the multicast router;

receiver: specify the port as the receiving port.

[Default]

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

[Command Modes]

Physical port configuration mode; privileged user.

[Executing Command Instruction]

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

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

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

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

[Explanation of command execution echo]

Set MVR port type as source port successfully

The source port is not in multicast VLAN, set unsuccessfully

Set MVR port type as source port unsuccessfully

Set MVR port type as receiver port successfully

The port has been in multicast VLAN, set unsuccessfully

Set MVR port type as receiver port unsuccessfully

[Example]

Set port 1 as receiving port:

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

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

Set port 1 as the source port:

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

Se the port 1 as the non-MVR port:

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

[Related commands]

Commands	Description
show mvr port [<i>portid</i>]	Show MVR port information

12.20 mvr vlan

[Function]

Configure multicast VLAN of MVR.

[Command Format]

mvr vlan *vlanid* [**schedule-list** *list-no*]

no mvr vlan

[Parameter]

vlanid: specify the VLAN that needs to receive the multicast data. Range is 1~4094, default is VLAN 1.

[Default]

Default is VLAN 1.

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

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

[Explanation of command execution echo]

Set the VLAN in which multicast data is received successfully

Set the VLAN in which multicast data is received unsuccessfully

Set the default VLAN in which multicast data is received successfully

Set the default VLAN in which multicast data is received unsuccessfully

[Example]

Set the multicast VLAN to 2:

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

Recover the default setting:

Raisecom(config)#**no mvr vlan**

[Related commands]

Commands	Description
show mvr	Show MVR configure information.

12.21 mvr vlan group

[Function]

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

[Command Format]

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

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

[Parameter]

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

ip-address: the type of class-map, apply AND operation between matches.

Default is match-all.

[Command Modes]

Physical port configuration mode; privileged user.

[Executing Command Instruction]

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

[Explanation of command execution echo]

Specify MVR group IP multicast address for specified VLAN ID successfully

Specify MVR group IP multicast address for specified VLAN ID unsuccessfully

Delete MVR group IP multicast address for specified VLAN ID successfully

Delete MVR group IP multicast address for specified VLAN ID unsuccessfully

MVR group address isn't class D address.

Invalid multicast VLAN

The input name too long.

Non MVR group cannot be added

[Example]

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

Raisecom(config)#**mvr enable**

Raisecom(config)#**mvr vlan 3**

Raisecom(config)#**mvr group 234.5.6.1 10**

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

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

Raisecom(config-port)#**mvr vlan 3 group 234.5.6.7**

Delete configuration:

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

[Related commands]

Commands	Description
show mvr port [<i>portid</i>]	Show MVR port information
show mvr port [<i>portid</i>] member	Show MVR port member information.

12. 22 permit | deny

[Function]

Set action of IGMP profile as permit or deny.

[Command Format]

{permit | deny}

[Parameter]

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

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

[Default]

The default operation is deny.

[Command Modes]

Profile configuration mode; Privileged user.

[Executing Command Instruction]

Set the operation of IGMP profile to permit or deny.

[Explanation of command execution echo]

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

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

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

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

Set the action to access to the IP multicast address unsuccessfully

[Example]

Set IGMP profile operation:

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

Raisecom(config-profile)#**permit**

[Related commands]

Commands	Description
ip igmp profile <i>profile-number</i>	Create IGMP profile.
show ip igmp profile	Show IGMP profile configuration information.

12. 23 range

[Function]

Set the address range for IGMP profile.

[Command Format]

[no] range *start-ip [end-ip]*

[Parameter]

start-ip: the starting address of the address range for IGMP profile.

end-ip: the ending address of the address range for IGMP profile.

[Default]

Default scale is all the multicast address.

[Command Modes]

profile configuration mode; privileged user.

[Executing Command Instruction]

Set the address range for IGMP profile, if do not specify the ending address, it stands for an IP address. Use **no range** *start-ip [end-ip]* to delete the range.

[Explanation of command execution echo]

Set the range of IP multicast addresses successfully

Set the range of IP multicast addresses unsuccessfully

Delete the range of IP multicast address successfully

Delete the range of IP multicast address unsuccessfully

Not an IP multicast group address

Invalid group address

[Example]

Set the range of IGMP profile from 234.5.6.7 to 234.5.7.7:

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

Raisecom(config-profile)#**permit**

Raisecom(config-profile)#**range** *234.5.6.7 234.5.7.7*

Delete the range of IGMP profile from 234.5.7.0 to 234.5.7.7:

Raisecom(config-profile)#**no range** *234.5.7.0 234.5.7.7*

[Related commands]

Commands	Description
ip igmp profile <i>profile-number</i>	Create IGMP profile.
{ permit deny }	Set IGMP profile action.
show ip igmp profile	Show IGMP profile configuration information.

12.24 show ip igmp filter

[Function]

Show IGMP filter configuration information.

[Command Format]

show ip igmp filter

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Use this command to show global configuration information which is IGMP filtered.

[Explanation of command execution echo]

Raisecom# **show ip igmp filter**

IGMP filter: Enable

[Example]

Raisecom# **show ip igmp filter**

[Related commands]

Commands	Description
ip igmp filter	Enable or disable IGMP filter function.

12.25 show ip igmp filter port

[Function]

Show the port configuration information of IGMP filter.

[Command Format]

Show ip igmp filter port [*portid*]

[Parameter]

portid: (optical), port number.

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Use this command to show port config information, which is IGMP filtered, if the parameter is not specified, show information for all the ports.

Filter represents that which IGMP profile is applied by the port. If it is 0, the port doesn't apply any IGMP profile.

[Explanation of command execution echo]

Show all the ports:

Raisecom#**show ip igmp filter port**

Port	Filter	Max Groups	Current Groups	Action

1	1	20	0	Deny
2	2	20	0	Deny

3	0	0	0	Deny
.....				
25	0	0	0	Deny
26	0	0	0	Deny

Show specified port:

Raisecom#**show ip igmp filter port 1**

IGMP Filter: 1

Max Groups: 20

Current groups: 0

Action: Deny

[Example]

Raisecom# **show ip igmp filter port 1**

[Related commands]

Commands	Description
ip igmp profile <i>profile-number</i>	Create IGMP profile information
ip igmp max-groups	The maximum number which is allowed to be added into group.
ip igmp max-groups action	The action is taken when the number of group added exceeds the allowed maximum number.

12.26 show ip igmp filter vlan

[Function]

Show MVR configuration

[Command Format]

Show ip igmp filter vlan [*vlanid*]

[Parameter]

vlanid , vlan number.

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Use the command to show filter information under VLAN

[Explanation of command execution echo]

1.

Router# show ip igmp filter vlan

VLAN	Filter	Max Groups	Current Groups	Action

1	22	512	10	drop
10	23	10	5	replace

2.

Router# show ip igmp filter vlan 1

VLAN	Filter	Max Groups	Current Groups	Action

1	22	512	10	drop

[Example]

Raisecom# **show ip igmp filter vlan**

[Related commands]

Commands	Description
ip igmp max-group vlan	On designated VLAN set the max group
vlanlist	number
ip igmp max-group action	On the designated VLAN set max group
vlanlist	number action
ip igmp filter profile vlan	On designated VLAN apply the defined filter
vlanlist	rule

12.27 show ip igmp profile

[Function]

Show the configuration information of IGMP profile.

[Command Format]

show ip igmp profile [*profile-number*]

[Parameter]

profile-number: optional, already defined IGMP profile number.

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Use this command to show IGMP profile configuration information.

When the parameter has not been specified, show all the already defined IGMP profile information.

[Explanation of command execution echo]

Show all the information:

Raisecom#**show ip igmp profile**

IGMP profile 1

permit

range 234.1.1.1 234.2.2.2

range 234.5.1.1 234.5.2.2

IGMP profile 2

Deny

range 234.1.1.1 234.2.2.2

range 234.5.1.1 234.5.2.2

Show designated ip igmp information:

Raisecom#**show ip igmp profile 1**

IGMP profile 1

permit

range 234.1.1.1 234.2.2.2

range 234.5.1.1 234.5.2.2

[Example]

Raisecom# **show ip igmp profile**

[Related commands]

Commands	Description
ip igmp profile <i>profile-number</i>	Create IGMP profile information
permit deny	Set IGMP profile action
range <i>start-ip [end-ip]</i>	Set IGMP profile range.

12. 28 show ip igmp snooping

[Function]

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

vlanid:VLAN ID range form 1 to 4094.

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

show ip igmp snooping show IGMP snooping state and particular VLAN state.

show ip igmp snooping mrouter show dynamic learning or manual configuration information of multi-cast router port.

show ip igmp snooping vlan *vlanid* show the state of particular VLAN.

show ip igmp snooping mrouter vlan *vlanid* show multicast router port information of designated VLAN.

If do not specify VLAN, show all the VLAN information.

[Example]

Show IGMP snooping configuration information:

Raisecom# **show ip igmp snooping**

IGMP snooping: Enable

IGMP snooping aging time: 50s

IGMP snooping active vlan: 1

IGMP snooping immediate-leave active vlan: --

Show all the multicast router information of all the VLAN:

Raisecom# **show ip igmp snooping mrouter**

<i>Ip Address</i>	<i>Port</i>	<i>VLAN</i>	<i>Age</i>	<i>Type</i>
-------------------	-------------	-------------	------------	-------------

Show IGMP snooping configuration information of VLAN 1:

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

IGMP snooping: Enable

IGMP snooping aging time: 50s

IGMP snooping on Vlan 1: Enable.

IGMP snooping immediate-leave on Vlan 1: Disable.

Show IGMP snooping multicast router information of VLAN 1:

Raisecom#**show ip igmp snooping mrouter vlan 1**

IGMP snooping: Enable

IGMP snooping aging time: 50s

IGMP snooping on Vlan 1: Enable.

IGMP snooping immediate-leave on Vlan 1: Disable.

12. 29 show mvr

[Function]

Show MVR configuration information.

[Command Format]

show mvr

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Use this command to show MVR global configuration information.

[Explanation of command execution echo]

Raisecom#**show mvr**

MVR Running: Enable

MVR Multicast VLAN: 1

MVR Max Multicast Groups: 256

MVR Current Multicast Groups: 0

MVR Timeout: 600 (second)

MVR Mode: Compatible

[Example]

Raisecom# **show mvr**

[Related commands]

Commands	Description
mvr { <i>enable</i> / <i>disable</i> }	Start/stop MVR
mvr vlan <i>vlanid</i>	Set multicast VLAN
mvr mode { <i>dynamic</i> / <i>compatible</i> }	Set MVR mode.
mvr group	Set MVR multicast group

12.30 show mvr member

[Function]

Show MVR configuration multicast group information.

[Command Format]

show mvr member [*ip-address*]

[Parameter]

ip-address: show designated IP group information, the IP address should be IP address of D type, format is A.B.C.D.

[Command Modes]

Privileged user; Privileged EXEC.

[Executing Command Instruction]

Show MVR configuration multicast group information.

MVR group state Active means there is port been added into this group (statistic or dynamic); Inactive means no port is added into the group.

Members item means the ports that have been added into this group, shows none if no ports been added.

[Explanation of command execution echo]

Raisecom#**show mvr members**

MVR Group IP Status Members

234.5.6.7	Active	1
234.5.6.8	Active	1
234.5.6.9	Inactive	None
234.5.6.10	Inactive	None
234.5.6.11	Inactive	None

[Example]

Raisecom# **show mvr members**

[Related commands]

Commands	Description
mvr {enable / disable}	Start /stop MVR
mvr group	Set MVR multicast group.

12.31 show mvr port

[Function]

Show MVR port configuration information.

[Command Format]

show mvr port [portid]

[Parameter]

portid: port ID.

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Show MVR port configuration information.

“running” stand for whether the port has started the MVR.

“type” stands for port MVR type, there are three types: non-MVR, source, receiver;

up/down stands for the connection status for the ports, active stands for the port belongs to a VLAN; inactive stands for the port is not belongs to a VLAN.

Immediate leave stand for whether the port is started or not.

[Explanation of command execution echo]

Show all the port information:

Raisecom#**show mvr port**

<i>Port</i>	<i>Running</i>	<i>Type</i>	<i>Status</i>	<i>Immediate Leave</i>

<i>1</i>	<i>Enable</i>	<i>Receiver</i>	<i>Inactive/down</i>	<i>Enable</i>
<i>2</i>	<i>Disable</i>	<i>Non-MVR</i>	<i>Inactive/down</i>	<i>Disable</i>
<i>3</i>	<i>Disable</i>	<i>Non-MVR</i>	<i>Inactive/down</i>	<i>Disable</i>
<i>4</i>	<i>Disable</i>	<i>Non-MVR</i>	<i>Inactive/down</i>	<i>Disable</i>
<i>5</i>	<i>Disable</i>	<i>Non-MVR</i>	<i>Inactive/down</i>	<i>Disable</i>
<i>6</i>	<i>Disable</i>	<i>Non-MVR</i>	<i>Inactive/down</i>	<i>Disable</i>
<i>7</i>	<i>Disable</i>	<i>Non-MVR</i>	<i>Inactive/Up</i>	<i>Disable</i>
.....				
<i>25</i>	<i>Disable</i>	<i>Non-MVR</i>	<i>Inactive/down</i>	<i>Disable</i>
<i>26</i>	<i>Disable</i>	<i>Non-MVR</i>	<i>Inactive/down</i>	<i>Disable</i>

Show individual port information:

Raisecom#**show mvr port 1**

Running: Enable

Type: Receiver

Status: Inactive/down

Immediate Leave: Enable

[Example]

Show all the port information:

```
Raisecom# show mvr port
```

Show designated port information:

```
Raisecom# show mvr port 1
```

[Related commands]

Commands	Description
mvr { <i>enable</i> / <i>disable</i> }	start/stop MVR
mvr vlan <i>vlanid</i>	Set multicast VLAN
mvr group	Set MVR multicast group.
mvr type { <i>source</i> / <i>receiver</i> }	Configure port MVR type.
mvr immediate	Configure immediate leave.
mvr vlan <i>vlanid</i> group <i>ip-address</i>	Configure port to static multicast group member.

Chapter 13

RMON Commands

13.1 clear rmon

[Function]

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

[Command Format]

clear rmon

[Command Modes]

Global configuration mode

[Executing Command Instruction]

Clear RMON configuration and recover to default configuration.

[Explanation of command execution echo]

Set successfully

[Example]

Raisecom(config)#**clear rmon**

13.2 rmon alarm

[Function]

Use add rmon alarm entries, use **no** format to delete.

[Command Format]

rmon alarm <1-512> MIBVAR [interval <1-3600>] {delta | absolute}
rising-threshold <1-65535>₁ [<1-65535>₂] **falling-threshold**
<0-2147483647>₃ [<1-65535>₄] [**owner** STRING]

no rmon alarm <1-512>

[Parameter]

<1-512>: Index number;

MIBVAR: the MIB variable which should be remotely monitored;

Interval: check the MIB variable time period;

<1-3600>: the time period for checking MIB variable (unit is second);

delta: check between the change for MIB variables;

absolute: check the absolute value for MIB;

rising-threshold: upper threshold value for MIB variable;

<1-65535>1: upper threshold value for MIB variable;

<1-65535>2: rising-threshold associated index;

falling-threshold: lower threshold value for MIB variable;

<0-2147483647>3: lower threshold value for MIB variable;

<1-65535>4: falling-threshold associated MIB variable;

owner: Alarm table associated owner;

STRING: owner characters.

[Default]

Default polling time period is 2s.

Default owner is config.

[Command Modes]

Global configuration mode

[Executing Command Instruction]

MIBVAR should be decimal dotted; this command should be efficient MIB variable and can be monitored, otherwise the MIB variable can not be monitored. Use **no rmon alarm <1-512>** command to delete associated Alarm.

[Explanation of command execution echo]

Wrong Mib variable format!

Wrong MIB variable!

Owner name is too long!

Set successfully.

Set unsuccessfully

[Example]

Set alarm 10, use it to monitor MIB variable 1.3.6.1.2.1.2.2.1.20.1, every 20 seconds, check the value whether it is rising or falling. If rise 15, Example rise from 10000 to 10015, spring alarm:

```
Raisecom(config)#rmon alarm 10 1.3.6.1.2.1.2.2.1.20.1 interval 20  
delta rising-threshold 15 1 falling-threshold 1 owner Johnson
```

[Related commands]

Commands	Description
show rmon alarm	Show rmon alarm table.

13.3 rmon event

[Function]

Use this command to add RMON event table, **no** command is used to delete the operation.

[Command Format]

```
rmon event <1-65535> [log] [trap] [ 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;

description: description;

STRING: description string;

owner: owner;

STRING: string of owner.

[Default]

The default community name is public.

The default description string is null.

The default owner is config.

[Command Modes]

Global configuration mode

[Executing Command Instruction]

Use the command to add and set the attribute of event.

[Explanation of command execution echo]

Description is too long!

Owner name is too long!

Set successfully.

Set unsuccessfully

[Example]

RMON event table:

Raisecom(config)#**rmon event 1 trap owner private**

[Related commands]

Commands	Description
Show rmon event	show RMON EVENT table.

13.4 rmon history

[Function]

Start the history statistical group function for some port; **no** format command is used to stop the function.

[Command Format]

rmon history {0-14} [shortinterval <1-600>] [longinterval <600-3600>] [buckets <10-1000>] [owner STRING]

no rmon history ip {0-14}

rmon history line {1-"MAX_LINE_STR"} [client {1-"MAX_CLIENT_STR"}] [shortinterval <1-600>] [longinterval <600-3600>] [buckets <10-1000>] [owner STRING]

rmon history client {1-"MAX_CLIENT_STR"} [shortinterval <1-600>] [longinterval <600-3600>] [buckets <10-1000>] [owner STRING]

no rmon history line {1-"MAX_LINE_STR"} [client {1-"MAX_CLIENT_STR"}]

no rmon history client {1-"MAX_CLIENT_STR"}

[Parameter]

ip: layer 3 port;

0-14: layer 3 port from 0-14;

port: physical port;

1-26: physical port, range is 1-26;

shortinterval: short polling interval time;

1-600: the short polling interval, range is 1-600, unit is second;

longinterval: long polling interval time;

600-3600: long time polling interval, range is 600-3600, unit is second;

buckets: history group data storage queue;

10-1000: the range for history group data storage queue is 10-1000;

owner: owner;

STRING: string of owner.

[Default]

Default short sampling time period is 30s.

Default long sampling time period is 1800s.

Default value for history group data storage queue is 10.

Default owner value is monitorHistory.

[Command Modes]

Global configuration mode

[Explanation of command execution echo]

Owner name is too long!

Set successfully.

Set unsuccessfully

[Example]

Start history statistic group function from IP interface 1 to 9:

```
Raisecom(config)#rmon history ip 1-9 shortinterval 60 buckets 50  
owner raisecom
```

Start physical interface 1-5, 10-18 and 25 history statistic group function:

Raisecom(config)#**rmon history port 1-5,10-18,25 shortinterval 60
longinterval 500 buckets 50 owner test**

[Related commands]

Commands	Description
show rmon history	Show the configuration result and information of history statistical group.

13.5 rmon statistic

[Function]

Start the statistical group function for particular port, **no** format command is used to stop the function.

[Command Format]

rmon statistics ip {0-14} [owner STRING]

rmon statistics line {1-"MAX_LINE_STR"} [client {1-"MAX_CLIENT_STR"}] [owner STRING]

rmon statistics client {1-"MAX_CLIENT_STR"} [owner STRING]

no rmon statistics ip {0-14}

no rmon statistics line {1-"MAX_LINE_STR"} [client {1-"MAX_CLIENT_STR"}]

no rmon statistics client {1-"MAX_CLIENT_STR"}

[Parameter]

ip: layer 3 port ;

0-14: layer 3 port from 0-14 ;

port-list: physical port ;

1-26: physical port, range is 1-26;

owner: owner;

STRING: string of owner.

[Default]

Owner default value is monitorStatistics.

[Command Modes]

Global configuration mode

[Explanation of command execution echo]

Owner name is too long !

Set successfully.

Set unsuccessfully

[Example]

Start statistic group function from IP interface 1 to 9:

Raisecom(config)#**rmon statistics ip 1-9 owner raisecom**

Start physical interface 1-5, 10-18 and 25 history statistic group function:

Raisecom(config)#**rmon statistics port 1-5,10-18,25 owner test**

[Related commands]

Commands	Description
show rmon statistics	Show configuration result and information of statistical group.

13.6 show rmon

[Function]

Show RMON module information

[Command Format]

show rmon [alarms|events|statistics[ip ipid|line lineid|client clientid]

[history[ip ipid|port portid]]

[Parameter]

Privileged EXEC mode; privileged user

[Instruction]

show rmon Type the information when RMON configuration is empty.

show rmon alarms Type the information when RMON alarm group configuration is empty.

show rmon events Type the information when RMON event group configuration is empty.

show rmon statistics[ip ipid|line lineid|client clientid] Type the information when RMON statistic information group is empty.

show rmon history [ip ipid|port portid] Type the information when RMON history information is empty.

[Explanation of command execution echo]

Ref. RFC 1757 for more detailed RMON statistic table information.

[Example]

Show RMON configuration table information

Raisecom#show rmon

Alarm group information:

Alarm 1 is active, owned by test

Monitors 1.3.6.1.2.1.2.2.1.5.1 every 100 seconds

Taking absolute samples, last value was 0

Rising threshold is 1000, assigned to event 1

Falling threshold is 10, assigned to event 2

On startup enable rising and falling alarm

Event group information:

Event 1 is active, owned by monitorEvent

Event generated at 0:0:0

Send TRAP when event is fired.

Statistics group information:

Physical port 2 is active, and owned by monitorEtherStats

Which has received

0 octets, 0 packets,

0 broadcast, 0 multicast packets,

0 undersized, 0 oversized packets,

0 fragments, 0 jabbers,

0 CRC alignment errors, 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

Physical port 3 is active, and owned by monitorEtherStats

Which has received

58003 octets, 900 packets,

5 broadcast, 895 multicast packets,

0 undersized, 0 oversized packets,

0 fragments, 0 jabbers,

0 CRC alignment errors, 0 collisions.

of dropped packet events (due to lack of resources): 0

of packets received of length (in octets):

64: 839, 65-127: 60, 128-255: 0,

256-511: 1, 512-1023: 0, 1024-1518:0

L3 Interface 0 is active, and owned by monitorEtherStats

Which has received

0 octets, 0 packets,

0 broadcast, 0 multicast packets,

0 undersized, 0 oversized packets,

0 fragments, 0 jabbers,

0 CRC alignment errors, 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

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

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.

Raisecom#show rmon statistics

Interface 2 is active, and owned by monitorEtherStats

Monitors 1.3.6.1.2.1.2.2.1.1.17825795(ifEntry.1.17825795),which has

Received 0 octets, 0 packets,

0 broadcast and 0 multicast packets,

0 undersized and 0 oversized packets,

0 fragments and 0 jabbers,

0 CRC alignment errors and 0 collisions.

#of dropped packet events (due to lack of resources): 0

#of packets received of length (in octets):

64: 0, 65-127: 0, 128-255: 0,

256-511: 0, 512-1023: 0, 1024-1518:0

Raisecom(config)#show rmon history

=====
=====

Entry index is 5, and owned by monitorHistory

Sample data from interface:

1.3.6.1.2.1.2.2.1.1.3(ifTable.3)

Sample every 30 seconds

Request number of buckets: 10

Granted number of buckets: 10

Sample number: 192, System time of the current Sample 3:25:12

Data Sample List

Octets	Packets	Broadcast	Multicast	Undersized	Oversized	

0	0	0	0	0	0	

Fragments	Packets	CRC Err	Collisions	DropEvents	Utilization	

0	0	0	0	0	0	

Sample number: 193, System time of the current Sample 3:26:2

Data Sample List

Octets	Packets	Broadcast	Multicast	Undersized	Oversized	

9136	138	9	129	0	0	

Fragments	Packets	CRC Err	Collisions	DropEvents	Utilization	

0	0	0	0	0	0	

=====

=====

Entry index is 6, and owned by monitorHistory

Sample data from interface:

1.3.6.1.2.1.2.2.1.1.3(ifTable.3)

Sample every 1800 seconds

Request number of buckets: 10

Granted number of buckets: 10

Sample number: 1, System time of the current Sample 0:46:34

Data Sample List

Octets	Packets	Broadcast	Multicast	Undersized	Oversized	

249936	3877	25	3852	0	0	

Fragments	Packets	CRC Err	Collisions	DropEvents	Utilization	

0	0	0	0	0	0	

Sample number: 2, System time of the current Sample 1:36:24

Data Sample List

Octets	Packets	Broadcast	Multicast	Undersized	Oversized	

|250759 |3884 |32 |3852 |0 |0
|

| Fragments| Packets| CRC Err | Collisions | DropEvents |Utilization|

|0 |0 |0 |0 |0 |0 |

Sample number: 3, System time of the current Sample 2:26:14

Data Sample List

| Octets | Packets | Broadcast | Multicast | Undersized | Oversized |

|250002 |3878 |25 |3853 |0 |0
|

| Fragments| Packets| CRC Err | Collisions | DropEvents |Utilization|

|0 |0 |0 |0 |0 |0
|

[Related commands]

Command	Description
show rmon alarms	Show RMON alarms table information

show rmon events	Show RMON events table information
show rmon history	Show RMON history table information

show rmon statistics	Show RMON statistics table information
---------------------------------	--

Chapter 14 ARP Management Commands

14.1 arp

[Function]

Add new table item of ARP mapping table, no format command can cancel operation.

[Command Format]

arp *ip-address mac-address*

[Parameter]

ip-address: IP address, in format of dotted decimal numeral, like A.B.C.D;

mac-address: hardware address, in format of HHHH.HHHH.HHHH.

[Command Modes]

Global configuration mode, Privileged EXEC

[Executing Command Instruction]

ARP table is maintained by dynamic ARP protocol. ARP searches the resolving result of IP address that maps to MAC address. It is automatic. When it is required to add static ARP entries, manually operation of ARP table is required. The IP address of static added ARP table should belong to IP network segment of switch layer-3.

Use **no arp** *ip-address* to delete ARP entries both dynamic and static.

[Explanation of command execution echo]

set successfully!

Adding static ARP entry successfully.

set unsuccessfully

Adding static ARP entry unsuccessfully.

[Example]

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

```
Raisecom(config)#arp 10.0.0.1 0050.8d4b.fd1e
```

Delete ARP entry which IP address is 10.0.0.1 in ARP table:

```
Raisecom(config)# no arp 10.0.0.1
```

[Related commands]

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

14.2 clear arp

[Function]

Clear all entries of ARP table.

[Command Format]

```
clear arp [schedule-list list-no]
```

[Parameter]

schedule-list: set start time, finish time and periodic time interval of schedule task;

list-no: schedule list range: <0-99>.

[Command Modes]

Global configuration mode and Privileged user

[Executing Command Instruction]

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

[Explanation of command execution echo]

set successfully!

Clear ARP entries successfully.

set unsuccessfully

Clear ARP entries unsuccessfully.

[Example]

Clear ARP table:

Raisecom(config)#**clear arp**

[Related commands]

Commands	Description
arp	Add a static MAC address entries.
show arp	Show all entries of ARP table.

14.3 show arp

[Function]

Show the item of ARP mapping table.

[Command Format]

show arp

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

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

[Explanation of command execution echo]

Display the information as below when **show arp** command executing successfully:

arp table aging-time is 6000 seconds(default:1200s)

ARP mode: Learn reply only:

<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>

Total: 3

Static: 1

Dynamic: 2

[Example]

Show ARP table:

Raisecom#**show arp**

[Related commands]

Commands	Description
arp	Add a static MAC address table.
arp mode { <i>learn-all</i> / <i>learn-reply-only</i> }	Set ARP dynamic learning mode.
clear arp	Clear up all the items in ARP address mapping table.

Chapter 15 SNMP Commands

15.1 show snmp access

[Function]

Use **show snmp access** to show snmp access group information.

[Command Format]

show snmp access

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Show snmp access group information.

[Example]

Show snmp access group information:

Raisecom#**show snmp access**

Index: 0

Group: initial

Security Model: usm

Security Level: authnopriv

Context Prefix: --

Context Match: exact

Read View: internet

Write View: internet

Notify View: internet

Index: 2

Group: *initialnone*

Security Model: *usm*

Security Level: *noauthnopriv*

Context Prefix: *--*

Context Match: *exact*

Read View: *system*

Write View: *--*

Notify View: *internet*

[Related commands]

Commands	Description
snmp-server access	Add or modify access control group.
no snmp-server access	Delete access control group.

15.2 show snmp community

[Function]

Use **show snmp community** to show the community information of snmp protocol.

[Command Format]

show snmp community

[Command Modes]

Privileged EXEC, privileged user

[Executing Command Instruction]

Use **show snmp community** to show the community information of snmp protocol.

[Example]

Show the community information of snmp protocol :

Raisecom#**show snmp community**

<i>Index</i>	<i>Community Name</i>	<i>View Name</i>	<i>Permission</i>
--------------	-----------------------	------------------	-------------------

<i>1</i>	<i>public</i>	<i>internet</i>	<i>ro</i>

[Related commands]

Commands	Description
snmp community	Set snmp group information.
show snmp view	Show snmp view information

15.3 show snmp config

[Function]

Use **show snmp config** command to show the basic config information of snmp.

[Command Format]

show snmp config

[Command Modes]

Privileged EXEC, privileged user

[Executing Command Instruction]

Use this command to show the different quantity statistics that is received or sent by SNMP Agent.

[Example]

Show the basic config information of snmp:

Raisecom#**show snmp config**

Contact Information: support@Raisecom.com

Device location : world china raisecom

SNMP trap status: *Enable*

SNMP keepalive trap status: *Enable*

Send keepalive trap per 500 seconds

SNMP EngineID: *800022b603000e5e1a2b3c*

[Related commands]

Commands	Description
snmp-server location	Set location information of snmp
snmp-server contact	Set snmp contact information
snmp-server enable traps	Enable snmp traps
snmp-server keepalive-trap	Enable/disable send keepalive trap periodically.
snmp-server keepalive-trap interval	Set interval of switch to sent keepalive trap to SNMP website station.

15.4 show snmp group

[Function]

Use **show snmp group** to show the map relationship between snmp user and access group. (Available to devices of ISCOM2000/2100/2800/2900/3000 series and RC5xx series.)

[Command Format]

show snmp group

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Show the map relationship between snmp user and access control group.

[Example]

Show the map relationship between snmp user and access control group:

Raisecom#**show snmp group**

Index: 0

Group: group1

User Name: guestuser1

Security Model: usm

Index: 1

Group: initialN/A

User Name: raisecomN/A

Security Model: usm

Index: 2

Group: initial

User Name: raisecommd5nopriv

Security Model: usm

Index: 3

Group: initial

User Name: raisecomshanopriv

Security Model: usm

[Related commands]

Commands	Description
snmp-server group	Add or modify the map relationship from one user to access control group.
no snmp-server group	Delete the map relationship from one user to access control group.

15.5 show snmp host

[Function]

Use **show snmp host** to show the information of target host server.

[Command Format]

show snmp host

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Use the command to show the information of target host server.

[Example]

Show the information of snmp target host server:

Raisecom#**show snmp host**

```
Index:          0

IP address:     10.168.  0. 16

Port:          162

User Name:      testuser2

SNMP Version:   v3

Security Level: authnopriv

TagList:        bridge config interface rmon snmp ospf
```

[Related commands]

Commands	Description
snmp-server host	Add or modify target host address.
no snmp-server host	Delete target address.

15.6 show snmp statistics

[Function]

Use **show snmp statistics** to show snmp statistical information.

[Command Format]

show snmp statistics

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Use this command to show the quantity statistics that are received and sent by SNMP agent.

[Example]

Show snmp statistical information:

Raisecom#**show snmp statistics**

SNMP packets input:162

Unsupported SNMP version SNMP PDUs: 0

Unknown SNMP community name SNMP PDUs: 0

SNMP community not allowed operation SNMP PDUs: 0

ASN.1 or BER errors SNMP PDUs: 0

Too big SNMP PDUs: 0

Name error SNMP PDUs: 0

Bad value SNMP PDUs: 0

ReadOnly SNMP PDUs: 0

GenErrs SNMP PDUs: 0

Get-Request and Get-Next PDUs MIB objects SNMP PDUs: 0

Set-Request MIB objects SNMP PDUs: 0

Get-Request MIB objects SNMP PDUs: 0

Getnext-Request MIB objects SNMP PDUs: 0

Set-Request MIB objects SNMP PDUs: 0

Get-Response PDUs SNMP PDUs: 0

Received Traps SNMP PDUs: 0

SNMP packets output:0

Error name SNMP PDUs: 0

Too big SNMP PDUs: 0

Bad value SNMP PDUs: 0

Gen Errs SNMP PDUs: 0

Get request SNMP PDUs: 0

Get-next SNMP PDUs: 0

Set Request SNMP PDUs: 0

Get Responses SNMP PDUs: 0

Trap SNMP PDUs: 0

Unsupported security level SNMP PDUs: 0

Not in time window SNMP PDUs: 0

Unknown user name SNMP PDUs: 0

Unknown EngineID SNMP PDUs: 0

Wrong Digests SNMP PDUs: 0

Decryption Errors SNMP PDUs: 0

15.7 show snmp trap remote

[Function]

Show the enable configuration of remote trap.

[Command Format]

show snmp trap remote

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Use the command to show the enable configuration of remote trap.

[Command executing echo]

Show the enable configuration of remote trap:

SNMP Remote Trap: Enable

[Example]

Show the enable configuration of remote trap:

Raisecom(config)#**show snmp trap remote**

[Related commands]

Commands	Description
snmp trap remote { <i>enable/ disable</i> }	Enable/disable remote trap.

15.8 show snmp user

[Function]

Use **show snmp user** to show snmp user information.

[Command Format]

show snmp user

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Show snmp user information.

[Example]

Show snmp user information:

Raisecom#**show snmp user**

Index: 0

User Name: guestuser1

Security Name: guestuser1

EngineID: 800022b603000e5e1a2b3c

Authentication: MD5

Privacy: NoPriv

Index: 1

User Name: raisecomnone

Security Name: raisecomnone

EngineID: 800022b603000e5e1a2b3c

Authentication: NoAuth

Privacy: NoPriv

Index: 2

User Name: raisecommd5nopriv

Security Name: raisecommd5nopriv

EngineID: 800022b603000e5e1a2b3c

Authentication: MD5

Privacy: NoPriv

Index: 3

User Name: raisecomshanopriv

Security Name: raisecomshanopriv

EngineID: 800022b603000e5e1a2b3c

Authentication: SHA

Privacy: NoPriv

[Related commands]

Commands	Description
snmp-server user	Add or modify user list.
no snmp-server user	Delete a snmp user

15.9 show snmp view

[Function]

Use **show snmp view** to show snmp view information.

[Command Format]

show snmp view

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Show snmp view information.

[Example]

Show snmp view information:

Raisecom#**show snmp view**

Index: 0

View Name: system

OID Tree: 1.3.6.1.2.1.1

Mask: --

Type: included

Index: 1

View Name: internet

OID Tree: 1.3.6

Mask: --

Type: *included*

[Related commands]

Commands	Description
snmp-server view	Add or modify view.
no snmp-server view	Delete view.

15.10 snmp trap remote

[Function]

Enable/disable remote trap.

[Command Format]

snmp trap remote *enable*

snmp trap remote *disable*

[Parameter]

enable: enable remote trap;

disable: disable remote trap.

[Default]

enable

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Use the command to enable/disable remote trap. When enable remote trap, it is authorized to sent trap to SNMP network management if receives remote OAM notification frame; when disable remote trap, can not sent trap to SNMP if receives remote OAM notification frame.

[Command executing echo]

Set the command successfully:

Set successfully

[Example]

Enable remote trap:

Raisecom(config)# **snmp trap remote enable**

[Related commands]

Commands	Description
[no] snmp-server enable traps	Enable snmp sends trap.

15.11 snmp-server access

[Function]

Add a SNMP access group. **no** command to delete.

[Command Format]

Add a SNMP access group:

snmp-server access *groupname* [**read** *readview*] [**write** *writeview*]
[**notify** *notifyview*] { **v1sm** | **v2csm** }

snmp-server access *groupname* [**read** *readview*] [**write** *writeview*]
[**notify** *notifyview*] [*contextname* { **exact** | **prefix** }] **usm** { **noauthnopriv** |
authnopriv }

Delete a SNMP access group:

no snmp-server access *groupname* [**context** *contextname*] **usm**
{ **noauthnopriv** | **authnopriv** }

no snmp-server access *groupname* { **v1sm** | **v2csm** }

[Parameter]

groupname: group name, length should be less 32 characters;

read: specify read view;

readview: the name of readview, the length should be less than 32 characters;

write: specify write view;

writeview: the name of writview, length should be less than 32 character;

notify: specify general view;

notifyview: notify the name of the view, the length should be less than 32 characters;

context: Specify the name of context;

contextname: the name of context or prefix, length should be less than 32 characters;

exact: contextname fully match context;

prefix: contextname match frontal characters of the context;

v1sm: (Security Model)SNMPv1;

v2csm: (Community based Security Model)SNMPv2c;

usm: (User based Security Model)SNMPv3;

noauthnopriv: Security level; do not encrypt and distinguish;

authnopriv: Security level, distinguish but do not encrypt.

[Default]

Default readview is Internet scope including all the MIB variables in 1.3.6 tree. Default write is empty; default notifyview is Internet. Default context match option is **exact**.

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

Set the priority of access group, the relationship between access group and view including the name of access group, security model, security level, write and read notifyview and name matching of context. The general read and write view is the view which is set by **snmp-server**

view. When the last option is **exact**, the content name of incoming message should fully match the contextname of access group; when the last option is **prefix**, the contextname of incoming message only need to match the prefix of the context.

When the security is **v1sm** or **v2csm**, security level is **noauthnopriv**.

[Explanation of command execution echo]

Set successfully.

Group name too long!

Read view name too long!

Write view name too long!

Notify view name too long!

Context prefix too long!

Unsupported security model !

Unsupported security level !

Set unsuccessfully!

[Example]

Creat a guestgroup access group, the security mode is **usm**, the security level is distinguish but not encrypted, readview is **mib2**, writeview and notifyview are default view:

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

Delete guestgroup:

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

[Related commands]

Commands	Description
show snmp access	Show all the items in the access table.

15.12 snmp-server community

[Function]

Set community name and the corresponding view and access priority.

[Command Format]

snmp-server community *community-name [view view-name] {ro | rw}*

no snmp-server community *community-name*

[Parameter]

community-name: community name, string, less than 32;

view view-name: view name, less than 32;

ro: Gives read access to the community, but does not allow write access;

rw: Gives read and write access to authorized management stations to all objects in the MIB.

[Default]

Default view is internet.

[Command Modes]

Global configuration mode; privileged user mode

[Executing Command Instruction]

SNMP community strings authenticate access to MIB objects and

function as embedded passwords. In order for the network management system to access the switch, the community string definitions on the NMS must match at least one of the three community string definitions on the switch.

Both SNMPv1 and SNMPv2 adopt community authentication solution. The SNMP message with community not complies with authenticated by device will be discarded. The community has read-only and read-write access privilege only. Just community with read-only privilege can query device information while community with read-write privilege can configure device.

This command can also designate view corresponding to community and makes the community can access designated MIB variable in switch only. If no view keyword was input, the community name corresponding to default view internet.

Explanation of command execution echo]

Set successfully!

Set community name successfully.

Community name is too long(less than 32)

The entered community name is longer than 32.

View name is too long(less than 32)

The entered view name is longer than 32.

No so many space for create community (less equal 8)

There are already 8 communities.

Set unsuccessfully.

Set community name unsuccessfully.

[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-only priority:

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

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

[Related commands]

Commands	Description
snmp-server view	Set a view.
show snmp community	Show SNMP community information
show snmp view	Show SNMP view information

15. 13 snmp-server contact

[Function]

Configure the network administrator 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

[Command Modes]

Global configuration mode; privileged user mode

[Executing Command Instruction]

The information includes the contact information of network administrator, so when help is needed, please refer this information for help.

[Explanation of command execution echo]

Set successfully!

Set unsuccessfully

[Example]

Set up the contact information to service@raisecom.com:

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

[Related commands]

Commands	Description
show snmp config	Show the contact information of network administrator.

15.14 snmp-server enable traps

[Function]

Enable the trap function of SNMP.

[Command Format]

[no] snmp-server enable traps

[Default]

Enable traps

[Command Modes]

Global configuration mode; privileged user mode

[Executing Command Instruction]

The switch will send notifications to SNMP managers when particular events occur if SNMP-server enables trap function.

[Explanation of command execution echo]

Set successfully!

Set unsuccessfully

[Example]

Set send ospf protocol trap enable:

Raisecom(config)# **snmp-server enable traps ospf**

[Related commands]

Commands	Description
snmp-server host	Set target host of trap.

15.15 snmp-server group

[Function]

Add or delete the mapping relationship of a user and access group. **no** command is used to delete.

[Command Format]

[no] snmp-server group groupname user username { v1sm | v2csm | usm }

[Parameter]

groupname: group name, the length is less than 32 characters.

user: specify user name.

username: username, the length should be less than 32 characters.

v1sm: (Community based Security Model) SNMPv1.

v2csm: (Community based Security Model) SNMPv2c.

usm: (User based Security Model) SNMPv3.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

A user will belong to an access group according to safety model, and different access group users have different access privilege.

[Explanation of command execution echo]

Set successfully

Command executing successfully.

Group name too long!

The length of access group name should not longer than 32 characters.

User name too long!

Please input user name in length lower than 32 characters.

Unsupported security model!

Set unsuccessfully!

Fail to set.

[Example]

Map guestuser1 with the security usm level to guestgroup:

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

Delete the mapping from guestuser1 to guestgroup:

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

[Related commands]

Commands	Description
----------	-------------

show snmp group	Display all the items in the mapping table.
------------------------	---

15.16 snmp-server host

[Function]

Add or delete an IP address of trap target.

[Command Format]

Add a SNMP target host server address:

```
snmp-server host A.B.C.D version {1|2c} NAME [udpport <1-65535>]  
[bridge] [config] [interface] [rmon] [snmp] [ospf]
```

```
snmp-server host A.B.C.D version 3 {noauthnopriv|authnopriv} NAME  
[udpport <1-65535>] [bridge] [config ] [interface] [rmon] [snmp]  
[ospf]
```

Delete a SNMP target host server address:

```
no snmp-server host A.B.C.D
```

[Parameter]

addrname: host server address name, length should be less than 32 characters.

paramsname: the parameter name of host server, used to select parameter, length should be less than 32 characters.

A.B.C.D: trap target host IP address, point decimal.

version: the SNMP version which is used by target host.

1: use SNMPv1

2c: use SNMPv2c

3: use SNMPv3\n

authnopriv: authentic but not privacy

noauthnopriv: neither authentic nor privacy.

NAME: SNMPv1/v2c group name or SNMPv3 use name.

udpport: specify UDP port.

<1-65535>: host address receive the udp port number of trap, range is 1-65525.

bridge: bridge trap;

config: config trap;

interface: interface trap;

rmon: rmon trap;

snmp: snmp trap;

ospf: ospf trap.

[Default]

The default UDP port is set to 162; traplist is all the trap.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Add or delete a target host address.

[Explanation of command execution echo]

Set successfully

User name is too long !

If the user name is longer than 32 characters, display above information.

The input IP address is wrong!

Set unsuccessfully!

[Example]

Add a host address of host_1, ip address is 172.20.21.1, username is Raisecom, SNMP version is v3, authentic but not privacy, all the traps:

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

Delete host address-host_1:

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

[Related commands]

Commands	Description
show snmp host	Show all the information in the host address table.

15.17 snmp-server location

[Function]

Set the description of switch physical location.

[Command Format]

```
[no] snmp-server location sysLocation
```

[Parameter]

sysLocation: define the physical location of switch

[Default]

No location description

[Command Modes]

Global configuration mode; privileged user mode

[Executing Command Instruction]

The physical location of the Switch can be viewed for the convenience of network administrators the locate it.

[Explanation of command execution echo]

Set successfully!

Set unsuccessfully!

[Example]

Set the position of switch as HaiTaiEdifice8th:

Raisecom(config)# **snmp-server location** *HaiTaiEdifice8th*

[Related commands]

Commands	Description
show snmp location	Show the physical position information of switch

15.18 snmp-server user

[Function]

Add a new user. **No** command to delete the operation.

[Command Format]

Add a SNMP user:

snmp-server user *username* [**remote** *engineid*] **authentication**{**md5** | **sha**} *authpassword*

snmp-server user *username* [**remote** *engineid*]

Delete a SNMP user:

no snmp-server user *username* [**remote** *engineid*]

[Parameter]

username: username, length should less than 32 characters.

remote: remote SNMP engine ID;

engineid: remote SNMP engine ID. The SNMP engine ID by which username can contact it.

authentication: Specify authentication algorithm.

md5: Use authentication algorithm md5;

sha: Use authentication algorithm sha;

authpassword: authentication password.

[Default]

Default situation is that there are no authentication and no privacy; the authentication password and authentication algorithm have to be selected beforehand; default SNMP engine ID is local engine ID.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Add or delete a user.

[Explanation of command execution echo]

Set sucessfully

Engine ID is too long!

Input engine ID is wrong!

Failed to get local engine ID!

Authentication key is wrong!

Set unsuccessfully!

[Example]

Add a user guestuser1, local engine ID; md5 authentication algorithm, authentication password is Raisecom; no privacy:

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

Add a user guestuser3, local engine ID; no authentication and no privacy:

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

Delete user guestuser3, local engine ID:

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

[Related commands]

Commands	Description
show snmp user	Show all the items in the user table.

15.19 snmp-server view

[Function]

Add a SNMP view, **no** command to delete the operation.

[Command Format]

Add a snmp view:

snmp-server view *view-name oid-tree [mask] {included | excluded}*

Delete a SNMP view:

no snmp-server view *view-name oid-tree*

[Parameter]

view-name: View name, length is below 32;

oid-tree:OID number, length is below 128;

mask: OID tree mask, length is below 128, OID format, OID option can only be 0 or 1;

included: MIB variable in OID tree;

excluded:MIB variable out of OID tree.

[Default]

All the numbers of mask are 1.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

SNMPv3 defines access mode based on view. Users can use the command to define a view. Mask is the mask of OID subtree, each of its digit corresponding to each option of its tree. If particular digit of the mask is 1, view should according to subtree corresponding option; if particular digit of the mask is 0, then it is not needed to match the subtree corresponding option. The mask length is 16 characters, that is to say it support the subtree with length 128. if subtree of a view is 1.3.6.1.2.1, mask is 1.1.1.1.0.1, the view contains actual subtree 1.3.6.1.x.1 (x can be any number), that is to say the first option of all nodes under 1.3.6.1.

[Explanation of command execution echo]

Set successfully

Name too long !

Oid tree Name NOT correct !

mask too long!

Mask NOT correct !

Set unsuccessfully!

View internet:1.3.6 should NOT be deleted!

[Example]

The following example display how to configure SNMP view:

Create view mib 2, view includes all the MIB variables under 1.3.6.1.2.1:

```
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1  
included
```

Delete view mib2, subtree is 1.3.6.1.2.1:

```
Raisecom(config)# no snmp-server view mib2 1.3.6.1.2.1
```

[Related commands]

Commands	Description
show snmp view	Show all the information in SNMP view table.



Chapter 16 Cluster Management

Commands

16.1 cluster

[Function]

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

[Command Format]

[no] cluster

[Default]

No cluster

[Command Modes]

Global configuration mode; Privileged EXEC

[Executing Command Instruction]

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

[Command Executing Echo]

This switch has been a member, it can not be a COMMANDER.

Cluster management startup unsuccessfully.

Cluster management shutdown successfully.

Cluster management shutdown unsuccessfully.

[Example]

Start cluster management:

Raisecom(config)#**cluster**

Stop cluster management:

Raisecom(config)#**no cluster**

[Related commands]

Commands	Description
show cluster	Show cluster management related information

16.2 cluster-autoactive

[Function]

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

[Command Format]

[no] cluster-autoactive

[Default]

Default configuration is autoactive function disabled.

[Command Modes]

Global configuration mode; Privileged EXEC.

[Executing Command Instruction]

Users can use **cluster-autoactive** command to enable automatically activating function. **no cluster-autoactive** command will disable automatically activating function. When the autoactive function is enabled, and the commander MAC address is configured, the switch will set itself

as an active member.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Start the **autoactive** function:

Raisecom(config)#**cluster-autoactive**

Stop the **auto active** function:

Raisecom(config)#**no cluster-autoactive**

[Related commands]

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

16.3 cluster-autoactive commander-mac

[Function]

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

[Command Format]

[no] cluster-autoactive commander-mac HHHH.HHHH.HHHH

[Default]

Default configuration is 0000.0000.0000.

[Command Modes]

Global configuration mode; Privileged EXEC.

[Executing Command Instruction]

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

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

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Configure the MAC address of autoactive associated switch to 1111.1111.1111:

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

Recover MAC address of the commander MAC address:

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

[Related commands]

Commands	Description
[no] cluster-autoactive	Enable or disable the autoactive function
show cluster	Show cluster management related information

16.4 member

[Function]

Add, active and delete cluster member.

[Command Format]

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

member HHHH.HHHH.HHHH suspend

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

[Parameter]

active: active this member

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

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

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

suspend: to suspend this member

all: delete all the members

[Command Modes]

Cluster configuration mode; privileged user.

[Executing Command Instruction]

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

[Explanation of command execution echo]

This device is not a COMMANDER.

There is no this member.

Member add unsuccessfully.

Member add successfully.

This member has been activated.

Add successfully, active successfully.

Add successfully, active unsuccessfully, this member is not operation up.

add successfully, active unsuccessfully, the switch be configed is a commander.

Add successfully, active unsuccessfully, the switch be configed is already a member.

Add successfully, active unsuccessfully, username or password is wrong.

Add successfully, active unsuccessfully, timeout.

This member has not been activated.

Delete member unsuccessfully.

Delete successfully

[Example]

Add the candidate 1111.1111.1111 to the cluster:

Raisecom(config-cluster)#**member 1111.1111.1111**

Add the candidate 1111.1111.1111 to the cluster and active the member:

Raisecom(config-cluster)#**member 1111.1111.1111 active**

Add and suspend the cluster member 1111.1111.1111:

Raisecom(config-cluster)#**member** *1111.1111.1111 suspend*

Delete cluster member 1111.1111.1111:

Raisecom(config-cluster)#**no member** *1111.1111.1111*

Delete all the cluster member:

Raisecom(config-cluster)#**no member** *all*

[Related commands]

Commands	Description
show cluster member [<i>HHHH.HHHH.HHHH</i>]	Show cluster member information.

16.5 member auto-build

[Function]

Automatically active all the member switches.

[Command Format]

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

[Parameter]

active: active cluster member

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

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

all: automatically build and active all the candidates.

[Command Modes]

Cluster configuration mode; privileged user.

[Executing Command Instruction]

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

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

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

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

[Explanation of command execution echo]

this device is not a COMMANDER.

there is no such a candidate.

Apply the command **member auto-build active** username password or **member auto-build active** username password all on the commander switch, which does have candidate.

there is no candidate that can be autoactivated.

Apply the command **member auto-build** on the switch, which cannot be auto-build.

too many members have been added.

too many members have been added.

HHHH.HHHH.HHHH : add successfully, active successfully.

HHHH.HHHH.HHHH : add successfully, active unsuccessfully, this member is not operation up.

HHHH.HHHH.HHHH : add successfully, active unsuccessfully, the switch be configed is a commander.

HHHH.HHHH.HHHH : add successfully, active unsuccessfully, the switch be configed is allready a member.

HHHH.HHHH.HHHH : add successfully, active unsuccessfully, usrxame or password is wrong.

HHHH.HHHH.HHHH : add successfully, active unsuccessfully, timeout

[Example]

Add all the candidates into the cluster and active them:

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

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

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

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

```
Raisecom(config-cluster)# member auto-build
```

[Related commands]

Commands	Description
show cluster member [HHHH.HHHH.HHHH]	Show cluster member information.

16.6 rcommand

[Function]

Under cluster mode, enter cluster member remotely from commander switch.

[Command Format]

rcommand {[*hostname*] [*HHHH.HHHH.HHHH*]}

[Parameter]

hostname: the cluster member's name

HHHH.HHHH.HHHH: the MAC address for cluster member who want to login.

[Command Modes]

Cluster configuration mode; privileged user (priority 15).

[Executing Command Instruction]

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

This command can only be applied on the switch which enable cluster function.

[Explanation of command execution echo]

Connect unsuccessfully!

Connection to host lost

Failed! This device is NOT a commander!

Failed! This hostname is NOT in the cluster!

Failed! This mac address is NOT in the cluster!

MAC address which match this hostname in the cluster::

AAAA.BBBB.CCCC

DDDD.EEEE.FFFF

Duplicate hostname in the cluster, please input the mac address of the device

Display the above information when the input device name is used by several users in a cluster.

[Example]

Login the cluster member with a MAC address AAAA.BBBB.CCCC:

raisecom(config-cluster)# **rcommand** AAAA.BBBB.CCCC

Login the cluster member “swA”:

raisecom(config-cluster)# **rcommand** swA

16.7 rndp

[Function]

Enable and disable RNDP (Raisecom Neighbor Discovery Protocol).

[Command Format]

rndp {*enable* / *disable*}

[Parameter]

enable: RNDP enable;

disable: RNDP disable.

[Default]

enable on all the ports

[Command Modes]

Global configuration mode or physical configuration mode; privileged user

[Executing Command Instruction]

RNDP is used to discover the directly connected switch within a LAN, obtain and record device information. RNDP is the foundation for RTDP (Raisecom Topology Discovery Protocol). Generally speaking, they are used together. Only if the device is discovered by RNDP, the device can be discovered and its parameters can be collected by RTDP. User can disable RNDP to deny other devices within the LAN to discover it; RNDP also can be disabled on particular port.

[Command Executing Echo]

Set successfully.

Set unsuccessfully.

[Example]

Deny RNDP globally:

Raisecom(config)#**rndp** disable

Enable RNDP globally:

Raisecom(config)#**rndp** enable

Deny RNDP under physical port configuration mode:

Raisecom(config-port)#**rndp** disable

[Related commands]

Commands	Description
show rndp	Show RNDP configuration information
show rndp neighbor	Show RNDP neighboring information.

16.8 rtdp

[Function]

Enable and disable RTDP (Raisecom Topology Discovery Protocol) function.

[Command Format]

rtdp { *enable* / *disable* }

[Parameter]

enable: enable RTDP collection function.

disable: disable RTDP collection function.

[Default]

switch RTDP function disable.

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

RTDP is used to collect all switches' information, which support the RTDP and RNDP function is started. When **rtdp enable** command is applied to start RTDP collection function, RTDP will collect information of all the switches within specified collection scale (use **rtdp max-hop command** to set). Generally speaking, RTDP and RCMP (Raisecom Cluster Management Protocol) are used together. In cluster management, when the user wants to enable the cluster management function of cluster member device within the protocol, user should start RTDP to find out this device and get basic information for the device.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Deny RTDP collection globally:

Raisecom(config)#**rtdp disable**

Enable RTDP collection globally:

Raisecom(config)#**rtdp enable**

[Related commands]

Commands	Description
rtdp max-hop	Set RTDP the maximum collection scale
show rtdp	Show RTDP config information
show rtdp device-list <i>[HHHH.HHHH.HHH][hostname]</i> [detailed]	Show RTDP device list information.

16.9 rtdp max-hop

[Function]

The maximum hop of RTDP (Raisecom Topology Discovery Protocol)

[Command Format]

rtdp max-hop *<1-16>*

no rtdp max-hop

[Parameter]

<1-16>: the maximum collection scale parameter (hop); first hop starts from directly connected device.

no: command used to recover default setting.

[Default]

The maximum hop of RTDP is 16 hops

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

Use this command to limit the range of RTDP collection.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Set the max-hop of FTDP to 2 hops:

```
Raisecom(config)# rtdp max-hop 2
```

Recovery the max-hop of RTDP to 16 hops:

```
Raisecom(config)# no rtdp max-hop
```

[Related commands]

Commands	Description
rtdp max-hop	Set the max-hop of RTDP.
show rtdp	Show RTDP config information
show rtdp device-list <i>[HHHH.HHHH.HHH/hostname] [detailed]</i>	Show RTDP device list information.

16.10 show cluster member

[Function]

Show cluster member information.

[Command Format]

```
show cluster member [ HHHH.HHHH.HHHH ]
```

[Parameter]

HHHH.HHHH.HHHH cluster member MAC address

[Command Modes]

all

[Executing Command Instruction]

You can use the command only on cluster commander switch.

[Explanation of command execution echo]

This device is not a COMMANDER.

When you use the command on a not-commander switch, the echo is as above.

MAC	Address	ActiveOperationState	ActiveManageState
-----	---------	----------------------	-------------------

Hostname

```
-----  
AAAA.BBBB.CCCC      up      active  
raisecom
```

When you execute the command on commander switch that has been added cluster member, the echo is as above.

[Example]

On switch B configure cluster-autoactive, cluster-autoactive commander-mac MAC-A;

Add member swB on swA, use command member MAC-B or member auto-build

```
A(config-cluster)#show cluster member
```

```
MAC Address      ActiveOperationState  ActiveManageState  
Hostname
```

```
-----  
000E.5E12.FD1E      Up      Desirable  
B
```

then when you use username and password to activate, it will inform you that This member has been acitved:

```
A(config-cluster)#show cluster member
```

```
MAC Address      ActiveOperationState  ActiveManageState  
Hostname
```

```
-----  
000E.5E12.FD1E      Up      Desirable  
B
```

Add the member that does not exist, then use username and password for activation. Then the member activation state will be down, activate it.

Use show:

MAC	Address	ActiveOperationState	ActiveManageState
Hostname			

1234.1234.1234		Down	Active
<unknown>			

[Related commands]

None

16. 11 show rndp

[Function]

Show RNDP configuration information.

[Command Format]

show rndp

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

User can use this command to check the RDNP global enable state and port enable state.

[Explanation of command execution echo]

The second and third line show the RNDP enable and port enable state respectively.

Global RNDP Configuration:

RNDP feature is currently enabled on the switch

Participant ports: 1-26

[Related commands]

Commands	Description
rndp	Set RNDP enable status
show rndp neighbor	Show RNDP adjacent information

16.12 show rndp neighbor

[Function]

show RNDP neighbor information.

[Command Format]

show rndp neighbor

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

User can use this command to check RNDP found neighbor information.

[Explanation of command execution echo]

The first line shows the MAC address of neighbor device

The second line shows the port numbers that is used to connect current device and neighbor device.

The third line shows the port numbers that is used to connect neighbor device and current device

The fourth line shows the device systemID, each device has exclusive systemID, i.e. ISCOM2826 system ID is 60003, but ISCOM2126 is 60005.

The fifth line shows the device hostname.

Mac Address LocalPort RemotePort SysID Hostname

<i>000e.5e00.c2c4</i>	<i>1</i>	<i>9</i>	<i>60003</i>	<i>swB</i>
<i>000e.5e11.4d0b</i>	<i>17</i>	<i>18</i>	<i>60003</i>	<i>Raisecom</i>
<i>000e.5e23.34e2</i>	<i>17</i>	<i>24</i>	<i>60003</i>	<i>Raisecom</i>

[Related commands]

Commands	Description
rndp	Set the enable status of RNDP
show rndp	Show RNDP configuration information.

16. 13 show rtdp

[Function]

Show RTDP configuration information.

[Command Format]

show rtdp

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

user can use this command to check RTDP configuration information.

[Explanation of command execution echo]

RTDP max-hop: 16

RTDP collecting feature: Disabled

RTDP reporting feature: Enabled

[Related commands]

Commands	Description
rtdp	Set RTDP enable status
rtdp max-hop	Set maximum collection scope of RTDP
show rtdp device-list	Show RTDP found device-list information

[HHHH.HHHH.HHH/hostname] [detailed]

16.14 show rtdp device-list

[Function]

Show RTDP collection information.

[Command Format]

show rtdp device-list *[HHHH.HHHH.HHHH / hostname]* **[detailed]**

[Parameter]

HHHH.HHHH.HHHH: the MAC address of need shown device;

hostname: the hostname of the device;

detailed: show detail device information.

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

User can use this command to check RTDP collected device information.

[Explanation of command execution echo]

The first line shows the MAC address of the device.

The second line showing: the device is found from which port.

The third line showing the device is found from which hop.

The fourth line showing the device system ID, each device has exclusive system ID, i.e. ISCOM 2826 system ID is 60003, but ISCOM 2126 system ID is 60005

The fifth line showing the device hostname.

Execution echo Detail information:

RTDP discovery device-list:

<i>MAC Address</i>	<i>RcvdPort</i>	<i>Hop</i>	<i>SysID</i>	<i>HostName</i>
--------------------	-----------------	------------	--------------	-----------------

<i>000e.5e00.c2c2</i>	<i>1</i>	<i>2</i>	<i>60003</i>	<i>swD</i>
-----------------------	----------	----------	--------------	------------

<i>000e.5e00.c2c8</i>	<i>1</i>	<i>2</i>	<i>60003</i>	<i>swC</i>
-----------------------	----------	----------	--------------	------------

<i>000e.5e00.c2c4</i>	<i>1</i>	<i>1</i>	<i>60003</i>	<i>swB</i>
-----------------------	----------	----------	--------------	------------

RTDP search by mac 000e.5e00.c2c4 result:

<i>MAC Address</i>	<i>RcvdPort</i>	<i>Hop</i>	<i>SysID</i>	<i>HostName</i>
--------------------	-----------------	------------	--------------	-----------------

<i>000e.5e00.c2c4</i>	<i>1</i>	<i>1</i>	<i>60003</i>	<i>swB</i>
-----------------------	----------	----------	--------------	------------

-Device cluster information:

Identity: member

Commander MAC: 000e.5e00.c366

AutoActive: on

AutoActive MAC: 000e.5e00.c366

-Device adjacency information:

<i>MAC Address</i>	<i>Native Port</i>	<i>Remote Port</i>
--------------------	--------------------	--------------------

<i>000e.5e00.c2c2</i>	<i>24</i>	<i>9</i>
-----------------------	-----------	----------

<i>000e.5e00.c2c8</i>	<i>1</i>	<i>9</i>
-----------------------	----------	----------

Detail information not only showing all the concise information, but also adding two other following information.

Device cluster information, including:

DeviceID(identity): can be member/candidate/commander;

Commander MAC: it is the MAC address of Commander that can be automatically active by device, and if the device is not the member, do not show the information.

AutoActive on-off(AutoActive): represent whether this device can be automatically active , can be on/off.

AutoActive MAC: the MAC address of Commander that can be automatically active, if the device is not allowed to be automatically active, do not show the information.

Device adjacent information:

The first line represents the downlink MAC address.

The second line represents the port number of the device that is used to connect the adjacent device.

The third line represents the port number of the adjacent device used to connect device.

[Related commands]

Commands	Description
rtdp	Set RTDP enable status.
rtdp max-hop	Set the maximum range of RTDP.
show rtdp	Show configuration information of RTDP.

Chapter 17 System Log Commands

17.1 logging console

[Function]

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

[Command Format]

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

no logging console

[Parameter]

<0-7>: log severity

alerts: need action immediately (severity=1)

critical: serious state (severity =2)

debugging: debug information (severity =7)

emergencies: system can not use (severity =0)

errors: error condition (severity =3)

informational: informational event (severity =6)

notifications: normal event under critical condition (severity=5)

warnings: warning condition (severity=4)

[Default]

Enable and the severity is **informational**

[Command Modes]

Global configuration mode; Privileged EXEC

[Executing Command Instruction]

Use this command to configure print logging information to console.

Severity of logging information.

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

[Command Executing Echo]

Set console logging information successfully

[Example]

Configure the severity level of logging console as alerts:

Raisecom(config)#logging console alerts

[Related commands]

Commands	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

17.2 logging file

[Function]

Configure and start to record logging file to flash file, the **no** command

will disable events to be logged in log output direction.

[Command Format]

logging file

no logging file

[Default]

Enable log information to logging file.

The mode of output is config

[Command Modes]

Global configuration mode; Privileged EXEC.

[Executing Command Instruction]

Use this command to output log information to flash file.

[Explanation of command execution echo]

Set successfully.

[Example]

Use this command to record log information in logging file.

Raisecom(config)#**logging file**

[Related commands]

Commands	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

17.3 logging host

[Function]

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

[Command Format]

logging **host** **A.B.C.D**
{local0|local1|local2|local3|local4|local5|local6|local7}
{<0-7>|alerts|critical|debugging|emergencies|errors|informational|notifications|warnings}
no logging host A.B.C.D

[Parameter]

local0-local7: equipment name of log host

<0-7>: log grade

alerts: need action immediately (severity=1)

critical: serious state (severity =2)

debugging: debug information (severity =7)

emergencies: system not available (severity =0)

errors: error condition (severity =3)

informational: informational event (severity =6)

notifications: normal and critical event (severity =5)

warnings: warning condition (severity=4)

[Default]

No assigned log host

[Command Modes]

Global configuration mode; Privileged EXEC.

[Executing Command Instruction]

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

Log description of log host:

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

[Explanation of command execution echo]

Set log host logging information successfully.

Set log host logging information unsuccessfully.

[Example]

Set log grade of the logging host as alearts and all of the information lower or equal to this log grade will be output to the host:

Raisecom(config)# **logging host** 10.0.0.1 local7 alerts

[Related commands]

Commands	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

17.4 logging on

[Function]

Use **logging on** to enable log function, use **no logging on** to disable log

function.

[Command Format]

[no] **logging on**

[Default]

Log function is enabled

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

Enable log function

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Enable log function:

Raisecom(config)#**logging on**

[Related commands]

Commands	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

17.5 logging time-stamp

[Function]

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

[Command Format]

logging time-stamp { *standard* / *relative-start* / *null* }

[no] logging time-stamp

[Parameter]

date-time: Absolute time after startup

relative-start: relative time of system enabled

null: not add time stamp

[Default]

Use date-time

[Command Modes]

Global configuration mode and Privileged EXEC

[Executing Command Instruction]

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

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

Relative time hh-mm-ss

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Enable log relative time:

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

[Related commands]

Commands	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

17.6 show logging

[Function]

Show log information.

[Command Format]

show logging [*file*]

[Parameter]

file: show the logging information which is stored in the file.

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Use this command to show the logging configuration information or logging information in the logging information saved in the logging file.

[Explanation of command execution echo]

Show logging information:

Raisecom#**show logging**

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

Console logging: enable, level=debug ,22 Messages logged

Monitor logging: disable, level=info ,0 Messages logged

Time-stamp logging messages: enable

Log host Information:

<i>Target Address</i>	<i>Level</i>	<i>Facility</i>	<i>Sent</i>	<i>Drop</i>

192.168. 1. 9	debug	local7	11	11
192.168. 1.185	debug	local7	11	11

Show the information saved in the logging file:

Raisecom#**show logging file**

Logging information in file

DEC-31-1999 00:04:45 SYS-I-START-A:System startup

DEC-31-1999 00:16:40 SYS-I-START-A:System startup

DEC-31-1999 03:54:37 SYS-I-START-A:System startup

DEC-31-1999 05:24:22 SYS-I-WRITE-A:Write system configuration

DEC-31-1999 04:02:35 SYS-I-START-A:System startup

DEC-31-1999 05:34:36 SYS-I-WRITE-A:Write system configuration

DEC-31-1999 05:37:41 SYS-I-WRITE-A:Write system configuration

[Example]

Show the log information saved in the file:

Raisecom#**show logging file**

[Related commands]

Commands	Description
Logging console	Start the console output direction of the logging file.
logging monitor	Start the monitor output direction of the logging file.
logging file	Start the output direction of logging file.
logging time-stamp	Set the time-stamp of logging information.

Chapter 18 Schedule Commands

18.1 cmd-str schedule-list

[Function]

Operating the command according to schedule mode or say, add the command into schedule list.

[Command Format]

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

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

[Parameter]

cmd-no: command in the schedule list, this is a dynamic variational command no.;

schedule-list: set start time, finish time and interval of periodic execution of schedule task;

list-no: the range of schedule list is <0-99>.

[Command Modes]

Global configuration mode, Privileged user

[Explanation of command execution echo]

Set successfully.

Current schedule list not existed.

[Example]

Raisecom(config)#**storm-control dlf schedule-list 1**

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

[Related commands]

Commands	Description
schedule-list <i>list-no</i>	Add or modify schedule list.
show schedule-list	Show information of schedule-list.

Commands list in support of schedule:

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

port-list (*all*/*{1-26}*) {*ingress/egress/both*}

filter {*enable/disable*}

[no] filter {*ip-access-list/mac-access-list/ access-list-map*}{*all*/*<0-399>*}

vlan-list {*all*/*{1-4094}*}

clear arp

flowcontrol {*on / off*}

ip igmp-snooping

no ip igmp-snooping

ip igmp-snooping

no ip igmp-snooping

no shutdown

shutdown

duplex {*full-duplex / half-duplex*}

speed { *auto / 10 / 100 /1000*}

clear interface port statistics

clear interface port *<1-"MAX_PORT_STR">* **statistics**

switchport protect

no switchport protect

rate-limit port-list (*all / {1-"MAX_PORT_STR"}*) **ingress**

rate-limit port-list (*all / {1-"MAX_PORT_STR"}*) **egress**

no rate-limit port-list (*all* | {1-"MAX_PORT_STR"}) (*ingress* | *egress* | *both*)

sntp server A.B.C.D

no sntp server

spanning-tree (*enable/disable*)

mac-address-table aging-time

no mac-address-table aging-time

mac-address-table learning (*enable* | *disable*) **port-list** (*all* | {1-"MAX_PORT_STR"})

mac-address-table static HHHH.HHHH.HHHH **vlan** <1-4094> **port** <1-"MAX_PORT_STR">

clear mac-address-table (*all* | *dynamic* | *static*)

mirror (*enable* | *disable*)

svl (*enable/disable*)

dlf-forwarding (*enable* | *disable*)

no relay (*bpdu* | *dot1x* | *lacp* | *garp* | *gmrp* | *gvrp* | *all*) **port-list** [{1-"MAX_PORT_STR"}]

relay (*bpdu* | *dot1x* | *lacp* | *garp* | *gmrp* | *gvrp* | *all*) **port-list** {1-"MAX_PORT_STR"}

storm-control ratio <1-100> <0-512>

storm-control ratio <1-100>

storm-control bps <0-1000> <0-512>

storm-control pps <0-262143>

storm-control all (*enable* | *disable*)

storm-control dlf (*enable* | *disable*)

storm-control multicast (*enable* | *disable*)

storm-control broadcast (*enable* | *disable*)

[no] **ip dhcp relay**(global configuration mode)

[no] ip dhcp relay(IP interface configuration mode)

[no] ip dhcp relay ip-list { all | ip-list } target-ip A.B.C.D

[no] ip dhcp relay target-ip A.B.C.D

[no] ip dhcp relay information option

ip dhcp relay information policy { drop | keep | replace }

[no] ip dhcp relay information trusted port-list { all | port-list }

[no] ip dhcp relay information trusted

[no] ip dhcp server (global configuration mode)

[no] ip dhcp server (IP interface configuration mode)

ip dhcp server ip-pool pool-name start-ip end-ip mask-ip ip <0-MAXIP>
[gateway gtw-address] [dns dns-address] [secondary-dns dns-address]

no ip dhcp server ip-pool pool-name

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

no ip dhcp server relay-ip A.B.C.D

ip dhcp snooping

no ip dhcp snooping

ip dhcp snooping port-list { all | port-list }

no ip dhcp snooping port-list { all | port-list }

ip dhcp snooping trust

no ip dhcp snooping trust

ip dhcp snooping information option

no ip dhcp snooping information option

18.2 schedule-list

[Function]

Add or modify schedule-list, this command used to set the starting time,

ending time and periodical execution interval.

[Command Format]

no command to delete a queue.

schedule-list *list-no* **start** {**up-time** *days time* [**every** **days time** [**stop** *days time*]]} | **date-time** *date time* [**every** {*day / week / days time*} [**stop** *date time*]]}

no schedule-list *list-no*

[Parameter]

list-no: dispatching list range is <0-99>;

up-time: Relative time after startup;

date-time: Absolute time after startup;

days time: a time period, the format is: days: <0-65535>, time: HH:MM:SS. Example: 3 3:2:1;

date time: a time point, input format is: MMM-DD-YYYY HH:MM:SS. Example: jan-1-2003 or 1-1-2003, the range of YYYY is 1970 to 2199.

[Command Modes]

Global configuration mode; privileged user.

[Explanation of command execution echo]

Set successfully.

input Date & Time should be MMM-DD-YYYY(1900-2199), HH:MM:SS format

[Example]

Raisecom# **schedule-list** 1 **start** **date-time** Feb-2-2004 0:0:0 **every**
6 0:0:0 **stop** Feb-2-2005 0:0:0

[Related commands]

Commands	Description
Show schedule-list	Show schedule-list information.

comd-str	Execute the command based on the
schedule-list <i>list-no</i>	way of dispatching.

18.3 show schedule-list

[Function]

Show schedule list information.

[Command Format]

show schedule-list [*list-no*]

[Parameter]

list-no: dispatching list range is <0-99>.

[Command Modes]

Privileged EXEC, privileged user

[Example]

Raisecom# **show schedule-list 1**

[Related commands]

Commands	Description
schedule-list <i>list-no</i>	Add or modify schedule list
comd-str schedule-list <i>list-no</i>	Apply the command based on the way of schedule list.

Chapter 19 Trouble Shooting Commands

19.1 driver

[Function]

The control switch to set device receives any packets.

[Command Format]

driver *{receive-packet/send-packet}* [**ethertype-classify** *{stp/ garp/ gmrp/ gvrp/ igmpsnoop/ lacp/ eapol/ loopdetect/ rcmp/ rcmpdata/ rndp/ rtdp/ arp/ ip/ relay/ others/ oam/ relay-stp}*] *{discard/syslog}* *{enable/disable}* [**port-list** *port-list*]

[Parameters]

receive-packet: packet receiving

send-packet: packet sending

enable: enable

disable: disable

discard: discard packet

syslog: information of syslog

port-list: port list

[Default]

Disable, Ethernet type is all types.

[Command Modes]

Global configuration mode; Privileged user

[Executing Command Instruction]

This command can control packets received or transmitted by the switch.

If no type be specified, control all types. If the packets type is specified,

only the specified ones will be in control. Classification of support only accords to Ethernet type, the Ethernet classification including:

stp	STP protocol packets (0x0042)
garp	GARP protocol packets (0x0043)
gmrp	GMRP protocol packets (0x2042)
gvrp	GVRP protocol packets (0x2142)
igmpsnoop	igmpsnoop protocol packets (0x0242)
larp	slow protocol frame protocol packets (0x8809)
eapol	EAPOL protocol packets (0x888e)
loop	loopback detection protocol packets (0x0898)
rcmp	RCMP protocol control packets (0x0899)
rcmpdata	RCMP protocol data packets (0x0897)
rndp	RNDP protocol packets (0x1a77)
rtdp	RTDP protocol packets (0x1a78)
arp	ARP protocol packets (0x0806)
ip	IP protocol packets (0x0800)
relay	relay protocol packets
others	other Ethernet packets
oam	oam protocol packets
relay-stp	relay-stp protocol packets

[Example]

Syslog all received packets:

Raisecom# **driver receive-packet** *syslog enable*

[Related commands]

Commands	Description
----------	-------------

show device-statistics	Show setting and statistics of CPU receive/transmit packets.
clear device-statistics	Clear CPU received and transmitted packets.

19.2 show buffer

[Function]

Show the buffer information of the port.

[Command Format]

show buffer [*port* <1-26>]

[Parameter]

port <1-26>: specify the port number (optional).

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

If the port number is not specified, show all the port driver pool information.

[Example]

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

Port 2

```

-----
Total mBlks: 500      Free mBlks: 500      DATA: 0

HEADER:  0      SOCKET:  0      PCB:    0

RTABLE:  0      HTABLE:  0      ATABLE:  0

SONAME:  0      ZOMBIE:  0      SOOPTS:  0

```

FTABLE: 0 RIGHTS: 0 IFADDR: 0

CONTROL: 0 OOBDATA: 0 IPMOPTS: 0

IPMADDR: 0 IFMADDR: 0 MRTABLE: 0

19.3 show diags

[Function]

Show port diagnose information.

[Command Format]

show diags *link-flap*

[Parameter]

link-flap: show UP/DOWN times and their speed(number of UP/DOWN at the last minute).

[Command Modes]

Privileged EXEC; privileged user.

[Example]

Raisecom#**show diags 1**

<i>Port</i>	<i>Total</i>	<i>Last Min</i>
-------------	--------------	-----------------

<i>19</i>	<i>2</i>	<i>0</i>
-----------	----------	----------

<i>21</i>	<i>2</i>	<i>2</i>
-----------	----------	----------

19.4 show memory

[Function]

Show memory information.

[Command Format]

show memory

[Command Mode]

Privileged EXEC; privileged user.

[Example]

Raisecom#**show memory**

FREE LIST:

<i>num</i>	<i>addr</i>	<i>size</i>

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

SUMMARY:

<i>status</i>	<i>bytes</i>	<i>blocks</i>	<i>avg block</i>	<i>max block</i>
---------------	--------------	---------------	------------------	------------------

current

<i>free</i>	34120840	5	6824168	32017512
-------------	----------	---	---------	----------

<i>alloc</i>	23460160	62554	375	-
--------------	----------	-------	-----	---

cumulative

<i>alloc</i>	23591248	64754	364	-
--------------	----------	-------	-----	---

19.5 show tech-support

[Function]

Show technical support information, all the information about trouble shooting.

[Command Format]

show tech-support

[Command Modes]

Privileged EXEC; privileged user.

[Example]

Raisecom#**show tech-support**

Chapter 20 Commands of Storm-control

20.1 creat vlan

[Function]

Create static VLAN.

[Command Format]

creat VLAN [*<3-4094>*] {*active/suspend*}

[Parameter]

<3-4094>: Range of VLAN.

[Default]

All ports belong to VLAN 1 by default.

[Command Modes]

Global configuration mode

[Executing Command Instruction]

Use this command to create static VLAN.

[Explanation of command execution echo]

Create successfully.

Create unsuccessfully.

[Example]

Create VLAN 4:

Raisecom(config)#**create vlan 4 active**

[Related commands]

Commands	Description
show vlan [<i><3-4094></i>]	Show VLAN configuration information.

20.2 name

[Function]

Configure the name of static VLAN.

[Command Format]

name *WORD*

[Parameter]

WORD: The name shall be less than 15 characters

[Default]

By default, the name of system default VLAN (VLAN1) is “Default” and cluster VLAN name is “Cluster-Vlan”, other name of static VLAN is string “VLAN” plus four bits VLAN ID, Example, the default name of VLAN1 is “VLAN0001”, VLAN 4094 default name is “VLAN4094”.

[Command Modes]

Static VLAN configuration mode; privileged user

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Set the name of VLAN 3 to “HR”:

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

[Related commands]

Commands	Description
name	Name static VLAN.
state	Set active status of static VLAN.
show vlan	Show VLAN configuration information.

20.3 show interface port switchport

[Function]

Show the configuration information of the VLAN.

[Command Format]

show interface port [*<1-MAXPORT>*] switchport

show interface client [*<1-MAXPORT>*] switchport

show interface line [*<1-MAXPORT>*] switchport

[Parameter]

<1-MAXPORT>: port list;

client: client port;

line: line port.

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Show VLAN configuration information of the port.

[Explanation of command execution echo]

Echo of ISCOM series switch:

X stands for port number.

Port X:

Administrative Mode: extend-access

Operational Mode: extend-access

Access Mode VLAN: 1(default)

Administrative Hybrid Allowed VLANs: 1,2

Operational Hybrid Allowed VLANs: none

Administrative Hybrid Untagged VLANs: none

Operational Hybrid Untagged VLANs: none

Administrative Trunk Allowed VLANs: all

Operational Trunk Allowed VLANs: none

Native Mode Vlan: 1(default)

Echo of RC5X1 device:

Port clientX:

PVID: 1

PVID override: Disabled

Double tag: Disabled

Vlan accept-frame: All

Vlan ingress filtering: None

Egress default : Unmodify

[Related commands]

Commands	Description
switchport access vlan	Show the ACCESS VLAN ID of the port
switchport hybrid allowed vlan	Set the port to allowable VLAN, when it is set to HYBRID mode.
switchport hybrid untagged vlan	Set the port to allowable UNTAG VLAN, when it is set to HYBRID mode.
switchport mode	Set the VLAN mode of the port.
switchport native vlan	Set the NATIVE VLAN for the port, when it is set to HYBRID or TRUNK mode.
switchport trunk allowed vlan	Set the port to allowable VLAN, when the port is set to TRUNK mode.

20.4 show vlan

[Function]

Show static VLAN configuration information.

[Command Format]

show vlan [{1-4094}]

[Parameter]

{1-4094}: VLAN ID list.

[Command Modes]

Privileged EXEC; Privileged user

[Executing Command Instruction]

Show all the static VLAN configuration information, including active and suspending.

[Explanation of command execution echo]

Echo 1:

Outer TPID: 0x9100

<i>VLAN</i>	<i>Name</i>	<i>State</i>	<i>Ports</i>

<i>1</i>	<i>Default</i>	<i>active</i>	<i>1-26</i>
<i>2</i>	<i>Cluster-Vlan</i>	<i>active</i>	<i>1-26</i>
<i>3</i>	<i>VLAN0003</i>	<i>suspend</i>	<i>1,2,10,20-25</i>

The above echo just is applicable to support double tag switch, such as: 3026/2826/2008/2026b/2026c/2017/2017a/2016c/2016/2016S/2026S/2126f/2126e/2126fl/2109f.

Echo 2:

<i>VLAN</i>	<i>Name</i>	<i>State</i>	<i>Ports</i>

<i>1</i>	<i>Default</i>	<i>active</i>	<i>1-26</i>
<i>2</i>	<i>Cluster-Vlan</i>	<i>active</i>	<i>1-26</i>
<i>3</i>	<i>VLAN0003</i>	<i>suspend</i>	<i>1,2,10,20-25</i>

The above echo is applicable to ISCOM series switches except the echo 1 listed.

Echo 3: this echo is applicable on RC5X1 switch:

Switch mode: Transparent

Core tag type: 0x9100

VLAN	Ports	Untag Ports	Priority
------	-------	-------------	----------

1	L:1;C:1-4	L:1;C:1-4	--
---	-----------	-----------	----

2	L:1;C:1-4	n/a	--
---	-----------	-----	----

[Related commands]

Commands	Description
name	Name static VLAN.
state	Set active status of static VLAN.
show vlan	Show VLAN configuration information.

20.5 state

[Function]

Set the active state of static VLAN.

[Command Format]

state {*active* / *suspend*}

[Parameter]

active: Set static VLAN active;

suspend: Set static VLAN suspend.

[Default]

Suspended by default.

[Command Modes]

The configuration exec of static VLAN; privileged user

[Executing Command Instruction]

All the configuration of static VLAN is enabled when VLAN is active. When static VLAN is suspend, users can configure it, such as delete/add port, set the VLAN name, system will remain the configuration. Once the VLAN is active, the configuration will work in system.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

Default vlan is always active.

[Example]

Set VLAN 2 active,exit VLAN configuration mode:

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

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

Raisecom(config)#

[Related commands]

Commands	Description
name	Name static VLAN.
state	Set active status of static VLAN.
show vlan	Show VLAN configuration information.

20.6 switchport access egress-allowed vlan

[Function]

set the VLAN that is allowed to pass in ACCESS mode

[Command Format]

Switchport access egress-allowed vlan {all | vlan-list / add add-vlan-list / remove remove-vlan-list}

No switchport access egress-allowed vlan

[Parameter]

all all vlan;

vlan-list vlan list, cover the configuration before directly;

add add the port allowed VLAN;

add-vlan-list the added VLAN list that is allowed to pass;

remove delete the VLAN that is allowed to pass;

remove-vlan-list the deleted VLAN list that are allowed to pass;

[Default]

By default only VLAN 1 is allowed to pass.

[Command Modes]

ethernet physical interface mode ; privileged user.

[Executing Command Instruction]

Use the command to set the VLAN list that is allowed to pass in ACCESS mode. In ACCESS mode the VLAN that are allowed to pass are all UNTAG VLAN. The configuration takes effect only to static VLAN, not to group VLAN, GVRP dynamic VLAN and etc.

When use set ACCESS allow VLAN list, it will inform user input 'y' for confirm; after user input 'y/Y' or ENTER the configuration will take effect, or if you input other value, the configuration will not take effect.

[Explanation of command execution echo]

Set unsuccessfully on port PORTID!

Set successfully.

[Example]

Allow VLAN 1, 3, 100 that is allow to pass in ACCESS mode

Raisecom(config-port)# **switchport access egress-allowed vlan 1,3,100**

Retore to default configuration

Raisecom(config-port)#**no switchport access egress-allowed vlan**

[Related commands]

Commands	Description
switchport access vlan	set port ACCESS VLAN ID
Switchport mode	Set port VLAN mode
show interface port <i>portlist switchport</i>	show port related VLAN configuration
Show vlan	Show VLAN configuration

20.7 switchport access vlan

[Function]

Set the ACCESS VLAN ID for the port.

[Command Format]

switchport access vlan <1-4094>

no switchport access vlan

[Parameter]

<1-4094>: Specify the ACCESS VLAN ID when port is set to ACCESS, EXTEND-ACCESS、DOT1Q-TUNNELmode.

[Default]

Default value is 1.

[Command Modes]

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

[Executing Command Instruction]

Specify the ACCESS VLAN ID when port is set to ACCESS, EXTEND-ACCESS, DOT1Q-TUNNEL mode. To UNTAG packet, use this value to mark TAG, port will give up TAG when transmit VLAN.

User can use **no switchport access vlan** command to recover default setting.

[Explanation of command execution echo]

Set unsuccessfully on port PORTID!

Set successfully.

[Example]

Set ACCESS VLAN ID of the port to 3:

Raisecom(config-port)# **switchport access vlan 3**

Recover ACCESS VLAN:

Raisecom(config-port)#**no switchport access vlan**

[Related commands]

Commands	Description
switchport hybrid allowed vlan	Set allowable VLAN when port is set to HYBRID mode.
switchport hybrid untagged vlan	Set allowable UNTAG VLAN when port is set to HYBRID mode.
switchport mode	Set the VLAN mode of the port.
switchport native vlan	Set the NATIVE VLAN when port is set to HYBRID or TRUNK mode.
switchport trunk allowed vlan	Set the allowable VLAN when port is set to TRUNK mode.
show interface port portlist switchport	Set port relevant VLAN setting.

20.8 switchport mode

[Function]

Set the VLAN mode for the port.

[Command Format]

switchport mode { *access* / *hybrid* [*double-tagging* / *dot1q-tunnel*] /
trunk [*double-tagging*] / *dot1q-tunnel* }

no switchport mode

[Parameter]

access: ACCESS mode, set port as UNTAG mode to sole VLAN;

hybrid: HYBRID mode, set the port as UNTAG or TAG mode to several VLAN;

hybrid dot1q-tunnel: set the port as HYBRID mode and enable the port add external Tag (SP Vlan Tag) for the packet entering the port by force (ignore the possibility that external or internal TAG may exist in packet);

trunk: TRUNK mode, set the port as TAG mode to several VLAN, as UNTAG mode in several Native vlan;

trunk double-tagging: set port as TRUNK mode and enable the port ability of recognizing and dealing with external Tag (SP Vlan Tag);

dot1q-tunnel: TUNNEL mode, the packets enter from this port can be marked double Tag.

Thereinto, all ISCOM series switches are in support of **access|hybrid|trunk** mode.

dot1q-tunnel, hybrid tunnel and double tag modes are supported by switches in type of ISCOM2826E/2828F/2852/2812GF/2924GF/2926/3026E/3028F/3052/3012GF/2109/2009 /2126S/2009A/2109A/2118.

[Default]

All the port default as EXTEND-ACCESS mode in VLAN 1.

[Command Modes]

Ethernet Physical port configuration mode; privileged user.

[Explanation of command execution echo]

Set unsuccessfully on port PORTID!

Set successfully.

[Executing Command Instruction]

When the port of the switch is connected to the terminal users, port can be set to ACCESS mode; port can be set to EXTEND-ACCESS mode when port is cascade mode but it isolated from other VLAN, and it can transmit default vlan and cluster vlan packet, port can be set to

DOT1Q-TUNNELmode when switch port is the ingress port of Q-in-Q network; port can be set to HYBRID mode when user want to set the VLAN hybrid mode of the port; when the port of switch is set to uplink TAG port, set it to TRUNK mode.

User can use **no switchport mode** to recover default setting.

[Example]

Set the port VLAN mode to be ACCESS mode:

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

Recover port VLAN mode:

```
Raisecom(config-port)#no switchport mode
```

[Related commands]

Commands	Description
switchport access vlan	Set the ACCESS VLAN ID of the port
switchport hybrid untagged vlan	Set the UNTAG VLAN when port is set to HYBRID mode.
switchport hybrid allowed valn	Set the allowed vlan when port is HYBRID mode.
switchport native vlan	Set the NATIVE VLAN when port is set to HYBRID or TRUNK mode.
switchport trunk allowed vlan	Set the allowed VLAN when port is set to TRUNK mode.
show interface port portlist switchport	Set port relevant VLAN configuration.

20.9 switchport trunk allowed vlan

[Function]

Set allowed VLAN when port is TRUNK mode.

[Command Format]

```
switchport trunk allowed vlan {all | vlan-list | add add-vlan-list |  
remove remove-vlan-list}
```

```
no switchport trunk allowed vlan
```

[Parameter]

all: all VLAN;

{1-4094}: VLAN list, overlay the former configuration directly;

add: add vlan base on the existent vlan;

add-vlan-list: add vlan list;

remove: remove vlan base on the existent vlan;

remove-vlan-list: remove vlan list.

[Default]

Default to be all.

[Command Modes]

Ethernet Physical port configuration mode; privileged user

[Explanation of command execution echo]

Set unsuccessfully on port PORTID!

Set successfully.

[Executing Command Instruction]

Set allowed VLAN when port is TRUNK mode.

Use **no switchport trunk allowed vlan** command to recover default setting.

[Example]

Set the allowed VLAN 2,3,100 when port is set to TRUNK mode:

Raisecom(config-port)# **switchport trunk allowed vlan 2-3,100**

Recover default setting:

Raisecom(config-port)#**no switchport trunk allowed vlan**

[Related commands]

Commands	Description
switchport access vlan	Set the ACCESS VLAN ID of the port
switchport hybrid	Set the UNTAG VLAN when port is set to

untagged vlan	HYBRID mode.
switchport hybrid allowed valn	Set the allowed vlan when port is HYBRID mode.
switchport mode	Set VLAN mode for the port.
switchport native vlan	Set the NATIVE VLAN when port is set to HYBRID or TRUNK mode.
show interface port portlist switchport	Set port relevant VLAN configuration.

20.10 switchport trunk native vlan

[Function]

Set port allowed VLAN in trunk mode

[Command Format]

switchport trunk native vlan

no switchport trunk native vlan

[Parameter]

Vlanid VLAN ID <1-4094>

[Default]

Default to be all.

[Command Modes]

Ethernet Physical port configuration mode; privileged user

[Explanation of command execution echo]

Set unsuccessfully on port PORTID!

Set successfully

[Executing Command Instruction]

Set native VLAN in trunk mode. In this mode, the untagged message coming into the port will use native VLAN tag, while the messages coming out will drop the tag.

Use **no switchport trunk native vlan** to restore to default configuration.

[Example]

Set native vlan to 3 in trunk mode

Raisecom(config-port)# **switchport trunk native vlan 3**

Restore to default configuration

Raisecom(config-port)#**no switchport trunk native vlan**

[Related commands]

Commands	Description
Switchport	Set trunk mode
trunk allowed	allowed VLAN list
vlan	
Switchport	Set trunk mode allowed
trunk untag	VLAN list
vlan	
Show interface	Show port related
port <i>portlist</i>	VLAN configuration
switchport	
Show vlan	Show VLAN
	configuration

20.11 switchport trunk untagged vlan

[Function]

Configure port allowed UNTAG VLAN in trunk mode

[Command Format]

switchport trunk untagged vlan {**all** | *vlan-list* | **add** *add-vlan-list* |
remove *remove-vlan-list*}

no switchport trunk untagged vlan

[Parameter]

all: all VLAN;

vlan-list: VLAN list, override the former configuration directly;

add: add vlan base on the existent vlan;

add-vlan-list: add vlan list;

remove: remove vlan base on the existent vlan;

remove-vlan-list: remove vlan list.

[Default]

By default UNTAG VLAN is VLAN 1

[Command Modes]

Ethernet Physical port configuration mode/port range mode; privileged user

[Explanation of command execution echo]

Set unsuccessfully on port PORTID!

Set successfully.

[Executing Command Instruction]

Use the command to set UNTAG VLAN that is allowed to pass in trunk mode. The configuration takes effect only to static VLAN, not to group VLAN or GVRP dynamic VLAN.

When user set trunk allowed VLAN list, it will inform user 'please input 'y' to confirm allowed VLAN, input 'y/Y' or ENTER for confirm so that the configuration can take effect, or the configuration will not take effect.

[Example]

Set UNTAGGED VLAN 1, 3, 100 in trunk mode

Raisecom(config-port)#**switchport trunk untagged vlan** 1, 3, 100

Restore to default configuration

Raisecom(config-port)#**no switchport trunk untagged vlan**

[Related commands]

Commands	Description
Switchport mode	Set port VLAN mode
Switchport trunk	Set trunk mode NATIVE VLAN

native vlan	
Switchport trunk allowed vlan	Set trunk mode allowed VLAN list
Show vlan	Show VLAN configuration

20. 12 vlan

[Function]

Create VLAN or enter static VLAN mode.

[Command Format]

vlan <3-4094>

vlan <3-4094> {*client*/*line*} [*<1-MAXPORT>*] <0-7> Supporting
device type: RC5X1

no vlan {**all** | <3-4094>}

[Parameter]

<3-4094>: VLAN ID;

<0-7>: priority;

client: client port;

line: line port;

all: All the static VLAN except default VLAN(VLAN ID is 1).

[Default]

By default, there are default VLAN and cluster VLAN available in the system, that is VLAN 1 and VLAN 2. All the ports are saved in VLAN 1 as extend-access mode.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

The user use command VLAN to enter configuration mode of static VLAN, if referenced VLAN is not available, system will create automatically. The state of static VLAN newly created is hung up, user

must activate it's configuration in configuration mode and quit configuration mode of VLAN, the referenced mode will be enabled.

User can use **no vlan** to delete static VLAN in the system.

[Example]

Enter configuration mode of static VLAN 4094:

```
Raisecom(config)# vlan 4094
```

Delete VLAN 3 form system:

```
Raisecom(config)#no vlan 3
```

[Related commands]

Commands	Description
name	The name static VLAN.
state	Set activation state of static VLAN.
shutdown	Show configuration of VLAN.



Chapter 21 QinQ and VLAN

Configuration Commands

21.1 mls double-tagging tpid

[Function]

Set/recover outer layer TAG TPID

[Command Format]

mls double-tagging tpid *HHHH*

no mls double-tagging tpid

[Parameter]

tpid: TPID;

HHHH: value of TPID, hexadecimal number, in range of 0x0000-0xFFFF.

[Command Modes]

Global configuration mode, privileged user (15)

[Executing Command Instruction]

Use this command to configure outer layer TAG TPID in global configuration mode; use no format command to recover default value and TPID is 0x8100 by default.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Set 0x9100 for outer layer TAG TPID:

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

Recover default value for outer layer TAG TPID:

Raisecom(config)# **no mls double-tagging tpid**

[Related commands]

Commands	Description
show switchport qinq	Show basic QinQ configuration information of port.

21.2 show interface vlan-mapping add-outer

[Function]

Show interface QinQ add TAG VLAN mapping rules.

[Command Format]

show interface port [*portid*] **vlan-mapping add-outer**

show interface line [*lineid*] **vlan-mapping add-outer**

show interface client [*clientid*] **vlan-mapping add-outer**

[Parameter]

vlan-mapping: VLAN mapping;

add-outer: add outer layer TAG;

portid: port id;

lineid: line port id;

clientid: client port id;

[Command Modes]

Any configuration mode; privileged user (10)

[Executing Command Instruction]

Use this command to show interface QinQ add TAG VLAN mapping rules in any configuration mode.

[Explanation of command execution echo]

<i>Port</i>	<i>Hw Status</i>	<i>Outer VLAN ID</i>	<i>Inner VLAN List</i>

<i>1</i>	<i>Enable</i>	<i>100</i>	<i>1-10</i>

[Example]

Set QinQ VLAN mapping rules at port 10:

```
Raisecom(config-port)# show interface port 10 vlan-mapping
add-outer
```

[Related commands]

Commands	Description
switchport vlan-mapping <i>vlanlist add-outer vlanid</i>	Configure QinQ add TAG VLAN mapping rules.
no switchport vlan-mapping add-outer <i>vlanid</i>	Delete QinQ add TAG VLAN mapping rules.
show interface line [<i>lineid</i>] vlan-mapping add-outer	Show QinQ add TAG VLAN mapping rules of line port.
show interface client [<i>clientid</i>] vlan-mapping add-outer	Show QinQ add TAG VLAN mapping rules of client port.

21.3 show interface vlan-mapping translate

[Function]

Set the interface VLAN translate rules.

[Command Format]

```
show interface port [portid] vlan-mapping {ingress | egress} translate

show interface line [lineid] vlan-mapping {ingress | egress} translate

show interface client [clientid] vlan-mapping {ingress | egress}
translate
```

[Parameter]

vlan-mapping: VLAN mapping;

ingress: ingress;

egress: egress;

translate: translate;

portid: port id;

lineid: line port id;

clientid: client port id;

[Command Modes]

Any configuration mode; privileged user (10)

[Executing Command Instruction]

Use this command to show interface VLAN translate rules in any configuration mode.

[Explanation of command execution echo]

Direction: Ingress

<i>Port</i>	<i>Outer VLAN ID</i>	<i>Customer VLAN List</i>	<i>Provider VLAN List</i>
-------------	----------------------	---------------------------	---------------------------

<i>1</i>	<i>100</i>	<i>1-10</i>	<i>50</i>

[Example]

Set VLAN translate rules at port 5:

Raisecom(config-port)# **show interface port 5 vlan-mapping ingress translate**

[Related commands]

Commands	Description
switchport vlan-mapping {ingress egress} <i>vlanlist</i> translate <i>vlanid</i>	Configure VLAN translate rules.
switchport vlan-mapping ingress outer {all <i>vlanlist</i>} inner {all <i>vlanlist</i>} translate outer <i>vlanid</i>	Configure VLAN translate rules.
no switchport vlan-mapping {ingress egress} translate <i>vlanid</i>	Delete VLAN translate rules.
show interface line [<i>lineid</i>] vlan-mapping ingress translate	Show VLAN translate rules of line port.
show interface client [<i>clientid</i>] vlan-mapping {ingress egress} tranlate	Show VLAN translate rules of client port.

21.4 show switchport qinq

[Function]

Show basic QinQ configuration information of port.

[Command Format]

show switchport qinq

[Parameter]

qinq: tag-in-tag

[Command Modes]

Any configuration mode; privileged user (10)

[Executing Command Instruction]

Use this command to show basic QinQ configuration of port in any configuration mode.

[Explanation of command execution echo]

```
Outer TPID: 0x9100

Port      QinQ Status
-----
1         Double-tagging
2         Dot1q-tunnel
3         --
4         --
```

[Example]

Show basic QinQ configuration information of port:

Raisecom(config-port)# **show switchport qinq**

[Related commands]

Commands	Description
no switchport qinq	Delete basic QinQ configuration information of port.
switchport qinq dot1q-tunnel	Enable basic QinQ function of port.

switchport qinq double-tagging

Enable double-tagging function of port.

21.5 switchport qinq dot1q-tunnel

[Function]

Enable/disable basic QinQ function of port.

[Command Format]

switchport qinq dot1q-tunnel

no switchport qinq

[Parameter]

qinq: tag-in-tag;

dot1q-tunnel: enable port TUNNEL function

[Default]

Basic QinQ function disables by default.

[Command Modes]

Interface or range interface configuration mode; privileged user (15)

[Executing Command Instruction]

Use this command to enable basic QinQ function of port in interface or range interface configuration mode. All ingress packets at the port will be added with TAG that is composed from default VLAN and TPID of port after enable QinQ function. Use no format command to disable QinQ function of port. The packets at port will be processed according to property of port after disable QinQ.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully on port XXX

[Example]

Enable basic QinQ function of port:

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

Disable basic QinQ function of port:

Raisecom(config-port)# **no switchport qinq**

[Related commands]

Commands	Description
show switchport qinq	Show basic QinQ configuration information of port.

21.6 switchport vlan-mapping add-outer

[Function]

Configure/delete QinQ add TAG VLAN mapping rules.

[Command Format]

switchport vlan-mapping *vlanlist* **add-outer** *vlanid*

no switchport vlan-mapping add-outer *vlanid*

[Parameter]

vlan-mapping: VLAN mapping;

vlanlist: inner VLANID of client network;

add-outer: add outer layer TAG;

vlanid: outer layer VLAN ID.

[Default]

Have not configured with VLAN mapping rule

[Command Modes]

Interface or range interface configuration mode; privileged user (15)

[Executing Command Instruction]

Use this command to configure QinQ add TAG VLAN mapping rules in interface or range interface configuration mode. If the input VLAN list repeats the existing VLAN mapping rules in one port, the configuration

will fail; the existing VLAN mapping rules will be deleted if VLAN ID corresponding VLAN mapping rule has already existed after translating, the later configured VLAN translate rule covers former one. Use no format command to delete interface QinQ add TAG VLAN mapping rule, the rule become invalid after deletion.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully on port XXX

Create vlan mapping rule unsuccessfully on port XXX on account of amount limit.

Vlan mapping rule conflict on port XXX

[Example]

Inner VLAN 3-8 add QinQ VLAN mapping rules for outer VLAN TAG 100:

Raisecom(config-port)# **switchport vlan-mapping 3-8 add-outer 100**

Delete QinQ VLAN mapping rules with outer VLAN TAG 100:

Raisecom(config-port)# **no switchport vlan-mapping add-outer 100**

[Related commands]

Commands	Description
show interface port [portid] vlan-mapping add-outer	Show interface QinQ add TAG VLAN mapping rules.
show interface line [lineid] vlan-mapping add-outer	Show line port QinQ add TAG VLAN mapping rules.
show interface client [clientid] vlan-mapping add-outer	Show client port QinQ add TAG VLAN mapping rules.

21.7 switchport vlan-mapping translate

[Function]

Configure/delete VLAN translate rules.

[Command Format]

switchport vlan-mapping {ingress | egress} *vlanlist* **translate *vlanid***

no switchport vlan-mapping {ingress | egress) **translate *vlanid***

[Parameter]

vlan-mapping: VLAN mapping;

ingress: ingress;

egress: egress;

vlanlist: inner VLAN IDs of client network;

translate: translate;

vlanid: outer layer VLAN ID;

[Default]

Have not configured with VLAN translate rule

[Command Modes]

Interface or range interface configuration mode; privileged user (15)

[Executing Command Instruction]

Use this command to configure VLAN translate rules in interface or range interface configuration mode. If the input VLAN list repeats the existing VLAN translate rules in one port, the configuration will fail; the existing VLAN translate rules will be deleted if VLAN ID corresponding VLAN translate rule has already existed after translating, the later configured VLAN translate rule covers former one. Use no format command to delete interface VLAN translate rule, the rule become invalid after deletion.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully on port XXX

Create vlan mapping rule unsuccessfully on port XXX on account of amount limit.

Vlan mapping rule conflict on port XXX

[Example]

Translate VLAN 5-10 TAG to VLAN translate rule of VLAN 100:

```
Raisecom(config-port)# switchport vlan-mapping ingress 5-10  
translate 100
```

Delete VLAN translate rule with outer TAG VLAN 100:

```
Raisecom(config-port)# no switchport vlan-mapping ingress translate  
100
```

[Related commands]

Commands	Description
switchport vlan-mapping ingress outer {all vlanlist} inner {all vlanlist} translate outer vlanid	Configure VLAN translate rules.
show interface port [portid] vlan-mapping {ingress egress} translate	Show VLAN translate rules of port.
show interface line [lineid] vlan-mapping {ingress egress} translate	Show line port VLAN translate rules.
show interface client [clientid] vlan-mapping {ingress egress} translate	Show client port VLAN translate rules.

Chapter 22 ACL and Network Security

Commands

22.1 access-list-map

[Function]

Create or delete access-list-map, use this command to enter ACL mapping table.

[Command Format]

access-list-map <0-399> {*permit* / *deny*}

no access-list-map <0-399>

[Parameter]

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

permit: Permit access if conditions are matched.

deny: Deny access if conditions are matched.

[Command Modes]

Global configuration mode; Privileged user.

[Executing Command Instruction]

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

[Explanation of command execution echo]

access list map 1 is used, can not modify deny or permit.

access list map 1 does not exist

access list map 1 is in use! The operation can't be completed!

[Example]

```
Raisecom(config)#access-list-map 1 deny
```

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

```
Raisecom(config)#no access-list-map 1
```

[Related commands]

Commands	Description
show access-list-map	Show access-list-map information.

22.2 clear filter statistics

[Function]

Clear filter statistics

[Command Format]

Clear filter statistics [*order*]

[Parameter]

Order: the serial number of filter

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

If the command does not have filter serial number, then all the filter statistic will be cleared; if it has, then only the statistics corresponding to the serial number.

[Explanation of command execution echo]

Set successfully

The command is executed successfully.

Set unsuccessfully

The command is executed unsuccessfully.

[Example]

Clear all the filter statistics:

```
Raisecom(config)#clear filter statistics
```

Clear the statistics information with filter number 1:

```
Raisecom(config)#clear filter statistic 1
```

[Related commands]

Command	Description
show filter	Show filter related information
filter enable disable	Enable/disable filter function

22.3 filter

[Function]

This command is used to add the filter rules. Use **no** form of this command to delete a filter rule. ISCOM 2826/3026 is not in support of the keyword **dougle-tagging**.

[Command format]

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

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

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

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

[Parameter]

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

all/{0-399}: Serial number of ACL, if “all”, it means all defined ACL;

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

ingress: filter at the receiving port;

egress: filter at the forwarding port;

from: the filtering receiving port at receiving port and forwarding port;

to: the filtering forwarding port at receiving port and forwarding port;

vlan-list<1-4094>: VLAN number;

double-tagging: filter rule is effective as per double TAG frame format.

[Command mode]

Global configuration mode; Privileged user.

[Executing Command Instruction]

This command is used to add one or more filter rules, the filter rule contains an ordered list of previous defined ACL or VLAN, the priority of these rules is decided by sequence of these filtering rules, the later the filtering rule is added, the higher priority it has. If there is conflicts when the switch tests the packets against the conditions in access list one by one, the higher priority filter rule will be effective (the later added rule). User should properly use all of these rules to limit the incoming packets.

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

[Explanation of command execution echo]

Set access list XX unsuccessfully

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

Set successfully

Set unsuccessfully

[Example]

Raisecom(config)#**filter ip-access-list 0 ingress portlist 5**

[Related commands]

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

22.4 filter {enable|disable}

[Function]

This command is used to enable filter function globally or disable the filter function.

[Command format]

filter *enable / disable*

[Parameter]

enable: Enable filtering function;

disable: Disable filtering function.

[Default]

Disable

[Command Modes]

Global configuration mode; Privileged user.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Raisecom(config)#**filter enable**

[Related commands]

Commands	Description
filter	Add filter rules into rule filter table.
show filter	Show related filter information.

22.5 ip-access-list

[Function]

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

[Command Format]

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

[Parameter]

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

permit: Permit access if conditions are matched.

deny: Deny access if conditions are matched.

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

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

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

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

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

[Command Modes]

Global configuration mode; Privileged user.

[Executing Command Instruction]

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

[Explanation of command execution echo]

The mask is wrong.

Set successfully

Set unsuccessfully

[Example]

Deny terminal device with source address 192.168.1.19 to ping other terminal device:

```
Raisecom (config)#ip-access-list 50 deny icmp 192.168.1.19  
255.255.255.255 any
```

[Related commands]

Commands	Description
no ip-access-list <i>{(0-399)/all}</i>	Delete all IP ACL entries.
show ip-access-list <i>{(0-399)}</i>	Show all the IP ACL entries.

22.6 mac-access-list

[Function]

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

[Command format]

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

[Parameter]

0-399: The number of MAC access control list;

permit: permit access if conditions are matched;

deny: deny access if conditions are matched;

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

HHHH.HHHH.HHHH / **any**: source MAC address, adopt dotted hexadecimal numeral, two characters for a group, any stands for any source MAC address;

HHHH.HHHH.HHHH / **any**: destination MAC address, adopt dotted hexadecimal numeral, two characters for a group, any stands for any destination MAC address.

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

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

[Explanation of command execution echo]

Set successfully

Set unsuccessfully!

[Example]

Raisecom (config)#**mac-access-list 10 deny any 1234.1234.1234**
1111.2222.3344

[Related commands]

Commands	Description
no mac-access-list (<i>{0-399}</i>)/ <i>all</i>)	Delete the speicified MAC access control list.
show mac-access-list [<i>{0-399}</i>]	Show information of specified MAC access control list.

22.7 match arp

[Function]

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

[Command format]

match arp opcode *{request / reply}*

match arp sender-mac *HHHH.HHHH.HHHH*

match arp target-mac *HHHH.HHHH.HHHH*

match arp sender-ip *A.B.C.D [A.B.C.D]*

match arp target-ip *A.B.C.D [A.B.C.D]*

no match arp opcode

no match arp sender-mac

no match arp target-mac *HHHH.HHHH.HHHH*

no match arp sender-ip

no match arp target-ip

[Parameter]

opcode: match ARP packet type.

request: match arp request packet.

reply: match arp reply packet.

sender-mac: match mac address of ARP sender.

target-mac: match ARP target hardware address.

HHHH.HHHH.HHHH: MAC address.

sender-ip: match IP address of ARP sender.

target-ip: match ARP target IP address.

ethertype: match layer 2 protocol type

A.B.C.D [A.B.C.D]: IP address (mask)

[Command mode]

ACLMap configuration mode; Privileged user.

[Executing Command Instruction]

Under access-list-map configuration mode, **match** command is used to define arp protocol match conditions. **Note**: there may be conflict during matching different types.

[Explanation of command execution echo]

Conflict with previous matches.

[Example]

```
Raisecom(config)# access-list-map 101 deny
```

```
Raisecom(config-aclmap)# match arp opcode request
```

```
Raisecom(config-aclmap)# match sender-mac 000e.5e23.4553
```

```
Raisecom(config-aclmap)# match sender-ip 10.0.0.0 255.0.0.0
```

```
Raisecom(config-aclmap)# no match arp opcode
```

[Related commands]

Commands	Description
show access-list-map [<i>acl-index</i>]	Show access-list-map information.

22.8 match ip

[Function]

Use this command to define ip protocol data matching of map table for

ACL.

[Command format]

match ip {*destination-address* / *source-address*} A.B.C.D [A.B.C.D]

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

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

match ip dscp {<0-63> / *af11* / *af12* / *af13* / *af21* / *af22* / *af23* / *af31* /
af32 / *af33* / *af41*/ *af42* / *af43* / *cs1* / *cs2* / *cs3* / *cs4* / *cs5* / *cs6* / *cs7* / *ef* /
default}

match ip no-fragments

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

match ip protocol <0-255>

no match ip {*destination-address* / *source-address*}

no match ip precedence

no match ip tos

no match ip dscp

no match ip no-fragments

no match ip protocol

[Parameter]

destination-address: match IP target address.

source-address: match IP source address.

precedence: match IP priority

<0-7>: IP priority value

routine: IP priority value is 0

priority: IP priority value is 1

immediate: IP priority value is 2

flash: IP priority value is 3

flash-override: IP priority value is 4

critical: IP priority value is 5

internet: IP priority value is 6

network: IP priority value is 7

tos: match IP TOS value

<0-15>: TOS value

normal: normal TOS value(0)

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

min-delay: minimum delay TOS value (8)

max-reliability: maximum reliable TOS value (2)

max-throughput: maximum throughput rateTOS value (4)

dscp: match IP dscp value.

<0-63>: ip dscp value.

af11: AF11 dscp value (001010)

af12: AF12 dscp value (001100)

af13: AF13 dscp value (001110)

af21: AF21 dscp value (010010)

af22: AF22 dscp value (010100)

af23: AF23 dscp value (010110)

af31: AF31 dscp value (011010)

af32: AF32 dscp value (011100)

af33: AF33 dscp value (011110)

af41: AF41 dscp value (100010)

af42: AF42 dscp value (100100)

af43: AF43 dscp value (100110)

cs1: CS1(priority 1) dscp value (001000)

cs2: CS2(priority 2) dscp value (010000)

cs3: CS3(priority 3) dscp value (011000)

cs4: CS4(priority 4) dscp value (100000)

cs5: CS5(priority 5) dscp value (101000)

cs6: CS6(priority 6) dscp value (110000)

cs7: CS7(priority 7) dscp value (111000)

default: default dscp value (000000)

ef: EF dscp value (101110)

no-fragments: match no-fragments packet

protocol: match IP protocol type.

<0-255>: P protocol type value.

ahp: Authentication Header protocol

esp: encapsulation security protocol

gre: general router encapsulation protocol

icmp: Internet Control Message Protocol

igmp: Internet Group message protocol

igrp: Interior gateway protocol

ipinip: IP-in-IP tunnel

ospf: Open Shortest-Path First

pcp: IP Payload Compression protocol

pim: Protocol Independent Multicast protocol

tcp: Transmission Control Protocol

udp: User Datagram Protocol

[Command format]

ACLMAP configuration mode; privileged user.

[Executing Command Instruction]

Under access-list-map configuration mode, **match** command is used to define IP protocol match conditions. Note: there may be conflict during matching different types. ToS or IP precedence and dscp confliction.

[Explanation of command execution echo]

Conflict with previous matches.

[Example]

Raisecom(config)# **access-list-map 101 deny**

Raisecom(config-aclmap)# **match ip destination-address 10.1.23.4.5**

Raisecom(config-aclmap)# **match ip precedence priority**

Raisecom(config-aclmap)# **match ip tos normal**

Raisecom(config-aclmap)# **match ip dscp 34**

Raisecom(config-aclmap)# **match ip no-fragments**

Raisecom(config-aclmap)# **match ip no-fragments**

Raisecom(config-aclmap)# **match ip ospf**

Raisecom(config-aclmap)# **no match ip protocol**

[Related commands]

Commands	Description
show access-list-map [<i>acl-index</i>]	Show access-list-map information.

22.9 match ip icmp

[Function]

Define icmp protocol match conditions.

[Command format]

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

[Parameter]

<0-255> [**<0-255>**]: ICMP message type.

[Command format]

ACLMap configuration mode; privileged user.

[Executing Command Instruction]

Under access-list-map configuration mode, **match** command is used to define IP ICMP protocol match conditions. Pay attention to the conflict among different types.

[Explanation of command execution echo]

Conflict with previous matchs.

[Example]

Raisecom(config)# **access-list-map 101 deny**

Raisecom(config-aclmap)# **match ip icmp 2 2**

Raisecom(config-aclmap)# **no match ip protocol**

[Related commands]

Commands	Description
show access-list-map [<i>acl-index</i>]	Show access-list-map information.

22.10 **match ip igmp**

[Function]

Use this command to define the IGMP protocol match condition.

[Command format]

match ip igmp {<0-255> / *dvmrp* / *query* / *leave-v2* / *report-v1* /

report-v2 /report-v3 /pim-v1}

[Parameter]

<0-255>: IGMP message type

dvmrp: Distance Vector Multicast Routing Protocol

leave-v2: IGMPv2 leave group

pim-v1: protocol individual message version 1

query: IGMP member query

report-v1: IGMPv1 member report

report-v2: IGMPv2 member report

report-v3: IGMPv3 member report

[Command Modes]

ACLMap configuration mode;Privileged user.

[Executing Command Instruction]

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

[Explanation of command execution echo]

conflict with previous matches.

[Example]

Raisecom(config)# **access-list-map 101 deny**

Raisecom(config-aclmap)# **match ip igmp query**

Raisecom(config-aclmap)# **no match ip protocol**

[Related commands]

Commands	Description
show access-list-map [<i>acl-index</i>]	Show access-list-map information.

Commands	Description
show access-list-map [<i>acl-index</i>]	Show access-list-map information.

22.11 match ip tcp

[Function]

Define the tcp protocol match conditions for ACL.

[Command Format]

```
match ip tcp { destination-port | source-port } { <0-65535> | bgp |
domain | echo | exec | finger | ftp | ftp-data | gopher | hostname | ident
| irc | klogin | kshell | login | lpd | nntp | pim-auto-rp | pop2 | pop3 |
smtp | sunrpc | syslog | tacacs | talk | telnet | time | uucp | whois |
www }
```

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

```
no match ip tcp { destination-port | source-port }
```

```
no match ip tcp {ack | fin | psh | rst | syn | urg }
```

[Parameter]

destination-port: match ip tcp Destination Port

source-port: match ip tcp source port

<0-65535>: tcp port number

bgp: Border Gateway Protocol (179)

domain: Domain Name Service (53)

echo: Echo protocol (7)

exec: Exec (rsh, 512)

finger: Finger (79)

ftp: file transmission protocol (21)

ftp-data: FTP data connection (20)

gopher: Gopher (70)

hostname: NIC hostname server (101)

ident: identification protocol (113)

irc: IRC protocol (194)

klogin: Kerberos login (543)

kshell: Kerberos shell (544)

login: Login (rlogin, 513)

lpd: printer service protocol(515)

nntp: Network News Transfer Protocol

pim-auto-rp: PIM Auto-RP (496)

pop2: Post Office Protocol Version 2(109)

pop3: Post Office Protocol Version 3 (110)

smtp: Simple Mail Transfer Protocol (25)

sunrpc: Remote Procedure Call protocol (111)

syslog: system log (514)

tacacs: TAC Acquisition and Control System (49)

talk: Talk (517)

telnet: Telnet (23)

time: Time (37)

uucp: Unix-to-Unix copy program (540)

whois: Nicname(43)

www: World Wide Web (HTTP, 80)

ack: match ACK

fin: match FIN

psh: match PSH

rst: match RST

syn: match SYN

urg: match URG

[Command format]

ACLMap configuration mode; privileged user.

[Executing Command Instruction]

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

[Explanation of command execution echo]

conflict with previous matchs.

[Example]

Raisecom(config)# **access-list-map 101 deny**

Raisecom(config-aclmap)# **match ip tcp destination-port smtp**

Raisecom(config-aclmap)# **match ip tcp source-port 6201**

Raisecom(config-aclmap)# **match ip tcp ack**

Raisecom(config-aclmap)# **match ip tcp fin**

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

Raisecom(config-aclmap)# **no match ip tcp fin**

[Related commands]

Commands	Description
show access-list-map [<i>acl-index</i>]	Show access-list-map information.

22.12 match ip udp

[Function]

Use this command to define udp protocol match conditions.

[Command format]

```
match ip udp { destination-port | source-port } { <0-65535> | biff |  
bootpc | bootps | domain | echo | mobile-ip | netbios-dgm | netbios-ns |  
netbios-ss | ntp | pim-auto-rp | rip | snmp | snmptrap | sunrpc | syslog  
| tacacs | talk | tftp | time | who }
```

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

[Parameter]

destination-port: match ip udp destination port

source-port: match ip udp source port

<0-65535>: udp port number

biff: Biff (mail notification, comsat, 512)

bootpc: boot protocol(BOOTP)client end (68)

bootps: boot protocol(BOOTP)server end (67)

domain: domain service protocol (53)

echo: echo protocol (7)

mobile-ip: mobile IP registration (434)

netbios-dgm: NetBios data message service (138)

netbios-ns: NetBios name service (137)

netbios-ss: NetBios session service (139)

ntp: Network Time Protocol (123)

pim-auto-rp: PIM Auto-RP (496)

rip: router information protocol(520)

snmp: Simple Network Management Protocol (161)

snmptrap: SNMP Traps (162)

sunrpc: Sun remote process control(111)

syslog: system log(514)

tacacs: TAC access control system (49)

talk: Talk (517)

tftp: Trivial File Transfer Protocol (69)

time: Time (37)

who: Who service (rwho, 513)

[Command Modes]

ACLMAP configuration mode; privileged use exec.

[Executing Command Instruction]

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

[Explanation of command execution echo]

Conflict with previous matchs.

[Example]

Raisecom(config)# **access-list-map 101 deny**

Raisecom(config-aclmap)# **match ip udp destination-port tacacs**

Raisecom(config-aclmap)# **match ip udp source-port 7306**

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

[Related commands]

Commands	Description
show access-list-map [<i>acl-index</i>]	Show access-list-map information.
show access-list-map [<i>acl-index</i>]	Show access-list-map information.

22.13 match user-define

[Function]

Define the user defined match conditions.

[Command format]

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

no match user-define

[Parameter]

MATCH-STRING: match data, hex string;

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

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

[Command Modes]

ACLMap configuration mode;Privileged user.

[Executing Command Instruction]

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

[Explanation of command execution echo]

Length of match data and mask is not equal!

The match data overrun the frame!

The match data is INVALID!

The mask data is INVALID!

[Example]

Raisecom(config)# **access-list-map 101 deny**

Raisecom(config-aclmap)# **match user-define a0 ff 24**

Raisecom(config-aclmap)# **no match user-define**

[Related commands]

Commands	Description
show access-list-map [<i>acl-index</i>]	Show access-list-map information.

22. 14 **match** (ACLMAP layer 2)

[Function]

Define the ACL layer-2 head data matching.

[Command format]

match mac {*destination/source*} *HHHH.HHHH.HHHH*

match cos <0-7>

match ethertype *HHHH* [*HHHH*]

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

no match mac {*destination/source*}

no match cos

no match ethertype

[Parameter]

mac: match layer 2 MAC address.

destination: match layer 2 destination MAC address.

source: match layer 2 source MAC address.

HHHH.HHHH.HHHH: MAC address.

cos: match cos value

ethertype: match the protocol type of layer 2

arp: match ARP

eapol: match eapol

flowcontrol: match flowcontrol

ip: match ip

ipv6: match ipv6

loopback: match loopback

mpls: match mpls unicast protocol.

mpls-mcast: match mpls multicast protocol.

pppoe: match pppoe

pppoedisc: match pppoe discovery protocol

x25: match x25 protocol.

x75: match x75 protocol.

[Command Modes]

ACLMAP configuration mode; privileged user.

[Executing Command Instruction]

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

[Explanation of command execution echo]

Conflict with previous matches.

[Example]

```
Raisecom(config)# access-list-map 101 deny
```

```
Raisecom(config-aclmap)# match mac destination 000e.5e11.2344
```

```
Raisecom(config-aclmap)# match cos 3
```

```
Raisecom(config-aclmap)# match ethertype 0800 ff00
```

```
Raisecom(config-aclmap)# match ipv6
```

```
Raisecom(config-aclmap)# no match cos
```

[Related commands]

Commands	Description
show access-list-map [<i>acl-index</i>]	Show access-list-map information.

22.15 show access-list

[Function]

This command is used to show the ACL information.

[Command format]

show (ip-access-list|mac-access-list) [{0-399}]

[Parameter]

ip-access-list/mac-access-list:The ACL type used by filtering rule.

{0-399}:Serial number of ACL, if the parameter is ignored, then that is the all the defined ACL.

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

This command is used to show the ACL information.

[Explanation of command execution echo]

Show the type of ACL, time for which is cited by the filtering rule, actual number of matching rule and other parameters.

[Example]

Show ip-access-list

Show mac-access-list 0-5

[Related commands]

Commands	Description
access-list	Relevant ACL
no access-list	Delete relevant ACL table.

22.16 show access-list-map

[Function]

This command is used to show ACL map table configured content for relevant type.

[Command format]

Show access-list-map *[0-399]*

[Parameter]

access-list-map:ACL map table

{0-399}:Serial number of ACL, if the parameter is ignored, then that is the all the defined ACL.

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

This command is used to show the configured content of ACL.

[Explanation of command execution echo]

Show the actual matching rule of ACL map.

[Example]

show access-list-map *10*

[Related commands]

Commands	Description
access-list-map	Define related ACL map table.
no access-list-map	Delete related ACL map table.

22.17 show filter

[Function]

This command is used to show the related information of filter.

[Command format]

show filter

[Command Modes]

Privileged EXEC

[Executing Command Instruction]

This command is used to show the related information of the filter. The content is shown based on the order of arrival, the earlier the ACL is added, the more frontal it is.

[Explanation of command execution echo]

Rule filter: Disable

Filter list(Larger order number, Higher priority):

Order ACL-Index IPort EPort VLAN Hardware

1 MAP 0 1 - - No

2 IP 0 - 3 - No

[Example]

show filter

[Related commands]

Commands	Description
filter	Put the filter rule into the rule filter table.
filter <i>enable / disable</i>	Start or cancel filter function.

Chapter 23 Commands of Storm-control

23.1 class-map(config)

[Function]

Create or delete class-map. Use this command can separate specific data flow and the matching conditions contain ACL, IP priority, DSCP and class, VLAN as well.

[Command Format]

class-map *class-map-name* [*match-all* / *match-any* / *double-tagging*]

no class-map *class-map-name*

[Parameters]

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

match-all: type of class-map, perform a logical-AND among all matches, default to be match-all.

match-any: type of class-map, perform a logical-OR among all matches.

double-tagging: type of class-map, the rule of this class-map definition will become effective as per double TAG frame format.

[Command Modes]

Global configuration mode; Privileged user.

[Executing Command Instruction]

Use the **class-map** command to separate specific data flow and the match criteria contain ACL, IP priority, DSCP and class, VLAN as well. Create a class-map by this command and enter (config-cmap) configuration view, match command can be used to define flow in the view. User need to assign type before creating a new class-map; if not, just enter

(config-cmap) configuration view.

[Explanation of command execution echo]

Create the class map successfully

Create the class map unsuccessfully

Delete the class map successfully

Delete the class map unsuccessfully

The input name is too long.

The class map does not exist.

The class map has existed.

[Example]

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

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

Raisecom(config)#**no class-map** aaa

[Related commands]

Commands	Description
show class-map [class-map-name]	Show class-map information.

23.2 class-map(config-pmap)

[Function]

In policy-map configuration mode, using **class-map** command to specify

a typical class-map and the service policy, the prompt will change to config-pmap-c after typing this command.

[Command format]

[no] class *class-map-name*

[Parameter]

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

[Command mode]

Policy-map (PMAP) configuration mode; Privileged user

[Executing Command Instruction]

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

[Explanation of command execution echo]

Set the class map successfully

Set the class map unsuccessfully

The input name is too long.

The class map does not exist.

[Example]

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

Raisecom(config-pmap-c)#**exit**

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

[Related commands]

Commands	Description
show policy-map [<i>policy-map-name</i>]	Show policy-map information.

23.3 clear service-policy statistics

[Function]

Clear QoS statistics information

[Command format]

clear service-policy statistics {**ingress** | **egress**} [*portid*] **class-map** [*cmap-name*]

clear service-policy statistics {**ingress** | **egress**} [*portid*]

clear service-policy statistics

clear service-policy statistics port [*portid*]

[Parameter]

Ingress | **egress**: stream direction

Portid: port number

Cmap-name: class name

[Command mode]

Global configuration mode; privileged user

[Executing Command Instruction]

- (1) clear the designated stream direction of the designated port and the statistics
- (2) clear the designated port policy statistics
- (3) clear all the policy statistics
- (4) clear designated port policy statistics

[Explanation of command execution echo]

Set unsuccessfully

Set successfully

[Example]

Clear the statistics of port 1, ingress, class is myclass

```
Raisecom(config)# clear service-policy statistics ingress 1 class-map  
myclass
```

Clear port 1 ingress statistics:

```
Raisecom(config)#clear service-policy statistics ingress 1
```

Clear all the delivered policy statistics

```
Raisecom(config)#clear service-policy statistics
```

[Related commands]

Commands	Description
Show service-policy statistics	Show policy statistics
Statistics enable disable	Enable/disable stream statistics

23.4 match

[Function]

It is used to define stream.

[Command format]

```
match { ip-access-list acl-index | mac-access-list acl-index |  
access-list-map acl-index | ip dscp dscp-list | ip precedence  
ip-precedence-list | class class-name | vlan vlanlist [double-tagging inner] }
```

```
no match { ip-access-list acl-index | mac-access-list acl-index |  
access-list-map acl-index | ip dscp | ip precedence | class class-name | vlan  
vlanlist }
```

[Parameter]

Ip-access-list acl-index – designate IP ACL number

Mac-access-list acl-index – designate MAC ACL number

Access-list-map acl-index- designate user defined ACL number

Ip dscp dscp-list- at the most 64 DSCP value can be designated, range is 0-63

Ip precedence *ip-precedence-list* – at most 8 IP priority value can be set, range is 0-7

Class *class-name-* designate class map name, the classmap can be only match-all type

Vlan *vlanlist-* designate VLAN ID, range is 1-4094

Double-tagging inner- it stands for the inner layer VLAN TAG

[Command Modes]

CMAP configuration mode; privileged user

[Executing Command Instruction]

Add the description information for policy map.

[Explanation of command execution echo]

Set the policy map description successfully

Set the policy map description unsuccessfully

The input name is too long.

[Example]

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

[Related commands]

Commands	Description
show policy-map [<i>policy-map-name</i>]	Show policy-map information.

23.5 mls qos mapping cos

[Function]

Configure the mapping from cos to local priority

[Command format]

mls qos mapping cos <*cosVal*> **to localpriority** <*localPriority*>

No mls qos mapping cos

[Parameter]

cosVal – cos value, range is 0-7

localPrioVal – local priority value, range is 0-7

[Parameter]

CoS value	0	1	2	3	4	5	6	7
Localpriority vaule	0	1	2	3	4	5	6	7

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Use the command to configure the mapping from cos to local priority

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Raisecom(config)# **mls qos mapping cos 5 to localpriority 3**

[Related commands]

Commands	Description
Show mls qos mapping cos	Show cos-localpriority mapping information

23.6 mls qos mapping dscp

[Function]

Configure the mapping from dscp to local priority

[Command format]

Mls qos mapping dscp <dscpVal> to localpriority <localPriority>

No mls qos mapping dscp

[Parameter]

dscpVal – dscp value, range is 0-63

localPrioVal – local priority value, range is 0-7

[Parameter]

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

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Use the command to configure the mapping from dscp to local priority

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Raisecom(config)# **mls qos mapping dscp 5 to localpriority 3**

[Related commands]

Commands	Description
Show mls qos mapping dscp	Show dscp-localpriority mapping information

23.7 mls qos port-priority

[Function]

Configure default priority and OVERRIDE

[Command format]

No mls qos port-priority <portPrioVal> [override]

[Parameter]

portPrioVal – designate default priority value for the port, range is 0-7, default value is 0

override – use port priority to replace the CoS value in the datapackets

[Default]

By default port-priority value is 0; override is disable

[Command Modes]

Port/range configuration mode; privileged user

[Executing Command Instruction]

Use the command to set default COS value and override function

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

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

Raisecom(config-port)# **mls qos port-priority 3**

Raisecom(config-port)# **mls qos port-priority 3 override**

Raisecom(config-port)# **no mls qos port-priority**

[Related commands]

Commands	Description
Show mls qos port	Show QoS port configuration

23.8 mls qos queue scheduler sp

[Function]

Show queue configuration

[Command format]

[No] mls qos queue scheduler

[Parameter]

None

[Default]

Default scheduler mode is SP

[Command Modes]

Privileged EXEC mode; privileged user

[Executing Command Instruction]

Show queue configuration

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Raisecom(config)# **mls qos queue scheduler sp**

Raisecom(config)#**no mls qos queue scheduler**

[Related commands]

Commands	Description
[no] mls qos queue {wrr drr wfq} <weightVal1> <weightVal2> <weightVal3> <weightVal4> [<weightVal5> <weightVal6> <weightVal7> <weightVal8>]	Configure schedule mode

23.9 mls qos queue scheduler wrr

[Function]

Show queue configuration

[Command format]

[No] mls qos queue scheduler

[Parameter]

None

[Default]

Default scheduler mode is SP

[Command Modes]

Privileged EXEC mode; privileged user

[Executing Command Instruction]

Show queue configuration

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Raisecom(config)# **mls qos queue scheduler wrr**

Raisecom(config)#**no mls qos queue scheduler**

[Related commands]

Commands	Description
[no] mls qos queue {wrr drr wfq} <weightVal1> <weightVal2> <weightVal3> <weightVal4> [<weightVal5> <weightVal6> <weightVal7> <weightVal8>]	Configure schedule mode

23.10 **mls qos queue wrr**

[Function]

Show queue configuration

[Command format]

[No] mls qos queue wrr <weightVal1> <weightVal2> <weightVal3>
<weightVal4> <weightVal5> <weightVal6> <weightVal7> <weightVal8>

[Parameter]

weightValn – queue DRR weight value, when the value is 0 it means SP
queue

[Default]

Default weight is 1

[Command Modes]

Privileged EXEC mode; privileged user

[Executing Command Instruction]

Show queue configuration

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Raisecom(config)# **mls qos queue wrr 10 10 5 5 8 10 1 2**

[Related commands]

Commands	Description
[no] mls qos queue scheduler {sp wrr drr wfq}	Configure schedule mode

23.11 mls qos trust port-priority

[Function]

Configure global or given port trust mode

[Command format]

mls qos trust port-priority

[Parameter]

None

[Default]

Default configuration is trust port-priority

[Command Modes]

Global/port configuration mode; privileged user

[Executing Command Instruction]

Use the command to configure global or given port trust mode

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Raisecom(config)# **mls qos queue trust port-priority**

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

Raisecom(config-port)#**mls qos trust port-priority**

[Related commands]

Commands	Description
Show mls qos	Show QoS configuration

23.12 **mls qos {aggregate-policer | class-policer | single-policer }**

[Function]

Configure policer.

[Command format]

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

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

[Parameter]

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

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

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

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

rate: limited speed, unit is Kbps.

burst: limited value of burst, unit is KB.

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

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

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

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

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

[Explanation of command execution echo]

Create the policer successfully.

Create the policer unsuccessfully.

Delete the policer successfully.

Delete the policer unsuccessfully.

The input name is too long.

The policer has not existed.

The policer has existed.

[Example]

```
Raisecom(config)# mls qos aggregate-policer sss 400 60 exceed-action  
drop
```

```
Raisecom(config)# mls qos aggregate-policer sss 400 60 exceed-action  
policed-dscp-transmit 3
```

```
Raisecom(config)# no mls qos aggregate-policer aaa
```

[Related commands]

Commands	Description
<code>show mls qos {aggregate-policer / class-policer / single-policer} [policer-name]</code>	Show policer information.

23.13 police

[Function]

Configure action for traffic.

[Command format]

```
[no] police policer-name
```

[Parameter]

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

[Command Modes]

PMAP-C configuration mode; privileged user.

[Executing Command Instruction]

Set the plastic action for the traffic.

[Explanation of command execution echo]

Apply the policer successfully.

Apply the policer unsuccessfully.

[Example]

Raisecom(config-pmap-c)#**police** aaa

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

[Related commands]

Commands	Description
show policy-map [<i>policy-map-name</i>]	Show policy-map information.

23.14 policy-map

[Function]

Create or delete **policy-map**.

[Command format]

[no] policy-map *policy-map-name*

[Parameter]

policy-map-name: specify the name of policy -map, maximum is 16 characters.

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

Use this command to create a policy-map and enter (config-pmap) configuration view. Use **set**, **trust** command to set the new priority for the traffic or set the new trust relationship under this view. One policy map can include several class map.

[Explanation of command execution echo]

Create the policy map successfully.

Create the policy map unsuccessfully.

Delete the policy map successfully.

Create the policy map unsuccessfully.

The input name is too long.

[Example]

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

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

Raisecom(config)# **no policy-map** *aaa*

[Related commands]

Commands	Description
show policy-map [<i>policy-map-name</i>]	Show policy-map information.

23.15 redirect-to port

[Function]

Configure the action of flow redirection.

[Command format]

redirect-to port *to-port*

no redirect-to port

[Parameter]

to-port: send the packet to the redirection port.

[Command Modes]

PMAP-C configuration mode; privileged user.

[Executing Command Instruction]

Configure the flow direction, packet meet this condition will be sent to redirection port, and don't send to the former forwarding port.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Raisecom(config-pmap-c)#**redirect-to port 3**

Raisecom(config-pmap-c)#**no redirect-to port**

[Related commands]

Commands	Description
show policy-map [<i>policy-map-name</i>]	Show policy-map information.

23. 16 service-policy

[Function]

Apply policy on the port.

[Command format]

service-policy *policy-map-name* **ingress** *portid* [**egress** *portlist*]

no service-policy *policy-map-name* **ingress** *portid*

[Parameter]

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

portid: ingress port ID

portlist: egress port ID

[Command Modes]

Global configuration mode; privileged user.

[Executing Command Instruction]

Apply the policy on the port. The setting is mutually exclusive with the trust on the port. If QoS still not has been started, setting doesn't work.

[Explanation of command execution echo]

Apply the policy successfully.

Apply the policy unsuccessfully.

The policy has attached on the port.

[Example]

Raisecom(config)# **service-policy** *aaa* **ingress** *1* **egress** *2-4*

Raisecom(config)#**no service-policy** *aaa* **ingress** *1*

[Related commands]

Commands	Description
show mls qos port [<i>portid</i>]	Show port information.

23. 17 set

[Function]

Configure the action of the traffic.

[Command format]

set { **ip dscp** *new-dscp* | **ip precedence** *new-precedence* | **cos** *new-cos* }

no set { **ip dscp** | **ip precedence** | **cos** }

[Parameter]

new-cos: modify the ingress packet cos value to a new value, and then classify the packets based on the new cos value.

new-dscp: first, change the ingress packet dscp value to a new value, then classify the packets based on the new dscp value.

new-precedence: first change the ingress packet precedence value to a new value, and then classify the packets based on the new value.

[Command Modes]

PMAP-C configuration mode; privileged user.

[Executing Command Instruction]

Users can set the action for the traffic and specify the new QOS value.

Set command and the **trust** (port mode and policy-map mode) command are mutually exclusive; it depends on which command is executed later.

[Explanation of command execution echo]

Set the dscp for the class map successfully.

Set the dscp for the class map unsuccessfully.

[Example]

Raisecom(config-pmap-c)#**set cos 3**

Raisecom(config-pmap-c)#**no set cos**

[Related commands]

Commands	Description
show policy-map [<i>policy-map-name</i>]	Show policy-map information.

23.18 show class-map

[Function]

Show class-map information.

[Command format]

show class-map [*class-map-name*]

[Parameter]

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

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Show class-map information.

[Explanation of command execution echo]

Raisecom#**show class-map**

Class Map match-any aaa (id 0)

Description:aaaaaaaaaaaaaaaa

Match none

[Example]

Raisecom# **show class-map**

[Related commands]

Commands	Description
class-map <i>class-map-name</i> [<i>match-all</i> / <i>match-any</i>]	Create class map.
description <i>WORD</i>	Set class map description information.
match	Set match announcement.

23. 19 show mls qos

[Function]

Show QoS configuration information.

[Command format]

show mls qos

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Show QoS configuration information.

[Explanation of command execution echo]

QOS is enabled:

Set the strict priority mode unsuccessfully.

Raisecom#**show mls qos**

[Example]

Raisecom# **show mls qos**

[Related commands]

Commands	Description
mls qos	Show the queue information.

23.20 **show mls qos mapping cos**

[Function]

Show CoS mapping configuration

[Command format]

Show mls qos mapping cos

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Show COS mapping configuration

[Explanation of command execution echo]

CoS-LocalPriority Mapping:

CoS:	0	1	2	3	4	5	6	7

LocalPriority:	0	1	2	3	4	5	6	7

[Example]

Raisecom# **show mls qos mapping cos**

[Related commands]

Commands	Description
Mls qos mapping cos <cosVal> to localpriority <localPrioVal>	Show COS to local priority mapping information

23.21 show mls qos mapping dscp

[Function]

Show dscp mapping configuration

[Command format]

Show mls qos mapping dscp

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Show DSCP mapping configuration

[Explanation of command execution echo]

DSCP-LocalPriority Mapping:

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

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

[Example]

Raisecom# show mls qos mapping dscp

[Related commands]

Commands	Description
Mls qos mapping cos <cosVal> to localpriority <localPrioVal>	Show COS to local priority mapping information

23.22 show mls qos mapping localpriority

[Function]

Show local priority to queue mapping configuraton

[Command format]

Show mls qos mapping localpriority

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Show DSCP mapping configuration

[Explanation of command execution echo]

LocalPriority-Queue Mapping:

LocalPriority:	0	1	2	3	4	5	6	7

Queue:	1	2	3	4	5	6	7	8

[Example]

Raisecom# **show mls qos mapping localpriority**

[Related commands]

None

23.23 show mls qos policer

[Function]

Show policer configuration information in QOS.

[Command format]

show mls qos policer [*police-name* | **aggregate-policer** |**class-policer** | **single-policer**]

[Parameter]

police-name: policer name.

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Show policer configuration information in QoS

[Explanation of command execution echo]

Raisecom#**show mls qos policer**

aggregate-policer bbb 50 500 exceed-action drop

Not used by any policy map

Raisecom#**show mls qos police aggregate-policer**

aggregate-policer bbb 50 500 exceed-action drop

Not used by any policy map

[Example]

Raisecom# **show mls qos policer**

[Related commands]

Commands	Description
mls qos {aggregate-policer class-policer single-policer} policername rate burst [exceed-action {drop policed-dscp-transmit dscp}]	Configure policer

23. 24 show mls qos port

[Function]

Show port configuration.

[Command format]

show mls qos port portlist

[Parameter]

portlist: port value range.

[Command Modes]

Global enable mode

[Executing Command Instruction]

This command show port configuration information.

[Explanation of command execution echo]

```
port          smac-policy          dmac-policy
vlan-policy

-----

<port-id>  < cos-override /          < cos-override /          <
cos-override /

          priority-set /          priority-set /          priority-set
/

cos-override & priority-set >          cos-override & priority-set >
cos-override & priority-set >
```

[Example]

Show configuration information of port 2 under global configuration mode:

```
Raisecom# show mls qos port 2
```

[Related commands]

Commands	Description
no vlan {2-4094} priority	Recover VLAN priority to default value.
vlan {2-4094} priority <0-7>	Configure VLAN priority.

23. 25 show mls qos queue

[Function]

Show queue configuration information.

[Command format]

```
show mls qos [ port portid] queue
```

[Parameter]

portid: port ID.

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Show queue configuration information.

[Explanation of command execution echo]

Raisecom#**show mls qos queueing**

the queue schedule mode: strict priority(SP)

wrr queue weights:

queueid-weights-delay

1 - 0 - 0

2 - 0 - 0

3 - 0 - 0

4 - 0 - 0

Cos-queue map:

cos-queueid

0 - 1

1 - 1

2 - 2

3 - 2

4 - 3

5 - 3

6 - 4

7 - 4

[Example]

Raisecom# **show mls qos port 1 queueing**

[Related commands]

Commands	Description
----------	-------------

Queue wrr-weight	Configure schedule mode.
Queue preempt-wrr	Configure schedule mode.
Queue strict-priority	Configure schedule mode.
Queue bounded-delay	Configure schedule mode.
Queue cos-map	Set the mapping from internal priority to queue.

23.26 show policy-map

[Function]

Show class-map information.

[Command format]

show policy-map [*policy-map-name*] [**class** *class-name*]

show policy-map port [*portId*]

[Parameter]

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

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

portid: port id

[Command Modes]

Privileged EXEC; privileged user.

[Executing Command Instruction]

Show policy-map information.

[Explanation of command execution echo]

Raisecom#**show policy-map port 1**

port 1:

Policy Map aaa:

Egerss:n/a

Class Map :aaa (match-any)

Raisecom#**show policy-map**

Policy Map aaa

Class aaa

police bbb

trust dscp

Raisecom#**show policy-map aaa class aaa**

Policy Map aaa

Class aaa

police bbb

trust dscp

[Example]

Raisecom# **show policy-map**

Raisecom# **show policy-map aaa**

Raisecom# **show policy-map class-map aaa**

Raisecom# **show policy-map aaa class-map aaa**

Raisecom# **show policy-map port 1**

[Related commands]

Commands	Description
Policy-map <i>policy-map-name</i>	Create policy map.
description <i>WORD</i>	Set policy map description information.
[no] class <i>class-map-name</i>	Apply class map on the policy.
set { ip dscp <i>new-dscp</i> ip precedence <i>new-precedence</i> cos <i>new-cos</i> }	Set the action.

[no] police <i>policer-name</i>	Apply policer.
trust [cos dscp ip-precedence]	Set the trust state for the traffic.

23.27 show service-policy statistics

[Function]

Show all the applied strategy statistics information

[Command format]

Show service-policy statistics

Show service-policy statistics port {portid}

[Parameter]

Portid – physical port ID

[Command Modes]

Privileged user

[Executing Command Instruction]

Use the command to show all the delivered Policy statistics

[Explanation of command execution echo]

Raisecom#**show service-policy statistics port 6**

PortID:6

Direction:Egress

PolicyName:ip-policy1

ClassName:class5

HwEnable:Yes

Unit:Pkts

PolicerName:agg-policy

PolicyerType:

Aggregate-policer

InprofilePkt64:5,567

OutprofilePkt64:1,887

Raisecom#**show service-policy statistics port 6**

PortID:6

Direction:Egress

PolicyName:ip-policy1

ClassName:class5

HwEnable:Yes

Unit:Bytes

PolicerName:agg-policy

PolicyerType:

Aggregate-policer

InprofilePkt64:7,567

OutprofilePkt64:1,887

[Example]

Raisecom# **show class-map**

[Related commands]

Commands	Description
Show policy-map	Show policy-map information

23. 28 trust cos

[Function]

Configure stream trust cos state (not supported yet)

[Command format]

Trust cos

No trust cos

[Parameter]

Cos – classify the ingress packets according to the CoS value. To untag packets, use port default CoS value, that is 0.

[Default]

Untrust

[Default]

PMap-C configuration mode; privileged user

[Executing Command Instruction]

Use the command to set the trusted packets cos

[Explanation of command execution echo]

Set the trust state for class map sucessfully

Set the trust state for the class map unsuccessfully

[Example]

Raisecom(config-pmap-c)#**trust cos**

Raisecom(config-pmap-c)#**no trust cos**

[Related commands]

Commands	Description
show policy-map [<i>policy-map-name</i>]	Show policy-map information.

23. 29 trust dscp

[Function]

Configure stream trust dscp state (not supported yet)

[Command format]

Trust dscp

No trust dscp

[Parameter]

DSCP – classify the ingress packets according to the DSCP value. To tag packets, use packets cos value; if they are untagged, use the packet default COS value. The switch will use CoS-to-DSCP mapping table to map CoS to DSCP

[Default]

Untrust

[Default]

PMAP-C configuration mode; privileged user

[Executing Command Instruction]

Use the command to set the stream trusted packets DSCP to be inner QoS priority

[Explanation of command execution echo]

Set the trust state for class map successfully

Set the trust state for the class map unsuccessfully

[Example]

Raisecom(config-pmap-c)#**trust dscp**

Raisecom(config-pmap-c)#**no trust dscp**

[Related commands]

Commands	Description
show policy-map [<i>policy-map-name</i>]	Show policy-map information.

Chapter 24 Dynamic ARP Inspection

Commands

24.1 debug dai

[Function]

Enable Dynamic ARP Inspection debugging function

[Command Format]

[no] debug dai

[Default]

Dynamic ARP Inspection debugging function is disabled on the equipment by default

[Command Modes]

Privileged EXEC mode. Privileged user.

[Executing Command Instruction]

Use **debug dai** to enable Dynamic ARP Inspection debugging function. Use **no debug dai** to disable Dynamic ARP Inspection debugging function.

[Explanation of command execution echo]

set successfully

When Dynamic ARP Inspection debugging function is enabled, the information above will be shown;

Set successfully

When Dynamic ARP Inspection debugging function is disabled, the information above will be shown.

[Example]

Enable Dynamic ARP Inspection debugging function on the equipment

Raisecom# **debug dai**

Disable Dynamic ARP Inspection debugging function on the equipment

Raisecom# **no debug dai**

[Related commands]

Command	Description
[no] ip arp-inspection static-config	Enable Dynamic ARP binding table rule function
[no] ip arp-inspection dhcp-snooping	Enable dynamic Dynamic DHCP Snooping binding table learning function
ip arp-inspection binding <i>A.B.C.D</i> <i>[HHHH.HHHH.HHHH]</i> [vlan <i>vlanid</i> port <i>port-id</i>	Configure static ARP binding table rule
no ip arp-inspection binding <i>A.B.C.D</i>	Delete static ARP binding table rule

24.2 ip arp-inspection

[Function]

Enable Static ARP Inspection binding table rule function

[Command Format]

[no] ip arp-inspection static-config

[Default]

Static ARP binding table rule function is disabled on the equipment by default

[Command Modes]

Global configuration mode; Privileged user.

[Executing Command Instruction]

Use **ip arp-inspection static-config** to enable static ARP binding table rule function. When the command is carried out, the configured static ARP inspection binding rule will take effect.

Use **no ip arp-inspection static-config** to disable static ARP binding table rule function. When the command is carried out, the configured static ARP inspection binding rule will take effect.

[Explanation of command execution echo]

Enable static config arp inspection successfully

When static ARP binding table rule is enabled, the information above will be shown;

Enable static config arp inspection unsuccessfully

When enabling static ARP binding table rule fails, the information above will be shown.

Disable static config arp inspection successfully

When static ARP binding table rule is disabled, the information above will be shown;

Disable static config arp inspection unsuccessfully

When disabling static ARP binding table rule fails, the information above will be shown.

[Example]

Enable static ARP binding table rule function on the equipment

Raisecom# **ip arp-inspection static-config**

Disable Dynamic ARP Inspection debugging function on the equipment

Raisecom# **no ip arp-inspection static-config**

[Related commands]

Command	Description
[no] ip arp-inspection dhcp-snooping	Enable dynamic Dynamic DHCP Snooping binding table learning function
ip arp-inspection binding A.B.C.D [HHHH.HHHH.HHHH] [vlan vlanid] port port-id	Configure static ARP binding table rule
no ip arp-inspection binding A.B.C.D	Delete static ARP binding table rule

show ip arp-inspection

Show ARP inspection global configuration and
port ARP trust configuration

24.3 ip arp-inspection trust

[Function]

Configure port trust ARP message

[Command Format]

[no] ip arp-inspection trust

[Default]

The port do not trust ARP message by default

[Command Modes]

Port configuration mode. Privileged user.

[Executing Command Instruction]

Use **ip arp-inspection trust** to configure port trust ARP message.

Use **no ip arp-inspection trust** to configure port distrust ARP message

[Explanation of command execution echo]

Set trust all arp packet on the port successfully

When configuring port trust ARP message successfully the message above will be shown

Set trust all arp packet on the port unsuccessfully

When configuring port distrust arp message unsuccessfully the message above will be shown

Set untrust all arp packet on the port successfully

When configuring port distrust ARP message successfully the message above will be shown

Set distrust all arp packet on the port unsuccessfully

When configuring port distrust arp message unsuccessfully the message above will be shown

[Example]

Configure trust ARP message under port

Raisecom(config-port)# **ip arp-inspection trust**

Configure distrust ARP message under port

Raisecom(config-port)# **no ip arp-inspection trust**

[Related commands]

Command	Description
show ip arp-inspection	Show ARP inspection global configuration and port ARP trust configuration

24.4 show ip arp-inspection

[Function]

Show the configured static ARP binding table rule function and dynamic DHCP Snooping binding table learning function enabling configuration.

Show port ARP message trust configuration

[Command Modes]

Privileged EXEC mode. Privileged user.

[Executing Command Instruction]

Use **show ip arp-inspection** to show ARP inspection global configuration and port ARP trust configuration

[Explanation of command execution echo]

Static Config ARP Inspection: *Enable*

DHCP Snooping ARP Inspection: *Enable*

Port *Trust*

1 no

2 no

.....

28 yes

show ip arp-inspection it means the operation is successful.

[Example]

Show ARP inspection global configuration and port ARP trust configuration:

Raisecom# **show ip arp-inspection**

[Related commands]

[no] ip arp-inspection static-config	Enable static ARP binding table rule configuration function
[no] ip arp-inspection dhcp-snooping	Enable dynamic DHCP Snooping binding table learning function
[no] ip arp-inspection trust	Configure port ARP trust



Chapter 25 — Keepalive Commands

25.1 show keepalive

[Function]

Show keepalive configuration

[Command format]

Show keepalive

[Parameter]

omitted

[Command Modes]

Enable mode; privileged user.

[Executing Command Instruction]

None

[Explanation of command execution echo]

None

[Example]

Show keepalive configuration:

Raisecom(config)#show keepalive

Keepalive Admin State: Disable

Keepalive trap interval: 300s

Keepalive trap count: 0

[Related commands]

Command	Description
snmp-server keepalive-trap (enable disable pause)	Show SNMP configuration
snmp-server keepalive-trap interval <120-28800>	Show keepalive configuration

25.2 snmp-server keepalive-trap

[Function]

Enable/disable send keepalive trap periodically.

[Command format]

snmp-server keepalive-trap {*enable/disable/pause*}

[Parameter]

enable: send keepalive trap periodically enable;

disable: send keepalive trap periodically disable, allowed loading;

pause: pause of sending keepalive and don't allowed loading.

[Default]

enable

[Command Modes]

Global configuration mode, Privileged user

[Executing Command Instruction]

The switch sends keepalive trap packets that contain basic information of the switch to make network management find the switch in very short time.

Use the command **snmp-server keepalive-trap** *disable* to stop sending and this command allowed loading.

Use the command **snmp-server keepalive-trap** *pause* to pause of

sending and this command don't allowed loading.

[Explanation of command execution echo]

Set successfully.

[Example]

Enable send keepalive trap periodically:

Raisecom(config)#**snmp-server keepalive-trap enable**

Disable send keepalive trap periodically:

Raisecom(config)#**snmp-server keepalive-trap disable**

[Related commands]

Commands	Description
show snmp config	Show basic information of snmp.

25.3 snmp-server keepalive-trap interval

[Function]

Set interval time for sending keepalive trap to SNMP network management, unit: second.

[Command format]

snmp-server keepalive-trap interval <120-28800>

no snmp-server keepalive-trap interval

[Parameter]

<120-28800>: interval of sending keepalive, unit: second.

[Default]

300 seconds

[Command Modes]

Global configuration mode, Privileged user

[Executing Command Instruction]

Use this command to set interval time for sending keepalive trap to

SNMP network management, unit: second.

[Explanation of command execution echo]

Set successfully.

[Example]

Send keepalive trap packet in interval of 500 seconds:

Raisecom(config)# **snmp-server keepalive-trap interval 500**

[Related commands]

Commands	Description
show snmp config	Show basic information of snmp.

Chapter 26 Unicast Router Commands

26.1 ip default-gateway

[Function]

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

[Command format]

ip default-gateway *A.B.C.D*

no ip default-gateway

[Parameter]

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

[Default]

No setting for gateway by default.

[Command Modes]

Global configuration mode; Privileged user

[Executing Command Instruction]

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

[Explanation of command execution echo]

Invalid next-hop IP address.

Can't Set gateway for cluster member.

Set successfully

[Example]

Set the default gateway to 10.0.0.1:

Raisecom(config)# **ip default-gateway** 10.0.0.1

Delete the configuration of default gateway:

Raisecom(config)# **no ip default-gateway**

[Related commands]

Commands	Description
show ip route	Show the system routing information.

26.2 ip route

[Function]

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

[Command format]

ip route *A.B.C.D₁* *A.B.C.D₂* *A.B.C.D₃*

no ip route *A.B.C.D₁* [*A.B.C.D₂*]

[Parameter]

A.B.C.D₁: network prefix;

A.B.C.D₂: mask;

A.B.C.D₃: next hop IP address;

A.B.C.D₁: network prefix;

A.B.C.D₂: mask.

[Default]

If command of **no** form has no network prefix, then delete all static routes.

If command of **no** form has no network mask, then delete all static routes that match to the prefix.

[Command Modes]

Global configuration mode; Privileged user

[Executing Command Instruction]

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

[Explanation of command execution echo]

Invalid destination IP address.

Invalid destination MASK.

Invalid next-hop IP address.

Can not set Connected Route to Static.

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

Can't add static route for cluster member

Inconsitent prifix and mask

No such static route !

Set successfully.

[Example]

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

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

Delete all static routes:

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

[Related commands]

Commands	Description
show ip route	Show information of route.

26.3 ip route aging-time

[Function]

Use the command **ip route aging-time** to set route aging time in hardware.

[Command format]

ip route aging-time <60-65535>

no ip route aging-time

[Parameter]

<60-65535>: Aging time (second).

[Default]

By default, the aging time is 180s

[Command Modes]

Global configuration mode, Privileged EXEC

[Executing Command Instruction]

Since hardware capacity is limit, route aging time periodically is needed. This command is used to set or recover aging-time period of route in hardware.

[Explanation of command execution echo]

set successfully.

[Example]

Set aging time to be 100 seconds:

Raisecom(config)#**ip route aging-time**100

Recover aging time to default value 180 seconds:

Raisecom(config)#**no ip route aging-time**

[Related commands]

Commands	Description
show ip route	Show route in hardware.

26.4 ip routing

[Function]

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

[Command format]

[no] ip routing

[Default]

The system disables ip packet transfer by software.

[Command Modes]

Global configuration mode; Privileged user

[Explanation of command execution echo]

Set successfully.

[Example]

Start the ip transfer function of software:

Raisecom(config)# **ip routing**

26.5 show ip protocol

[Function]

Show the global and configuration information of active RIP/OSPF interfaces.

[Command format]

show ip protocol

[Default]

Don't show any information if RIP/OSPF haven't started up.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

The information displayed by the **show ip protocols** command is useful in debugging router operations. Information in the Router Information Sources field of the **show ip protocols** output can help you identify a router suspected of delivering bad router information.

[Example]

Show 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

<i>IF index</i>	<i>Send</i>	<i>Recv</i>	<i>Metric</i>	<i>Auth-mode</i>	<i>Auth-key</i>	<i>State</i>

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

Distance(default is 120):120

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

[Related commands]

Commands	Description
router rip	Enable RIP.
network	Enable RIP on the specified network segment.
router ospf	Enable OSPF.
network	Specify the network to run OSPF.

26.6 show ip route

[Function]

Use **show ip route** to show the route of system route table.

[Command format]

show ip route { *connected* / *ospf* / *rip* / *static* / *hardware* }

[Parameter]

connected: straight connected router information;

ospf: ospf router information;

rip: rip router information;

static: static router information;

hardware: hardware router information.

[Default]

Show all the routers.

[Command Modes]

Privileged EXEC; privileged user

[Executing Command Instruction]

Use this command to show IP router information, can show different route information based on their types, also can show route information for particular network prefix. Also can use this command to show the route information in hardware transmit table.

[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

Total route count: 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

Total route count: 2

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

Total route count: 4

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*

Subnet route table

**H 11.0.0.0/255.0.0.0 VLAN=3 port=13 NextHopMAC=000E.5EB3.7305*

The total number of routes showed: 2 .

The total number of host routes: 8192, occupied host routes: 1.

The total number of network routes: 65536, occupied network routes: 1

[Related commands]

Commands	Description
ip route	Configure static IP route

Chapter 27 OAM Commands

27.1 clear oam event

[Function]

Clear OAM event information note.

[Command format]

clear oam event

[Command Modes]

Interface configuration mode, Privileged user

[Executing Command Instruction]

Log OAM event, including link event and fault event. This command will clear the entire event and log again.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Clear OAM event information note:

Raisecom(config-port)#**clear oam event**

[Related commands]

Commands	Description
show oam event	Show OAM statistic information.

27.2 clear oam statistics

[Function]

Clear OAM frame statistic.

[Command format]

clear oam statistics

[Command Modes]

Interface configuration mode, Privileged EXEC

[Executing Command Instruction]

Statistic transmission and receiving frame on OAM link, including frame types: information, link event note, loopback, variable request, variable response, organization private, unknown type and repeat link event notes. This command will clear the entire frame type statistics and start again from zero.

[Explanation of command execution echo]

Set successfully

[Example]

Clear link OAM frame statistic:

Raisecom(config-port)#**clear oam statistics**

[Related commands]

Commands	Description
show oam statistics	Show OAM frame statistic information.

27.3 oam enable

[Function]

Enable and disable OAM function.

[Command format]

oam {*disable* | *enable*}

[Parameter]

disable: disable OAM function;

enable: enable OAM function.

[Default]

Enable OAM function.

[Command Modes]

Interface configuration mode, Privileged EXEC

[Executing Command Instruction]

Open and close OAM link function. When OAM function enables and if the link interface is UP, it enter OAM discovery process immediately. When there is at least one OAM in subject mode at the link ends, OAM enters operational state after discovering successfully, use can manage and monitor by command provide by OAM.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

[Example]

Disable OAM link function:

Raisecom(port)#**oam disable**

Enable OAM link function:

Raisecom(port)#**oam enable**

[Related commands]

Commands	Description
show oam	Show OAM information.

27.4 oam peer event trap

[Function]

Enable and disable all OAM link event trap at the other end.

[Command format]

oam peer event trap {*disable* | *enable*}

[Default]

Disable the entire OAM link event trap at the other end.

[Command Modes]

Interface configuration mode, Privileged EXEC

[Executing Command Instruction]

Enable and disable all OAM link event trap for the other end.

If the OAM link event trap is enabled, OAM will send the trap to network management center when it receive OAM link event (OAM must be in master mode).

[Explanation of command execution echo]

Set successfully.

[Example]

Enable peer link OAM event trap:

Raisecom(port)#**oam peer event trap enable**

Disable peer link OAM event trap:

Raisecom(port)#**oam peer event trap disable**

[Related commands]

Commands	Description
show oam trap	Show OAM event trap information.

27.5 oam remote-loopback

[Function]

Enable and disable remote loopback function.

[Command format]

[no] oam remote-loopback

[Command Modes]

Privileged EXEC, interface configuration mode

[Executing Command Instruction]

This function helps to detecting network faults in time.

With remote loopback enabled, the OAM entity operating in active OAM mode issues remote loopback requests and the peer responds to them.

This function can only take effect when OAM work in master mode and operational state. It is only allow one link in loopback.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully. OAM discovery unsuccessfully complete.

Set unsuccessfully. There is another loopback.

Set unsuccessfully. There is a loopback on another interface.

Set unsuccessfully. The peer doesn't react.

Set unsuccessfully. OAM is passive.

Set unsuccessfully. There is no remote loopback.

[Example]

Startup link OAM remote loopback:

Raisecom(port)#**oam remote-loopback**

Stop link OAM remote loopback:

Raisecom(port)#**no oam remote-loopback**

[Related commands]

Commands	Description
show oam loopback	Show OAM loopback information.

27.6 show oam

[Function]

Review OAM basic function configuration.

[Command format]

show oam [**port-list** *port-list*]

[Parameter]

port-list: port list.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

Use this command to review link OAM basic information. Including local working mode, management state, maximal message length, configuration version and function in support.

[Explanation of command execution echo]

Raisecom#**show oam**

Port: 1

Mode: Active

Administrate state: Enable

Operation state: Disabled

Max OAMPDU size: 1518

Config revision: 0

Supported functions: Loopback, Event

.....

Raisecom#**show oam port-list 1**

Port: 1

Mode: Active

Administrate state: Enable

Operation state: Disabled

Max OAMPDU size: 1518

Config revision: 0

Supported functions: Loopback, Event

[Example]

Show basic information of the entire OAM links:

Raisecom#**show oam**

[Related commands]

Commands	Description
oam { <i>active</i> / <i>passive</i> }	Set OAM working mode.
oam { <i>disable</i> / <i>enable</i> }	Enable/disable OAM link.

27.7 show oam loopback

[Function]

Review OAM remote loopback information.

[Command format]

show oam loopback [**port-list** *port-list*]

[Parameter]

port-list: port list.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

Use this command to review link OAM remote loopback information.

Including local loopback state and loopback response enable condition.

[Explanation of command execution echo]

Raisecom#**show oam loopback**

Port: 1

Loopback status: No

Loopback react: Ignore

.....

Raisecom#**show oam loopback** *port-list 1*

Port: 1

Loopback status: No

Loopback react: Ignore

[Example]

Show loopback information of the entire OAM link:

Raisecom#**show oam loopback**

[Related commands]

Commands	Description
[no] oam remote-loopback	Start/stop OAM remote loopback.
oam loopback	Enable/disable OAM remote loopback response.

27.8 show oam peer

[Function]

Review peer OAM basic function configuration.

[Command format]

show oam peer [**port-list** *port-list*]

[Parameter]

port-list: port list.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

Uses this command to review peer link OAM basic information. The

showing information includes peer MAC address, manufacturer OUI, manufacturer information, mode setting, maximal message length, configuration version and supported functions. Show nothing if link OAM is in not operational state.

[Explanation of command execution echo]

Raisecom#**show oam peer**

Port: 1

Port: 2

Peer MAC address: 000E.5E40.6A22

Peer vendor OUI: 000E5E

Peer vendor info: 1

Peer mode: Passive

Peer max OAMPDU size: 1518

Peer config revision: 0

Peer supported functions: Loopback, Event, Variable

Port: 3

.....

Raisecom#**show oam peer port-list 2**

Port: 2

Peer MAC address: 000E.5E40.6A22

Peer vendor OUI: 000E5E

Peer vendor info: 1

Peer mode: Passive

Peer max OAMPDU size: 1518

Peer config revision: 0

Peer supported functions: Loopback, Event, Variable

[Example]

Show the peer link OAM basic information:

Raisecom#**show oam peer**

[Related commands]

Commands	Description
oam { <i>active</i> / <i>passive</i> }	Set OAM working mode.
oam { <i>disable</i> / <i>enable</i> }	Start/stop link OAM.

27.9 show oam peer event

[Function]

Review peer OAM reported event.

[Command format]

show oam peer event [**port-list** *port-list*]

show oam peer event critical

show oam peer event port-list *port-list* **critical**

[Parameter]

port-list: port list.

line-list: line port list;

client-list: client port list.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

Uses this command to review peer link OAM reported event, including link event and critical event.

The showing information includes peer locate link, event occur time, window, threshold, current value and event number. Critical event doesn't have window and threshold setting and current value items, so these items shows 0.

[Explanation of command execution echo]

Raisecom#**show oam peer event**

Port: 1

Port: 2

.....

Raisecom#**show oam peer event port-list 1**

Port: 1

Raisecom#**show oam peer event critical**

Port: 1

Port: 2

.....

Raisecom#**sh oam event port-list 1 critical**

Port: 1

[Example]

Show the entire link OAM event note:

Raisecom#**show oam peer event**

Show the entire peer link critical event note:

Raisecom#**show oam peer event critical**

[Related commands]

Commands	Description
----------	-------------

clear oam event	Clear event notification.
------------------------	---------------------------

27.10 show oam statistics

[Function]

Review OAM frame statistic information.

[Command format]

show oam statistics [**port-list** *port-list*]

[Parameter]

port-list: port list.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

Statistic transmission and receiving frame on OAM link, including frame types: information, link event note, loopback, variable request, variable response, organization private, unknown type and repeat link event notes. This command shows the frame type total received and transmitted by OAM since system boot or the last time frame statistic clear.

[Explanation of command execution echo]

Raisecom#**show oam statistics**

Port: 1

	<i>Tx</i>	<i>Rx</i>

<i>Information</i>	<i>: 0</i>	<i>0</i>
<i>Event notification</i>	<i>: 0</i>	<i>0</i>
<i>Loopback control</i>	<i>: 0</i>	<i>0</i>
<i>Variable request</i>	<i>: 0</i>	<i>0</i>
<i>Variable response</i>	<i>: 0</i>	<i>0</i>

Organization specific : 0 0

Unsupported codes : 0 0

Duplicate event notification : 0 0

Port: 2

Tx Rx

Information : 3655 500

Event notification : 0 0

Loopback control : 0 0

Variable request : 0 0

Variable response : 0 0

Organization specific : 3 500

Unsupported codes : 0 0

Duplicate event notification : 0 0

.....

Raisecom#show oam statistics port-list 2

Port: 2

Tx Rx

Information : 3982 500

Event notification : 0 0

Loopback control : 0 0

Variable request : 0 0

Variable response : 0 0

Organization specific : 3 500

Unsupported codes : 0 0

Duplicate event notification : 0 0

[Example]

Show the entire link OAM frame statistic information:

Raisecom#**show oam statistics**

Show the line 2 OAM frame statistic information:

Raisecom#**show oam peer statistics** *port-list* 2

[Related commands]

Commands	Description
clear oam statistics	Clear OAM frame statistic.

27.11 show oam trap

[Function]

Review OAM link event notify trap information.

[Command format]

show oam trap [**port-list** *port-list*]

[Parameter]

port-list: port list.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

The showing information contains link monitor event, peer link event trap enable condition and latest OAM loss and discover trap total as well as happen time.

[Explanation of command execution echo]

Raisecom#**show oam trap**

Port: 1

Event trap: Disable

Peer event trap: Disable

Discovery trap total: 0

Discovery trap timestamp: 0 days, 0 hours, 0 minutes

Lost trap total: 0

Lost trap timestamp: 0 days, 0 hours, 0 minutes

Port: 2

Event trap: Disable

Peer event trap: Disable

Discovery trap total: 1

Discovery trap timestamp: 0 days, 2 hours, 25 minutes

Lost trap total: 1

Lost trap timestamp: 0 days, 2 hours, 41 minutes

.....

Raisecom#show oam trap port-list 2

Port: 2

Event trap: Disable

Peer event trap: Disable

Discovery trap total: 1

Discovery trap timestamp: 0 days, 2 hours, 25 minutes

Lost trap total: 1

Lost trap timestamp: 0 days, 2 hours, 41 minutes

[Example]

Show the entire link OAM event notify trap information:

Raisecom#**show oam trap**

Show the line 1 OAM event notify trap information:

Raisecom#**show oam peer trap** *line 1*

[Related commands]

Commands	Description
oam event trap	Enable/disable link event trap notification.

Chapter 28 Extended OAM Commands

28.1 clear extended-oam statistics

[Function]

Clear extended OAM statistics.

[Command format]

clear extended-oam statistics [**line-list** *line-list*]

[Parameter]

line-list: line port list;

client-list: client port list.

[Command Modes]

Global configuration mode, Privileged user

[Executing Command Instruction]

Clear extended OAM statistics by this command. After operating this command, the entire types of extended OAM frame on the specified link statistic value clear to zero and start to statistic again.

[Explanation of command execution echo]

Set successfully

[Example]

Clear the entire link extended OAM frame statistic:

Raisecom(config-port)#**clear extended-oam statistics**

[Related commands]

Commands	Description
show extended-oam statistics	Show extended OAM frame statistics information.

28.2 description

[Function]

Set port description of remote device.

[Command format]

description line *line-id WORD*

description client *client-id WORD*

no description line *line-id*

no description client *client-id*

[Parameter]

line-id: Line port ID;

client-id: Client port ID.

[Command Modes]

Remote port configuration mode, Privileged user

[Executing Command Instruction]

Use this command to set description information under remote port configuration mode. **no** format command will delete this operation.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

The description is too long.

Set successfully.

[Example]

Set description for remote device user port 1 as “user A”:

Raisecom(config-remoteport)#**description client 1 userA**

Delete description of remote device user port 1:

Raisecom(config-remoteport)#**no description client /**

[Related commands]

Commands	Description
show interface port detail	Show details of remote device port.

28.3 download

[Function]

Download file from server or center device.

[Command format]

download {*bootstrap* | *system-boot* | *fpga*} *FILENAME*

download startup-config [*FILENAME*]

[Parameter]

bootstrap: system boot file;

system-boot: system startup file;

startup-config: system configuration file;

fpga: FPGA file;

FILENAME: filename on server or center device.

[Command Modes]

Interface configuration mode, Privileged user

[Executing Command Instruction]

This command can download the file from center device to remote device flash (it must be master for OAM mode).

The command **download** {*bootstrap* | *system-boot* | *fpga*} *FILENAME* download file from center site to remote device via expanded OAM protocol.

The command of **download startup-config** [*FILENAME*] download file from center site to remote device via expended OAM protocol. The file

name can also be undersigned and use the default name. Default name:
remote device type+ center OAM link ID+ suffix.

If remote device supports file transport: FILE_ID, for example
FILE_5.conf

Or else, the file name is FRAME_ID, for example FRAME_2.conf

[Explanation of command execution echo]

Waiting...Start

Getting source file...Done

Writing to destination...Done

Success!

Failed!(File name error)

Waiting...Start

Getting source file...

Failed!(mem alloc error)

Waiting...Start

Getting source file...

Failed!(File to operate too large error)

Waiting...Start

Getting source file...

Failed!(Unknown error)

Waiting...Start

Getting source file ...Done

Writing file to destination ...

Failed ! (Opening file failed)

Waiting...Start

Getting source file ...Done

Writing file to destination ...

Failed ! (File writing failed)

[Example]

Download system file to remote device from center device:

Raisecom(config-port)#**download** *system-boot system.Z*

Download configuration file to remote device from center device, using default file name:

Raisecom(config-port)#**download** *startup-config*

[Related commands]

Commands	Description
erase	Delete file in flash.
dir	Show the file storage in flash.
upload	File upload.

28.4 download remote

[Function]

Download the file from server to the flash of center device.

[Command format]

download { *remote-bootstrap* / *remote-system-boot* /
remote-startup-config / *remote-fpga* } *ftp A.B.C.D USERNAME*
PASSWORD FILENAME LOCAL-FILENAME

download { *remote-bootstrap* / *remote-system-boot* /
remote-startup-config / *remote-fpga* } *tftp A.B.C.D FILENAME*

LOCAL-FILENAME

[Parameter]

remote-bootstrap: system boot file of remote device;

remote-system-boot: system startup file of remote device;

remote-startup-config: system configuration file of remote device;

remote-fpga: FPGA file of remote device;

tftp: download via tftp protocol;

ftp: download via ftp protocol;

A.B.C.D: IP address of server;

USERNAME: user name of ftp server;

PASSWORD: password of ftp server;

FILENAME: file name of server and device;

LOCAL-FILENAME: file name of center device.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

This command can download the file (bootstrap , system-boot , startup-config and fpga file) from server to center device flash. These files will be added with suffix automatically as following:

ile	u
typ	f
e	f
	i
	x

yste
m-b
oot

Z

tart
up-
con
fig

c
o
n
f

oots
trap

b
o
o
t

pga

v
m

The command can not run successfully if the file name is identical to default file name in center flash. That is to say, remote system boot file should not named as system-boot; configuration file should not named as startup-config; FPGA file should not named as fpga. Since the center device system bootstrap file is not saved in flash, the boot file of remote can named as bootstrap.

[Explanation of command execution echo]

Waiting...Start

Getting source file...Done

Writing to destination...Done

Success!

Failed! (Invalid IP Address)

Failed!(User name error)

Failed!(Password error)

Failed!(File name error)

Waiting...Start

Connecting to server failed

Failed !

Waiting...Start

Getting source file...

Failed!(Open file error)

Waiting...Start

Getting source file...

Failed!(Time Out error)

Waiting...Start

Getting source file...

Failed!(mem alloc error)

Waiting...Start

Getting source file...

Failed!(File to operate too large error)

Waiting...Start

Getting source file...

Failed!(Unknown error)

Waiting...Start

Getting source file ...Done

Writing file to destination ...

Failed ! (Opening file failed)

Waiting...Start

Getting source file ...Done

Writing file to destination ...

Failed ! (File writing failed)

[Example]

Download remote system boot file from server to center file system by tftp protocol:

```
Raisecom#download remote-system-boot tftp 10.168.0.11 sys1.z system1
```

Download remote system boot file from server to center file system by ftp protocol:

```
Raisecom#download remote-startup-config ftp 10.168.0.11 user user  
start.conf start2
```

[Related commands]

Commands	Description
erase	Delete specified file in flash.
dir	Show the file storage in flash.
upload	File upload.

28.5 duplex

[Function]

Use **duplex** command to set duplex mode of the client ports.

[Command format]

```
duplex { full | half }
```

[Parameter]

full: full-duplex;

half: half-duplex.

[Command Modes]

Remote port configuration mode; Privileged user

[Executing Command Instruction]

Use this command to configure remote client port duplex mode under remote port configuration mode. Different type of physical port can configure different duplex modes.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Set successfully

[Example]

Configure the remote user port to be half-duplex:

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

[Related commands]

Commands	Description
speed <i>(auto 10 100 1000)</i>	Configure remote device speed.
show interface port	Show remote port information.
show interface port detail	Show details of remote port.

28.6 erase

[Function]

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

[Command format]

erase

[Command Modes]

Remote configuration mode and privileged user

[Executing Command Instruction]

Use **erase** to delete the designated file in remote flash file system under remote configuration mode. After reboot remote device, recover default configuration. Run this command need to input “yes” for confirmation.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Erase specified file..

Erase remote configuration file successfully

Erase specified file..

Remote device X erase configuration file unsuccessfully

[Example]

Raisecom(config-remote)#**erase**

[Related commands]

Commands	Description
Write	Save the system configuration of remote device.

28.7 extended-oam notification

[Function]

Enable and disable extended OAM notification.

[Command format]

expanded-oam notification *enable*

expanded-oam notification *disable*

[Parameter]

enable: enable extended OAM notification;

disable: disable extended OAM notification.

[Default]

Enable extended OAM information.

[Command Modes]

Global configuration mode, Privileged user

[Executing Command Instruction]

Enable and disable extended OAM notification. If the OAM passive mode is enabled in local, it will send extended OAM notification. Or else it will not send. If it is active mode in local, expanded OAM notification will be send no matter the function is enabled.

[Explanation of command execution echo]

Set successfully.

[Example]

Raisecom(config)#**extended-oam notification** *disable*

[Related commands]

Commands	Description
show extended-oam notification	Show OAM information frame configuration

28.8 **fault-pass**

[Function]

Enable/disable fault pass function.

[Command format]

fault-pass enable

fault-pass disable

fault-pass enable to client *client-portlist*

fault-pass disable to client *client-portlist*

[Parameter]

enable: enable fault pass;

disable: disable fault pass;

client-portlist: user port list.

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

Use this command under remote configuration mode to enable/disable remote fault pass. For remote RC551, users can designate port transfer the fault to or cancel the ports not transfer to anymore, default to not designate port list transfer to and enable fault transfer to all ports or cancel all transfer ports. Remote RC552 is not in support of designating port transfer to.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Remote device X should not specify fault-pass port list

Set successfully

[Example]

Enable remote fault pass function, pass the fault to all user ports:

Raisecom(config-remote)#**fault-pass enable**

Disable pass fault to client port 1:

Raisecom(config-remote)#**fault-pass** *disable to client 1*

[Related commands]

Commands	Description
show interface port detail	Show detail information of remote port.

28.9 flowcontrol

[Function]

Enable or disable the flow control function at the remote client port.

[Command format]

flowcontrol on

flowcontrol off

[Parameter]

on: Enable flow control function;

off: Disable flow control function.

[Command Modes]

Remote configuration mode; Privileged user

[Executing Command Instruction]

Enable or disable the flow control function at the remote client port under remote port configuration mode.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Set successfully

[Example]

Disable flowcontrol of remote client port:

Raisecom(config-remoteport)#**flowcontrol** *off*

Enable remote client port:

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

[Related commands]

Commands	Description
show interface port	Show information of remote ports.
show interface port detail	Show details of remote ports.

28. 10 hostname

[Function]

Use **hostname** command to configure system name of remote host.

Use **no hostname** command to recover default system name.

[Command format]

hostname *HOSTNAME*

no hostname

[Parameter]

HOSTNAME: new appointed system name to user.

[Default]

The default value of hostname is raisecom.

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

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

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Hostname can not exceed 32 characters !

Set successfully

[Example]

Change the hostname to “A”:

Raisecom(config-remote)#**hostname A**

[Related commands]

Commands	Description
show remote-device information	Show information of remote device.

28.11 inside-loopback

[Function]

Enable remote device optical inside loopback.

[Command format]

inside-loopback

inside-loopback *mac-exchange crc-recalculate*

no inside-loopback

[Parameter]

mac-exchange: switch MAC address;

crc-recalculate: recalculate CRC.

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

Enable remote device optical inside loopback.

Made the response device switch MAC address and recalculate the CRC.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Set successfully

[Example]

Enable remote optical inside loopback and exchange MAC address, don't recalculate CRC:

Raisecom(config-remote)#**inside-loopback** *mac-exchange*

[Related commands]

Commands	Description
show inside-loopback	Show inside-loopback parameter and state.

28.12 interface client

[Function]

Enter physical interface configuration of client device.

[Command format]

interface client *port-id*

[Parameter]

port-id: user port ID.

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

In Remote configuration mode, set client port configuration such as:
speed, duplex, flow control, rate-limiting.

[Explanation of command execution echo]

Remote device X has no this port!

[Example]

Enter configuration mode of remote client 1 port:

Raisecom(config-remote)#**interface client 1**

28.13 ip address

[Function]

Set IP address of remote device.

[Command format]

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

no ip address *ip-address*

[Parameter]

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

ip-mask: interface IP mask, format is A.B.C.D;

vlan-list: VLAN ID of corresponding layer 3 interface.

[Command Modes]

Remote configuration mode and Privileged user

[Executing Command Instruction]

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

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Set successfully

Can not assign ip address for vlan 2(cluster)

Can't set the same IP address on multiple remote devices

Invalid network mask

Invalid IP address or network mask

[Example]

Set remote interface IP address to 192.168.1.2, associated VLAN ID is 2:

Raisecom(config-remote)# **ip address** 192.168.1.2 255.255.255.0 1

Erase interface IP address:

Raisecom(config-remote)# **no ip address** *192.168.1.2*

[Related commands]

Commands	Description
show remote-device information	Show information of remote device.
ip default-gateway <i>A.B.C.D</i>	Set IP default gateway for remote interface.

28. 14 **ip default-gateway**

[Function]

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

[Command format]

ip default-gateway *A.B.C.D*

no ip default-gateway

[Parameter]

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

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

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

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Set successfully

Invalid next-hop IP address.

[Example]

Set the default gateway to 10.0.0.1:

Raisecom(config-remote)# **ip default-gateway** 10.0.0.1

Delete the configuration of default gateway:

Raisecom(config-remote)# **no ip default-gateway**

[Related commands]

Commands	Description
show remote-device information	Show the information of remote device.

28.15 line-speed auto

[Function]

Enable and disable optical port speed 1000M auto-negotiation.

[Command format]

line-speed auto

no line-speed auto

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

This command can be only used on 1G port, 100M port is unavailable.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Set successfully

[Example]

Enable optical port speed 1000M auto-negotiation:

Raisecom(config-remote)#**line-speed auto**

Disable optical port speed 1000M auto-negotiation:

Raisecom(config-remote)#**no line-speed auto**

[Related commands]

Commands	Description
show interface port	Show remote device port information.
show interface port detail	Show remote device port detail.

28.16 rate-limit

[Function]

Set bandwidth limit for remote device.

[Command format]

rate-limit line *line-id* **ingress** *rate*

rate-limit client *client-id* **ingress** *rate*

rate-limit line *line-id* **engress** *rate*

rate-limit client *client-id* **ingress** *rate*

no rate-limit line *line-id* **ingress**

no rate-limit client *client-id* **ingress**

no rate-limit line *line-id* **egress**

no rate-limit client *client-id* **egress**

[Parameter]

ingress: ingress;

egress: egress;

line-id: Line port id;

client-id: Client port id ;

rate: rate from 1 to 1048576 Kbps.

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

Set rate limit for ingress and egress (the result may be different from academic value).

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Fail to set ingress rate on remote device X!

Fail to set engress rate on remote device X!

Set successfully

[Example]

Set client port 1 ingress bandwidth at 10Mbps:

```
Raisecom(config-remote)#rate-limit client 1 ingress 10000
```

Set client port 1 egress bandwidth at 5Mbps:

```
Raisecom(config-remote)#rate-limit client 1 egress 5000
```

Delete rate limit for client port 1:

```
Raisecom(config-remote)#no rate-limit client 1 egress
```

[Related commands]

Commands	Description
show interface port detail	Show remote device details.

28.17 reboot

[Function]

Reboot remote device.

[Command format]

reboot

[Command Modes]

Remote configuration mode; privileged user

[Executing Command Instruction]

“Yes” should be entered to confirm the operation when the command is used to reboot switch.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Remote device X reboot operation is not carried out.

[Example]

Raisecom(config-remote)#**reboot**

Please input 'yes' to confirm:yes

28.18 remote-device

[Function]

Enter remote configuration mode. remote management commands is installed under this mode, and it is available to manage related remote device under this mode.

[Command format]

remote-device

[Command Modes]

Interface/Range configuration mode; privileged user

[Executing Command Instruction]

Use this command to enter remote configuration mode.

[Explanation of command execution echo]

Port X remote device extended-oam link is not established.

Line X remote device extended-oam link is not established.

[Example]

Enter remote configuration mode from the port:

Raisecom(port)#**remote-device**

[Related commands]

Commands	Description
----------	-------------

exit	Return previous command or logout.
quit	Return previous command or logout.

28.19 show cable-diagnostics

[Function]

Show remote cable diagnostics.

[Command format]

show cable-diagnostics

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

Check the diagnostics of remote link in remote configuration mode.

[Explanation of command execution echo]

<i>Remote device</i>	<i>Attribute</i>	<i>Status</i>	<i>Length(m)</i>
-----	-----	-----	-----
<i>1</i>	<i>Not Issued</i>	<i>N/A</i>	<i>0</i>

[Example]

Raisecom(config-remote)#**show cable-diagnostics**

[Related commands]

Commands	Description
test cable-diagnostics	Perform remote link diagnostics.

28.20 show extended-oam statistics

[Function]

Show extended oam statistics information.

[Command format]

show extended-oam statistics line-list *line-list*

[Parameter]

line-list: line port list;

client-list: client port list.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

Show extended oam statistics information, including sending, receiving and all kinds of OAM frame

[Explanation of command execution echo]

Raisecom#**show extended-oam statistics** *line 1*

Port: 1

	<i>Tx</i>	<i>Rx</i>

<i>Variable Get:</i>	<i>35</i>	<i>0</i>
<i>Variable Set:</i>	<i>3</i>	<i>0</i>
<i>Get response:</i>	<i>0</i>	<i>35</i>
<i>Set response:</i>	<i>0</i>	<i>3</i>
<i>File Read Request:</i>	<i>0</i>	<i>0</i>
<i>File Write Request:</i>	<i>0</i>	<i>0</i>
<i>File transfer data:</i>	<i>0</i>	<i>0</i>
<i>File transfer ack:</i>	<i>0</i>	<i>0</i>
<i>notification:</i>	<i>0</i>	<i>1</i>
<i>Static Information :</i>	<i>0</i>	<i>0</i>
<i>Dynamic Information:</i>	<i>0</i>	<i>0</i>
<i>Configuration:</i>	<i>0</i>	<i>0</i>

<i>Command:</i>	<i>0</i>	<i>0</i>
<i>Connect:</i>	<i>0</i>	<i>0</i>
<i>Others:</i>	<i>0</i>	<i>0</i>

[Example]

Show all link OAM frame statistics information:

Raisecom#**show extended-oam statistics**

Show link 2 OAM frame statistic information:

Raisecom#**show extended-oam statistics line-list 2**

[Related commands]

Commands	Description
clear extended-oam statistics	Clear extended OAM frame statistics.

28. 21 show extended-oam status

[Function]

Show extended OAM link state.

[Command format]

show extended-oam status line-list *line-list*

[Parameter]

line-list: line port list;

client-list: client port list.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

Show extended oam link state.

[Explanation of command execution echo]

<i>Ifindex</i>	<i>Extended OAM Status</i>
----------------	----------------------------

1: *operational*

2: *nonoperational*

Extended-oam Notification: Enable

Config-request: Enable

[Example]

Show all extended OAM link status:

Raisecom#**show extended-oam status**

Show link line 2 extended OAM status:

Raisecom#**show extended-oam status line 1**

28.22 show inside-loopback

[Function]

Show loopback state and parameter.

[Command format]

show inside-loopback

[Command Modes]

Remote configuration mode, Privileged EXEC

[Executing Command Instruction]

Show loopback state and parameter in remote configuration mode.

Remote device interface information will not be shown if remote device is unconnected or OAM link is not established.

[Explanation of command execution echo]

Raisecom(config-remote)#**show remote-device information**

Local port: 1

Loopback status: No

Loopback MAC address exchange: Yes

Loopback CRC recalculate: Yes

[Example]

Raisecom(config-remote)#**show inside-loopback**

[Related commands]

Commands	Description
inside-loopback	Enable loopback for remote device.

28.23 show interface port

[Function]

Show state of particular or all the ports.

[Command format]

show interface *port*

show interface *client* In support of: RC551

show interface *line* In support of: RC551

[Parameter]

port-list: port list;

client-list: client port list;

line-list: line port list.

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

Use this command under remote configuration mode to review remote device port information: including management state, operation state, speed and duplex and control.

[Explanation of command execution echo]

Raisecom(config-remote)#**show interface port**

Local Port: 12

Port	Admin	Operate	Speed/Duplex	Flowcontrol	Flowcontrol
------	-------	---------	--------------	-------------	-------------

line 1	enable	up(100M/full)	100M/full	off	disable
client 1	disable	down	auto	off	disable
client 2	disable	down	auto	off	disable
client 3	disable	down	auto	off	disable
client 4	enable	up(100M/full)	auto	off	disable

[Example]

Raisecom(config-remote)#**show interface port**

[Related commands]

Commands	Description
shutdown	Enable/disable remote client port.
duplex {full half}	Configure duplex for remote device.
speed (<i>auto 10 100 1000</i>)	Configure speed for remote device.
flowcontrol { <i>on off</i> }	Set the start and shutdown for flow control function of the port.
show interface port detail	Show details of remote port.

28.24 show interface port detail

[Function]

Show interface detail information.

[Command format]

show interface *port detail*

show interface *client* In support of: RC551

show interface *line* In support of: RC551

[Parameter]

port: physical port;

client-list: client port list;

line-list: line port list.

detail: detail information.

[Command Modes]

Remote configuration mode; Privileged user

[Executing Command Instruction]

Use this command under remote configuration mode to review remote port information.

[Explanation of command execution echo]

Raisecom(config-remote)#**show interface port detail**

Local port: 12, remote port: line 1

Administer: enable

Operate: up(100M/full)

Speed/Duplex set: 100M/full

Flowcontrol state: off

Flowcontrol set: disable

Ingress rate-limit: 0(No rate-limit)

Egress rate-limit: 0(No rate-limit)

Port description:

Fault pass enable: Disable

Fault pass to ports: n/a

Fault pass status: Normal

Optical module type: Unknown

SD status: Normal

Local port: 12, remote port: client 1

Administer: disable

Operate: down

Speed/Duplex set: auto

Flowcontrol state: off

Flowcontrol set: disable

Ingress rate-limit: 0(No rate-limit)

Egress rate-limit: 0(No rate-limit)

Port description:

Fault pass enable: Disable

Fault pass to ports: n/a

Fault pass status: Normal

[Example]

Raisecom(config-remote)#**show interface port detail**

[Related commands]

Commands	Description
shutdown	Shutdown or open client port.
rate-limit	Set rate limit of remote port.
fault-pass	Enable/disable fault-pass of remote optical port.
description	Set description of remote port.
duplex {full half}	Configure duplex of remote device.
speed (auto 10 100 1000)	Configure speed of remote device.
flowcontrol {on off}	Open/close flowcontrol of client port.
show interface port detail	Show details of remote port.

28.25 show interface port statistics

[Function]

Show the packet statistical information for particular or all the ports.

[Command format]

show interface *port* **statistics**

show interface *client* **statistics** In support of: RC551

show interface *line* **statistics** In support of: RC551

[Parameter]

port: physical port;

client-list: client port list;

line-list: line port list.

[Command Modes]

Remote configuration mode; privileged user

[Executing Command Instruction]

Show the packet statistical information for particular or all the ports.

[Explanation of command execution echo]

Raisecom(config-remote)#**show interface** *port* *sstatistics*

Local port: 12, remote port:line 1

InOctets: 61,860

InPkts: --

InUcastPkts: 0

InMulticastPkts: 780

InBroadcastPkts: 0

OutOctets: 125,334

OutPkts: --

<i>OutUcastPkts:</i>	<i>0</i>
<i>OutMulticastPkts:</i>	<i>789</i>
<i>OutBroadcastPkts:</i>	<i>809</i>
<i>ErrorPkts:</i>	<i>--</i>
<i>DropEvents:</i>	<i>0</i>
<i>CRCAlignErrors:</i>	<i>0</i>
<i>UndersizePkts:</i>	<i>0</i>
<i>OversizePkts:</i>	<i>0</i>
<i>Fragments:</i>	<i>0</i>
<i>Jabbers:</i>	<i>0</i>
<i>Collisions:</i>	<i>0</i>

Local port: 12, remote port:client 1

<i>InOctets:</i>	<i>0</i>
<i>InPkts:</i>	<i>--</i>
<i>InUcastPkts:</i>	<i>0</i>
<i>InMulticastPkts:</i>	<i>0</i>
<i>InBroadcastPkts:</i>	<i>0</i>
<i>OutOctets:</i>	<i>0</i>
<i>OutPkts:</i>	<i>--</i>
<i>OutUcastPkts:</i>	<i>0</i>
<i>OutMulticastPkts:</i>	<i>0</i>
<i>OutBroadcastPkts:</i>	<i>0</i>
<i>ErrorPkts:</i>	<i>--</i>
<i>DropEvents:</i>	<i>0</i>

<i>CRCAAlignErrors:</i>	<i>0</i>
<i>UndersizePkts:</i>	<i>0</i>
<i>OversizePkts:</i>	<i>0</i>
<i>Fragments:</i>	<i>0</i>
<i>Jabbers:</i>	<i>0</i>
<i>Collisions:</i>	<i>0</i>

[Example]

Raisecom(config-remote)#**show interface port statistics**

28.26 show oam capability

[Function]

Show OAM management capability supported by remote device.

[Command format]

show oam capability

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

Show OAM management capability supported by remote device in remote configuration mode. OAM has 9 kinds of capability: OAM file transmission, IP address and gateway configuration, SNMP community configuration, port configuration, environment monitor, remote device reset, remote device configuration saving and erasing and host name configuration.

[Explanation of command execution echo]

Raisecom(config-remote)#**show oam capability**

Local port: 12

OID parse capability

[Support]

File transmission via OAM

[Support]

<i>IP address and default-gateway configuration</i>	<i>[Support]</i>
<i>SNMP community configuration</i>	<i>[Support]</i>
<i>Port configuration</i>	<i>[Support]</i>
<i>Device environment monitor</i>	<i>[Support]</i>
<i>Device reboot</i>	<i>[Support]</i>
<i>Save remote device current configuration to flash file</i>	<i>[Support]</i>
<i>Device configuration file erasion</i>	<i>[Support]</i>
<i>Device hostname configuration</i>	<i>[Support]</i>
<i>OAM notification enable configuration</i>	<i>[Support]</i>
<i>SFP</i>	<i>[Support]</i>
<i>Q-in-Q</i>	<i>[Support]</i>
<i>Cable-diagnostics</i>	<i>[Support]</i>

[Example]

Raisecom(config-remote)#**show oam capability**

28.27 show remote-device information

[Function]

Show basic information for remote device.

[Command format]

show remote-device information

[Command Modes]

Remote configuration mode, Privileged EXEC

[Executing Command Instruction]

This command can show remote device information in remote configuration mode, including port ID, device name, product name, host name, version for hardware and software, port number, FPGA chip

ID and software number, IP subnet configuration, SNMP community configuration, device temperature and voltage.

[Explanation of command execution echo]

Raisecom(config-remote)#**show remote-device information**

Local Port: 12

Product Name: RC551-4FE

Hostname: Raisecom

Operation Software Version: 3.1.680.RC551-4FE.28.20061002

Hardware Version: Rev.A

Total ports: 5

IP Address:10.0.5.128,IP address Mask:255.0.0.0

Management Vlan: 1

Port:line 1,client 1-client 4

Untag port:line 1,client 1-client 4

IP Default-gateway:n/a

Community Name:n/a, Access:n/a

OAM Notification:Enable

Device current temperature:34 (Celsius)

<i>Ref. Volt(mv)</i>	<i>Current Volt(mv)</i>
----------------------	-------------------------

<i>3300</i>	<i>3317</i>
-------------	-------------

<i>2500</i>	<i>2513</i>
-------------	-------------

<i>1800</i>	<i>1758</i>
-------------	-------------

1200

1252

[Example]

Raisecom(config-remote)#**show remote-device information**

28. 28 show sfp

[Function]

Show remote SFP module information.

[Command format]

show sfp

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

Show remote SFP module information in remote configuration mode.

[Explanation of command execution echo]

Local port: 1

Port: 1

Exist: Yes

Module type: SFP

Optical interface: LC

Media type: 9/125 fiber

RX LOS: normal

TX fault: normal

TX enable: Enable

Speed: 125M

Transport distance: 12345km

Wave length: 1477nm

Vendor: WTD

Product type: RTX191DA

Version: 0001

Serial number: B009822

[Example]

Raisecom(config-remote)#**show sfp**

28.29 show snmp trap remote

[Function]

Show remote trap enable configuration.

[Command format]

show snmp trap remote

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

This command can show remote trap enable configuration.

[Explanation of command execution echo]

Raisecom#**show snmp trap remote**

SNMP Remote Trap: Enable

[Example]

Raisecom(config)# **show snmp trap remote**

[Related commands]

Commands	Description
snmp trap remote {enable disable}	Enable/disable remote trap switch.

28. 30 shutdown

[Function]

Shutdown the client port, use **no** command to open the port.

[Command format]

shutdown

no shutdown

[Command Modes]

Remote port configuration mode; privileged user

[Executing Command Instruction]

Use this command under remote port configuration mode to shutdown and open client port.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Set successfully

[Example]

Shut down the client port:

Raisecom(config-remoteport)# **shutdown**

Open the client port:

Raisecom(config-remoteport)# **no shutdown**

[Related commands]

Commands	Description
show interface port	Show port information on remote device.
show interface port detail	Show details of remote device port.

28.31 snmp trap remote

[Function]

Enable/disable remote trap switch.

[Command format]

snmp trap remote *enable*

snmp trap remote *disable*

[Parameter]

enable: enable remote trap switch;

disable: disable remote trap switch.

[Default]

enable

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Enable/disable remote trap switch. When enable trap, system send trap to SNMP network management if receives OAM notification frame; when disable trap, system doesn't send trap to SNMP if receives OAM notification frame.

[Explanation of command execution echo]

Set successfully

[Example]

Raisecom(config)#**snmp trap remote** *enable*

[Related commands]

Commands	Description
[no] snmp-server enable traps	Enable/disable trap transmitting function.

28. 32 snmp-server community

[Function]

Configure SNMP community name for remote device.

[Command Format]

snmp-server community *community-name* {*ro* | *rw*}

no snmp-server community *community-name*

[Parameter]

community-name: community name, string, less than 32;

ro: specify the access privilege of the community is ready-only;

rw: specify the access privilege of the community is ready-write.

[Command Modes]

Remote configuration mode; privileged user mode

[Executing Command Instruction]

Configure SNMP community name for remote device in remote configuration mode. the configured community is line 3 in the community table index, the view is internet.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Set successfully

Community name can not exceed 20 characters!

[Example]

Raisecom(config-remote)#**write**

[Related commands]

Commands	Description
show remote-device information	Show information of remote device.

28. 33 speed

[Function]

Use this command to set rat of client port.

[Command format]

speed (*10* / *100* / *1000*)

[Parameter]

auto: speed auto-negotiation;

10: speed is 10Mbps;

100: speed is 100Mbps;

1000: the speed the 1000Mbps.

[Command Modes]

Remote port configuration mode; privileged user

[Executing Command Instruction]

Different type of client port can configure different speed.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Set successfully

[Example]

Set up the client port speed at 10Mbps:

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

[Related commands]

Commands	Description
duplex {full half}	Configure duplex for remote device.
show interface port	Show port information of remote device.
show interface port detail	Show details of remote device port.

28.34 switch-mode double-tagged-vlan

[Function]

Set Double tagged VLAN forwarding mode for remote device.

[Command format]

switch-mode double-tagged-vlan native-vlan <1-4094>

switch-mode double-tagged-vlan native-vlan <1-4094> line

switch-mode double-tagged-vlan tpid HHHH native-vlan <1-4094>

**switch-mode double-tagged-vlan tpid HHHH native-vlan <1-4094>
line**

[Parameter]

native-vlan: native vlan;

<1-4094>: VLAN ID;

line: Line as ingress port;

tpid: outer tag TPID;

HHHH: outer tag id hexadecimal numeral, range from 0000 to FFFF.

[Command Modes]

Remote configuration mode, Privileged EXEC

[Executing Command Instruction]

Use this command to set Double tagged VLAN forwarding mode for remote device. After set device double TAG mode, no matter the packet enter from ingress port has TAG or not, it will be tagged with specified TPID and out side TAG of native VLAN ID.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Set successfully

[Example]

Set remote working mode is double TAG, TPID is 0x9100, native VLAN is 1, ingress port is client port:

```
Raisecom(config-remote)#switch-mode double-tagged-vlan native-vlan 1
```

Set remote working mode is double TAG, TPID is 0x8100, native VLAN is 3, ingress port is line port:

```
Raisecom(config-remote)#switch-mode double-tagged-vlan tpid 8100 native-vlan 3 line
```

[Related commands]

Commands	Description
show remote-device information	Show remote device information.
switch-mode dot1q-vlan	Set Dot1q VLAN mode for remote device.

switch-mode transparent

Set transparent mode for remote device.

28.35 switch-mode transparent**[Function]**

Set transparent mode.

[Command format]**switch-mode transparent****[Command Modes]**

Remote configuration mode, Privileged user

[Executing Command Instruction]

Use this command to set transparent mode.

[Explanation of command execution echo]*Remote device X does not support the command.**Remote device X extended-oam link is not established.**Remote device X set unsuccessfully.**Set successfully***[Example]**Raisecom(config-remote)#**switch-mode transparent****[Related commands]**

Commands	Description
show remote-device information	Show remote device information
switch-mode double-tagged-vlan	Set Double tagged VLAN mode for remote device
switch-mode dot1q-vlan	Set Dot1q VLAN mode for remote device

28.36 system mtu

[Function]

Set maximal frame length for local and remote device.

[Command format]

system mtu <1500-8000>

[Parameter]

<1500-8000>: the size of frames.

[Command Modes]

Remote configuration mode, Privileged EXEC

[Executing Command Instruction]

The maximum MTU may be different according to different remote device.

The maximum allowable system MTU for RC552-GE is 1916bytes or 1536bytes. For RC552-GE as the remote device, if you set the mtu to 1916, value can be 1536 or 1916.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Set successfully

[Example]

Raisecom(config-remote)#**system mtu 1916**

[Related commands]

Commands	Description
show remote-device information	Show remote device information
show system mtu	Show MTU of local device.

28.37 test cable-diagnostics

[Function]

Dummy cable diagnostics. This command is available to ISCOM2000/2100/2800/2900/3000 series and RC5XX series.

[Command format]

test cable-diagnostics

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

Execute dummy cable diagnostics for remote device.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Local port: 1

Test will affect link state and traffic.

Test will take a few seconds to run.

Use 'show cable-diagnostics' to read the test results.

Remote device xx is running cable-diagnostics.

[Example]

Raisecom(config-remote)#**test cable-diagnostics**

[Related commands]

Commands	Description
show cable-diagnostics	Show cable diagnostics for remote device.

28. 38 upload

[Function]

Upload system file, configuration file to remote device. This command is available to ISCOM2000/2100/2800/2900/3000 series and RC5XX series.

[Command format]

upload {*startup-config* | *system-boot* } **ftp** *A.B.C.D* *USERNAME*
PASSWORD *FILENAME*

upload {*startup-config* | *system-boot* } **tftp** *A.B.C.D* *FILENAME*

upload system-boot *FILENAME*

upload startup-config

[Parameter]

system-boot: system boot file;

startup-config: system configuration file;

tftp: tftp protocol for download;

ftp: ftp protocol for download;

A.B.C.D: IP address for server;

USERNAME: username for ftp server;

PASSWORD: password for ftp server;

FILENAME: file on server or center device.

[Command Modes]

Remote configuration mode, Privileged user

[Executing Command Instruction]

Upload system file, configuration file and FPGA file from server. Only **upload startup-config** command can upload multiple files simultaneously.

upload {startup-config | system-boot} ftp A.B.C.D USERNAME PASSWORD FILENAME LOCAL-FILENAME command upload file to center device via extended OAM and then upload to server by FTP.

upload {startup-config | system-boot} tftp A.B.C.D FILENAME LOCAL-FILENAME upload to center device via extended OAM from remote device and then upload to server by TFTP from center device.

upload system-boot FILENAME command upload file from remote device. File name can not be the default name.

upload startup-config command upload file from remote to center device via OAM, then save file name as default. Default name: remote device type+ center OAM link ID+ suffix.

If remote device supports file transport: *FILE_ID*, for example *FILE_5.conf*

Or else, the file name is *FRAME_ID*, for example *FRAME_2.conf*

This command uploads multiple files. There isn't any effect if some device can not upload file.

[Explanation of command execution echo]

Waiting...Start

Getting source file...Done

Writing to destination...Done

Success!

Failed!(Invalid IP Address)

Failed!(User name error)

Failed!(Password error)

Failed!(File name error)

Waiting...Start

Connecting to server failed

Failed !

Waiting...Start

Getting source file...

Failed!(mem alloc error)

Waiting...Start

Getting source file...

Failed!(File to operate too large error)

Waiting...Start

Getting source file ...Done

Failed ! (OAM link X busy)

Waiting...Start

Getting source file ...Done

Failed ! (OAM link X Time out)

Waiting...Start

Getting source file ...Done

Failed ! (Remote X not support this command)

Waiting...Start

Getting source file ...Done

Failed ! (Extend OAM link X not established)

Waiting...Start

Getting source file...

Failed!(Unknown error)

Waiting...Start

Getting source file ...Done

Writing file to destination ...

Failed ! (Opening file failed)

Waiting...Start

Getting source file ...Done

Writing file to destination ...

Failed ! (File writing failed)

Can't upload multiple remote device files to server at one time.

Failed !

[Example]

Use TFTP protocol to upload system boot file to server:

```
Raisecom(config-remote)#upload system-boot tftp 10.168.0.11 sys1.z
```

Use FTP protocol to upload startup configuration file to server:

```
Raisecom(config-remote)#upload startup-config ftp 10.168.0.11 user  
user start1.conf
```

Upload system boot file to server:

```
Raisecom(config-remote)#upload system-boot system5.boot
```

Upload startup configuration file to server, use default file name:

```
Raisecom(config-remote)#upload startup-config
```

[Related commands]

Commands	Description
erase	Delete specified file in flash.
dir	Show file in flash.
download	Download file.

28.39 upload remote

[Function]

Upload file from device to server. This command is available to ISCOM2000/2100/2800/2900/3000 series and RC5XX series.

[Command format]

```
upload {remote-bootstrap / remote-system-boot / remote-startup-config /  
remote-fpga} ftp A.B.C.D USERNAME PASSWORD FILENAME  
LOCAL-FILENAME
```

```
upload {remote-bootstrap / remote-system-boot / remote-startup-config /  
remote-fpga} tftp A.B.C.D FILENAME LOCAL-FILENAME
```

[Parameter]

remote-bootstrap: boot file for remote device;

remote-system-boot: start file for remote device;

remote-startup-config: configuration file for remote device;

remote-fpga: FPGA file for remote device;

tftp: tftp protocol for download;

ftp: ftp protocol for download;

A.B.C.D: IP address for server;

USERNAME: username for ftp server;

PASSWORD: password for ftp server;

FILENAME: file name for server;

LOCAL-FILENAME: file name on center device.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

This command can upload the file from center device to server. these file can be system-boot, startup-config, fpga and bootstrap.

File name: specified file+ suffix.

	u
ile	f
typ	f
e	i
	x

yste

m-b

oot

Z

tart

up-c

onfi

g

c

o

n

f

oots

trap

b

o

o

t

pga

v

m

e

User can not upload default file.

[Explanation of command execution echo]

Waiting...Start

Getting source file...Done

Writing to destination...Done

Success!

Failed! (Invalid IP Address)

Failed!(User name error)

Failed!(Password error)

Failed!(File name error)

Waiting...Start

Connecting to server failed

Failed !

Waiting...Start

Getting source file...

Failed!(Open file error)

Waiting...Start

Getting source file ...Done

Writing file to destination ...

Failed ! (Opening file failed)

Waiting...Start

Getting source file ...Done

Writing file to destination ...

Failed ! (File writing failed)

Waiting...Start

Getting source file ...Done

Writing file to destination ...

Failed!(Time Out error)

Waiting...Start

Getting source file ...Done

Writing file to destination ...

Failed!(Unknown error)

[Example]

Use TFTP protocol to upload system1/Z in center FLASH to server:

Raisecom#**upload remote-system-boot tftp 10.168.0.11 sys1.z system1**

Use TFTP protocol to upload FILE_5.conf in center FLASH to server:

Raisecom#**upload remote-startup-config ftp 10.168.0.11 user user
start.conf FILE_5**

[Related commands]

Commands	Description
erase	Delete specified file in flash.
dir	Show file in flash.

download	File download.
-----------------	----------------

28.40 write

[Function]

The command is used to save configuration information of current system. This command is available to ISCOM2000/2100/2800/2900/3000 series and RC5XX series.

[Command format]

write

[Command Modes]

Remote configuration mode, privileged user

[Executing Command Instruction]

Use the command to save configuration information of current system, then the saved system command will be executed automatically after reset the system, a new configuration of the switch is not needed.

[Explanation of command execution echo]

Remote device X does not support the command.

Remote device X extended-oam link is not established.

Remote device X set unsuccessfully.

Saving remote current configuration...

Save remote current configuration successfully

Saving remote current configuration...

Remote device save current configuration unsuccessfully

[Example]

Raisecom(config-remote)#**write**

[Related commands]

Commands	Description
erase	Delete referenced files in system

Chapter 29 Digital Diagnostic Commands

29.1 show interface port transceiver

[Function]

Show performance parameter value and threshold value, etc. information of optical module.

[Command format]

show interface port [*port-list*] **transceiver** [*threshold-violations*]
[*detail*]

[Parameter]

port-list: port list.

threshold-violations: information of threshold-violation.

detail: details.

[Command Modes]

Privileged EXEC mode, Privileged user

[Executing Command Instruction]

Use this command to show performance parameter value and threshold value, etc. information of optical module.

[Explanation of command execution echo]

Raisecom#**show interface port** [*port-list*] **transceiver**

If device is externally calibrated, only calibrated values are printed.

++ : high alarm, ,+ : high warning, - : low warning, -- : low alarm.

Tx: transmit, Rx: receive, mA: milliamperes.

	<i>supply</i>	<i>Tx bias</i>	<i>Optical</i>	<i>Optical</i>	
	<i>Temperature</i>	<i>Voltage</i>	<i>Current</i>	<i>Tx Power</i>	<i>Rx Power</i>
<i>Port</i>	<i>(Celsius)</i>	<i>(Volts)</i>	<i>(mA)</i>	<i>(dBm)</i>	<i>(dBm)</i>

Raisecom# **show interface port** [*port-list*] **transceiver detail**

transceiver trap:<transceiver trap switch>

++ : high alarm, + : high warning, - : low warning, -- : low alarm.

The threshold values are calibrated.

	<i>High Alarm</i>	<i>High Warn</i>	<i>Low Warn</i>	<i>Low</i>
<i>Alarm</i>				
	<i>Temperature</i>	<i>Threshold</i>	<i>Threshold</i>	<i>Threshold</i>
<i>Threshold</i>				
<i>Port</i>	<i>(Celsius)</i>	<i>(Celsius)</i>	<i>(Celsius)</i>	<i>(Celsius)</i>
<i>(Celsius)</i>				

	<i>High Alarm</i>	<i>High Warn</i>	<i>Low Warn</i>	<i>Low</i>
<i>Alarm</i>				
	<i>supply voltage</i>	<i>Threshold</i>	<i>Threshold</i>	<i>Threshold</i>
<i>Threshold</i>				
<i>Port</i>	<i>(Volts)</i>	<i>(Volts)</i>	<i>(Volts)</i>	<i>(Volts)</i>
<i>(Volts)</i>				

	<i>TX bias</i>	<i>High Alarm</i>	<i>High Warn</i>	<i>Low Warn</i>	<i>Low</i>
<i>Alarm</i>					

	<i>Current</i>	<i>Threshold</i>	<i>Threshold</i>	<i>Threshold</i>
<i>Threshold</i>				
<i>Port</i>	<i>(mA)</i>	<i>(mA)</i>	<i>(mA)</i>	<i>(mA)</i>

	<i>Optical</i>	<i>High Alarm</i>	<i>High Warn</i>	<i>Low Warn</i>
<i>Low Alarm</i>				

	<i>Transmit Power</i>	<i>Threshold</i>	<i>Threshold</i>	<i>Threshold</i>
<i>Threshold</i>				
<i>Port</i>	<i>(dBm)</i>	<i>(dBm)</i>	<i>(dBm)</i>	<i>(dBm)</i>
<i>(dBm)</i>				

	<i>Optical</i>	<i>High Alarm</i>	<i>High Warn</i>	<i>Low Warn</i>
<i>Low Alarm</i>				
	<i>Receive Power</i>	<i>Threshold</i>	<i>Threshold</i>	<i>Threshold</i>
<i>Threshold</i>				
<i>Port</i>	<i>(dBm)</i>	<i>(dBm)</i>	<i>(dBm)</i>	<i>(dBm)</i>
<i>(dBm)</i>				

Raisecom#**show interface port [port-list] transceiver threshold violations**

DDDD: days, HH: hours, MM: minutes, SS: seconds

	<i>Time since Last Known</i>		
	<i>Threshold Violation</i>		<i>Type(s) of Last</i>
<i>Known</i>			
<i>Port</i>	<i>(DDDD:HH:MM:SS)</i>		<i>Threshold</i>
<i>Violation(s)</i>			

[Example]

Review port 2 digital diagnostic parameters:

Raisecom# **show interface port 2 transceiver**

[Related commands]

Commands	Description
snmp trap transceiver	Enable/disable send parameter state abnormal trap.

29.2 snmp trap transceiver

[Function]

Enable/disable send parameter state abnormal trap.

[Command format]

snmp trap transceiver {*enable/disable*}

[Parameter]

enable: enable transceiver traps.

disable: disable transceiver traps.

[Default]

enable

[Command Modes]

Global configuration mode, Privileged user

[Executing Command Instruction]

Use this command to enable/disable send parameter state abnormal trap.

[Explanation of command execution echo]

Set successfully.

[Example]

Disable transceiver parameter abnormal traps:

Raisecom(config)#**snmp trap transceiver** *disable*

[Related commands]

Commands	Description
show interface transceiver detail	Show digital diagnostic details.

Chapter 30 802.1x Commands

30.1 clear dot1x statistics

[Function]

Clear EAPOL statistics of port.

This command is available to ISCOM2000/2100/2800/2900/3000 series and 5X1-4FE.

[Command format]

clear dot1x port-list *port-list* **statistics**

clear dot1x line *line-list* **statistics**

clear dot1x client *client-list* **statistics**

[Parameter]

port-list: port list.

line-list: line port list.

client-list: client port list.

[Command Modes]

Global configuration mode

[Executing Command Instruction]

Use this command to clear EAPOL statistics of port.

[Explanation of command execution echo]

Set successfully

[Example]

Clear statistic information of port 1 under global configuration mode:

Raisecom(config)#**clear dot1x** *port-list 1* **statistics**

[Related commands]

Commands	Description
show dot1x port-list <i>port-list</i> statistics	Show port statistic information of 802.1x protocol.
show dot1x line <i>line-list</i> statistics	Show line port statistic information of 802.1x protocol.
show dot1x client <i>client-list</i> statistics	Show client port statistic information of 802.1x protocol.

30.2 dot1x auth-control

[Function]

Configure 802.1x authorization for the port.

This command is available to ISCOM2000/2100/2800/2900/3000 series and 5X1-4FE.

[Command format]

dot1x auth-control{*authorized-force* | *unauthorized-force* | *auto*}

[Parameter]

authorized-force: force port authorized mode. Indicate the port is always in authorized mode, permit users access network and the service supplied by switch without authorization.

unauthorized-force: force port unauthorized mode. Indicate the port is always in unauthorized mode, not permit users access network and the service supplied by switch without authorization.

auto: auto-negotiation the authorization mode. Permit transmitting and receiving EAPOL message before authorization, no permit users' access network and the service supplied by switch.

[Default]

auto

[Command Modes]

physical interface configuration

[Executing Command Instruction]

802.1x authorization based on port, this command determines port authorization mode of user direct.

[Explanation of command execution echo]

Set successfully.

Port x set unsuccessfully.

[Example]

Using force authorized mode on relevant port under physical interface configuration mode:

Raisecom(config-port)# **dot1x auth-control** *authorized-force*

[Related commands]

Commands	Description
show dot1x port-list <i>port-list</i>	Show port statistic information of 802.1x protocol.
show dot1x line <i>line-list</i>	Show line port statistic information of 802.1x protocol.
show dot1x client <i>client-list</i>	Show client port statistic information of 802.1x protocol.

30.3 dot1x reauthentication

[Function]

Configure 802.1x authorization for the port.

This command is available to ISCOM2000/2100/2800/2900/3000 series and 5X1-4FE.

[Command format]

dot1x reauthentication {*enable* |*disable*}

[Parameter]

enable: enable 802.1x reauthorization function.

disable: disable 802.1x reauthorization function.

[Default]

disable

[Command Modes]

physical interface configuration

[Executing Command Instruction]

System will reauthenticate the authorized port periodically. The authorization state will not change during process of reauthentication.

[Explanation of command execution echo]

Set successfully.

Port x set unsuccessfully.

[Example]

Enable reauthentication function on relevant port under physical interface configuration mode:

Raisecom(config-port)# **dot1x reauthentication enable**

[Related commands]

Commands	Description
show dot1x port-list <i>port-list</i>	Show port statistic information of 802.1x protocol.
show dot1x line <i>line-list</i>	Show line port statistic information of 802.1x protocol.
show dot1x client <i>client-list</i>	Show client port statistic information of 802.1x protocol.

30.4 dot1x timer quiet-period

[Function]

Configure quiet period timer of 802.1x port.

This command is available to ISCOM2000/2100/2800/2900/3000 series and 5X1-4FE.

[Command format]

[no] dot1x timer quiet-period *quiet-period-value*

[Parameter]

quiet-period: quiet period timer. After user fail to authentication, the switch need a quiet period and this period is determined by quiet period timer and then initiate authentication again. The switch in quiet period deals with no message. Relevant configuration value is *quiet-period-value* <10-120>.

[Default]

Default configuration of all timers:

Timer	Variable	Configured value
quiet-period	<i>quiet-period-value</i>	60s

[Command Modes]

physical interface configuration

[Executing Command Instruction]

Command **dot1x timer quiet-period** is used to configure timer configuration value of 802.1x quiet period.

Command **no dot1x timer quiet-period** is used to recover timer configuration value of 802.1x quiet period.

[Explanation of command execution echo]

Set successfully.

Port x set unsuccessfully.

[Example]

Set quiet period timer configuration value on relevant port under physical interface configuration mode:

Raisecom(config-port)# **dot1x timer quiet-period 2400**

Recover default value of quiet period timer on relevant port under physical interface configuration mode:

Raisecom(config-port)# **no dot1x timer quiet-period**

[Related commands]

Commands	Description
show dot1x port-list <i>port-list</i>	Show port statistic information of 802.1x protocol.
show dot1x line <i>line-list</i>	Show line port statistic information of 802.1x protocol.
show dot1x client <i>client-list</i>	Show client port statistic information of 802.1x protocol.

30.5 dot1x timer reauth-period

[Function]

Configure 802.1x port reauthentication timer.

This command is available to ISCOM2000/2100/2800/2900/3000 series and 5X1-4FE.

[Command format]

[no] dot1x timer reauth-period *reauth-period-value*

[Parameter]

reauth-period: reauthentication timer. In the time of this timer setting, system enable 802.1x reauthentication, corresponding configuring value is *reauth-period-value*<1-65536>.

[Default]

Default configuration of all timers:

Timer	Variable	Configured value
reauth-period	<i>reauth-period-value</i>	3600s

[Command Modes]

physical interface configuration

[Executing Command Instruction]

Command **dot1x timer reauth-period** is used to configure 802.1x reauthentication timer configuration value.

Command **no dot1x timer reauth-period** is used to recover default value of 802.1x reauthentication timer configuration value.

[Explanation of command execution echo]

Set successfully.

Port x set unsuccessfully.

[Example]

Set reauthentication timer configuration value on relevant port under physical interface configuration mode:

Raisecom(config-port)# **dot1x timer reauth-period 2400**

Set reauthentication timer default value on relevant port under physical interface configuration mode:

Raisecom(config-port)# **no dot1x timer reauth-period**

[Related commands]

Commands	Description
show dot1x port-list <i>port-list</i>	Show port statistic information of 802.1x protocol.
show dot1x line <i>line-list</i>	Show line port statistic information of 802.1x protocol.
show dot1x client <i>client-list</i>	Show client port statistic information of 802.1x protocol.

30.6 dot1x timer server-timeout

[Function]

Configure server timeout timer of 802.1x port.

This command is available to ISCOM2000/2100/2800/2900/3000 series and 5X1-4FE.

[Command format]

[no] dot1x timer server-timeout *server-timeout-value*

[Parameter]

server-timeout: Authorization Server timeout timer. The timer define 802.1x protocol entity and radius server community timeout total time.

Radius re-send times and sending interval is decided by switch radius client side. The re-send time of switch radius client side is 3 and waiting time for every time is 5 seconds.

[Default]

Default configuration of all timers:

Timer	Variable	Configured value
server-timeout	<i>server-timeout-value</i>	100s

[Command Modes]

physical interface configuration

[Executing Command Instruction]

Command **dot1x timer server-timeout** is used to configure timer configuration value of 802.1x server.

Command **no dot1x timer server-timeout** is used to recover timer configuration value of 802.1x server.

[Explanation of command execution echo]

Set successfully.

Port x set unsuccessfully.

[Example]

Set server timer configuration value on relevant port under physical interface configuration mode:

Raisecom(config-port)# **dot1x timer server-timeout 2400**

Recover default value of server-timeout timer on relevant port under physical interface configuration mode:

Raisecom(config-port)# **no dot1x timer server-timeout**

[Related commands]

Commands	Description
----------	-------------

show dot1x port-list <i>port-list</i>	Show port statistic information of 802.1x protocol.
show dot1x line <i>line-list</i>	Show line port statistic information of 802.1x protocol.
show dot1x client <i>client-list</i>	Show client port statistic information of 802.1x protocol.

30.7 dot1x timer supp-timeout

[Function]

Configure port Request/Challenge re-transmitting timer in process of 802.1x authentication.

This command is available to ISCOM2000/2100/2800/2900/3000 series and 5X1-4FE.

[Command format]

[no] dot1x timer supp-timeout *supp-timeout-value*

[Parameter]

supp-timeout: Supplicant authorization timeout timer, the switch will startup supp-timeout timer when it send Request/Challenge message to client side (the message is used to request encrypt MD5 content). In the time of this timer setting, the switch re-transmit request if user request side fails to response, corresponding configuring value is *supp-timeout-value*<10-120>.

[Default]

Default configuration of all timers:

Timer	Variable	Configured value
supp-timeout	<i>supp-timeout-value</i>	30s

[Command Modes]

physical interface configuration

[Executing Command Instruction]

Command **dot1x timer supp-timeout** is used to configure timer configuration value of re-transmitting Request/Challenge message by 802.1x.

Command **no dot1x timer supp-timeout** is used to recover timer configuration value of re-transmitting Request/Challenge message by 802.1x.

[Explanation of command execution echo]

Set successfully.

Port x set unsuccessfully.

[Example]

Set Request/Challenge re-transmitting timer configuration value on relevant port under physical interface configuration mode:

Raisecom(config-port)# **dot1x timer supp-timeout 2400**

Recover default value of Request/Challenge re-transmitting on relevant port under physical interface configuration mode:

Raisecom(config-port)# **no dot1x timer supp-timeout**

[Related commands]

Commands	Description
show dot1x port-list <i>port-list</i>	Show port statistic information of 802.1x protocol.
show dot1x line <i>line-list</i>	Show line port statistic information of 802.1x protocol.
show dot1x client <i>client-list</i>	Show client port statistic information of 802.1x protocol.

30.8 dot1x timer tx-period

[Function]

Configure port Request/Identity re-sending timer in process of 802.1x authentication.

This command is available to ISCOM2000/2100/2800/2900/3000 series and 5X1-4FE.

[Command format]

[no] dot1x timer tx-period *tx-period-value*

[Parameter]

tx-period: transmission timeout timer, the switch will startup the timer when it sends Request/Identity message to client side. In the time of this timer setting, the switch re-transmit request if user request side fails to send authentication message, corresponding configuring value is *tx-period-value*<10-120>.

[Default]

Default configuration of all timers:

Timer	Variable	Configured value
tx-period	<i>tx-period-value</i>	30s

[Command Modes]

physical interface configuration

[Executing Command Instruction]

Command **dot1x timer tx-period** is used to configure timer configuration value of re-transmitting Request/Identity message by 802.1x.

Command **no dot1x timer tx-period** is used to recover timer configuration value of re-transmitting Request/Identity message by 802.1x.

[Explanation of command execution echo]

Set successfully.

Port x set unsuccessfully.

[Example]

Set Request/Identity re-transmitting timer configuration value on relevant port under physical interface configuration mode:

Raisecom(config-port)# **dot1x timer tx-period 2400**

Recover default value of Request/Identity re-transmitting on relevant port

under physical interface configuration mode:

Raisecom(config-port)# **no dot1x timer tx-period**

[Related commands]

Commands	Description
show dot1x port-list <i>port-list</i>	Show port statistic information of 802.1x protocol.
show dot1x line <i>line-list</i>	Show line port statistic information of 802.1x protocol.
show dot1x client <i>client-list</i>	Show client port statistic information of 802.1x protocol.

30.9 show dot1x

[Function]

Review configuration information of port 802.1x.

This command is available to ISCOM2000/2100/2800/2900/3000 series and 5X1-4FE.

[Command format]

show dot1x port-list *port-list*

show dot1x line *line-list*

show dot1x client *client-list*

[Parameter]

port-list: port list.

line-list: line port list.

client-list: client port list.

[Command Modes]

Privileged EXEC mode

[Executing Command Instruction]

Use this command to review port 802.1x configuration information.

[Example]

Show configuration information of particular 802.1x port under privileged EXEC mode:

Raisecom#**show dot1x port-list 1**

[Related commands]

Commands	Description
dot1x { <i>enable</i> <i>disable</i> }	Enable/disable 802.1x authorization based on port.
dot1x auth-control { <i>authorized-force</i> <i>unauthorized-force</i> <i>auto</i> }	Configure 802.1x port authorization mode.
dot1x reauthentication { <i>enable</i> <i>disable</i> }	Configure 802.1x port reauthentication function.
dot1x timer reauth-period <i>reauth-period-value</i>	Configure 802.1x port reauthentication timer
dot1x timer tx-period <i>tx-period-value</i>	Configure re-transmitting Request/Identity timer of 802.1x port.
dot1x timer supp-timeout <i>supp-timeout-value</i>	Configure re-transmitting Request/Challenge timer of 802.1x port.
dot1x timer server-timeout <i>server-timeout-value</i>	Configure radius server authentication total time out time.
dot1x timer quiet-period <i>quiet-period-value</i>	Configure 802.1x port quiet period timer.

30.10 show dot1x statistics

[Function]

Clear EAPOL statistics of port.

This command is available to ISCOM2000/2100/2800/2900/3000 series and 5X1-4FE.

[Command format]

show dot1x port-list *port-list* **statistics**

show dot1x line *line-list* **statistics**

show dot1x client *client-list* **statistics**

[Parameter]

port-list: port list.

line-list: line port list.

client-list: client port list.

[Command Modes]

Privileged EXEC mode

[Executing Command Instruction]

Use this command to query port statistic information during authentication.

[Example]

Show statistic information of port 1 under privileged EXEC mode:

Raisecom# **show dot1x port-list 1 statistics**

[Related commands]

Commands	Description
clear dot1x port-list <i>port-list</i> statistics	Clear port statistic information.
clear dot1x line <i>line-list</i> statistics	Clear line port statistic information.
clear dot1x client <i>client-list</i> statistics	Clear client port statistic information.

30.11 show radius-server

[Function]

Show configuration of RADIUS server.

This command is available to ISCOM2000/2100/2800/2900/3000 series and 5X1-4FE.

[Command format]

show radius-server

[Command Modes]

Privileged EXEC mode

[Executing Command Instruction]

Before using 802.1x authentication, configure RADIUS server IP, KEY and other information correctly. This command will show RADIUS server configuration information.

[Example]

Show configuration information of RADIUS server under privileged EXEC mode:

```
Raisecom# show radius-server
```

[Related commands]

Commands	Description
radius <i>ipaddress</i>	Set authentication server IP.
radius-key <i>string</i>	Set public key among RADIUS servers.

Chapter 31 IP Source Guard Commands

31.1 ip source binding

[Applicable Equipment]

ISCOM2828

[Function]

Use the command to configure static binding relationship

[Command Format]

ip source binding *ip-address* [*mac-address*] [**vlan** *vlanid*] **port** *port-id*

[Parameter]

Ip-address source IP address

Mac-address source MAC address

Vlanid VLAN ID

Port-id binding port ID

[Command Modes]

Privileged EXEC, privileged user

[Executing Command Instruction]

The following binding types are supported:

IP+PORT/IP+MAC+PORT/IP+VLAN+PORT/IP+MAC+VLAN+PORT.

Covering dynamic binding relationship is supported. When there is the same IP dynamic binding relationship in the binding table unit, the manually configured binding relationship using the command will cover the old dynamic binding relationship, but the existed static binding relationship can not be covered.

[Explanation of command execution echo]

Set successfully

When static binding relationship is configured successfully the information above will be shown below;

Set unsuccessfully

When static binding relationship is configured unsuccessfully the information above will be shown below.

[Example]

Raisecom (config)# **ip source binding 1.2.3.4 port 10**

[Related commands]

Command	Description
show ip source binding [port <i>port-id</i>]	Show the configured port binding

31.2 ip verify source

[Function]

Use this global command to enable static binding function. Use **no ip verify source** to stop this function.

[Command Format]

[no] ip verify source

[Default]

By default static binding function is disabled.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

By default IP Source Guard global static binding function is disabled, in condition that global static binding function is disabled, the configured static binding relationship will not be sent to the hardware, and the

binding relationship will not take effect. Only when global static binding function is enabled can static binding relationship takes effect.

[Explanation of command execution echo]

Set successfully

When global static binding function is enabled successfully, the information above will be shown.

Set unsuccessfully

When global static binding function is enabled unsuccessfully, the information above will be shown.

Set successfully

When global static binding function is disabled successfully, the information above will be shown.

Set unsuccessfully

When global static binding function is disabled unsuccessfully, the information above will be shown.

[Example]

Enable static binding function:

Raisecom (config)# **ip verify source**

Disable static binding function:

Raisecom (config)# **no ip verify source**

[Related commands]

Command	Description
show ip verify source	Show static/dynamic function and port trust state

31.3 ip verify source trust

[Applicable Equipment]

ISCOM2828

[Function]

Use the command to configure a port to trust state, use **no ip verify source trust** to configure the port to distrust state.

[Command Format]

[no] ip verify source trust

[Default]

By default all the ports are configured in distrust state.

[Command Modes]

Privileged EXEC, Privileged user

[Executing Command Instruction]

When the port is configure to trust state, all the static/dynamic binding relationship can not be written into the hardware, and all the stream on the port can be transmitted normally; when the port is configured distrust state and global static/dynamic switch is on, al the static/dynamic binding relationship on the port can be written into the hardware, only the stream that has DHCP messages or accords with the binding relationship can be transmitted normally, while the others will be dropped.

[Explanation of command execution echo]

Set successfully

When port trust function is enabled successfully, the information above will be shown.

Set unsuccessfully

When port trust function is enabled unsuccessfully, the information above will be shown.

Set successfully

When port distrust function is disabled successfully, the information above will be shown.

Set unsuccessfully

When port distrust function is disabled unsuccessfully, the information above will be shown.

[Example]

Configure port trust:

Raisecom (config)# **ip verify source trust**

Configure port distrust

Raisecom (config)# **no ip verify source trust**

[Related commands]

Command	Description
show ip verify source	Show static/dynamic function and port trust state

31.4 show ip verify source

[Applicable Equipment]

ISCOM2828

[Function]

Show static/dynamic function and port trust state

[Command Format]

[no] ip verify source trust

[Command Modes]

Privileged EXEC

[Related commands]

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

[no] ip verify source trust	Configure port trust/distrust state
[no] ip verify source dhcp-snooping	Global dynamic binding function switch
[no] ip verify source	Global static binding function switch

Chapter 32 Auto-configuration and load commands

32.1 service config

[Function]

Operating auto-configuration and load task. This command is available to device types of ISCOM2000/2100/2800/2900/3000 series.

[Command format]

service config

[Command Modes]

Global configuration mode, Privileged user

[Executing Command Instruction]

Use this command to operating auto-configuration and load. It will fail to set if there is auto-configuration and load task running.

[Explanation of command execution echo]

Start auto configuration load task.

Getting FILENAME from server A.B.C.D.

Acquiring tfip server address failed.

Loading FILENAME of server A.B.C.D.

Getting FILENAME from server A.B.C.D failed.

Loading FILENAME of server A.B.C.D failed.

Writing FILENAME from server A.B.C.D to local configuration file.

Writing local configuration file failed.

Loading FILENAME of server A.B.C.D failed.

Loading FILENAME of server A.B.C.D succeeded

Another auto configuration task is running.

[Example]

Operating auto-configuration and load task:

Raisecom(config)# **service config**

[Related commands]

Commands	Description
service config filename <i>FILENAME</i>	Command for configuring filename.
no service config filename	Recover configuration filename.
service config tftp-server <i>A.B.C.D</i>	Configure server address.
no service config tftp-server	Recover server address.
service config overwrite <i>{enable/disable}</i>	Enable/disable local configuration file overwrite function.
service config startup <i>{enable/disable}</i>	Enable/disable auto-configuration and load of power on startup.
show service config	Show state and auto-configuration setting.

32.2 service config filename

[Function]

Configure filename. This command is available to ISCOM2000/2100/2800/2900/3000 series.

[Command format]

service config filename *FILENAME*

[Parameter]

FILENAME: the file name.

[Command Modes]

Global configuration mode, Privileged user

[Executing Command Instruction]

The filename can not set be blank, only when operating its inverse command, the filename can be blank. The longest filename can be 80 characters, range from 1 to 80. Operating this command in condition that there is no auto-configuration and load task being run.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

The input file name is too long.

Invalid file name

[Example]

Operating auto-configuration load:

Raisecom(config)# **service config**

[Related commands]

Commands	Description
service config	Startup auto-configuration and load.
no service config filename	Recover configuration filename.
service config tftp-server A.B.C.D	Configure server address.
no service config tftp-server	Recover server address.
service config overwrite {enable/disable}	Enable/disable local configuration file overwrite function.

service config startup {enable/disable}	Enable/disable auto-configuration and load of power on startup.
show service config	Show state and auto-configuration setting.

32.3 service config filename rule

[Function]

Set configure filename rule

[Command format]

[no] service config filename rule [<80001-89999>]

[Parameter]

Rule: command rule

<80001-89999>: rule number, range is 80001-89999

[Command Modes]

Global configuration mode; privileged user (priority 15).

[Executing Command Instruction]

In global configuration mode, use the command to set configure filename rule. If the rule ID is available, it will cover the former rule ID directly. In the process of auto-configuration load, the configure filename will be established according to the rule and download startup-file from TFTP server. Without designated rule ID, it will inform use the make sure 3 questions, and the create rule ID according to the question user choose, if the answer user input is not in the range of candidate answers, then the configuration fails.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

Se unsuccessfully. Rule number is not supported yet!

Set unsuccessfully. Rule setting error!

Please check device type rule, configuration filename

0 – includes no device type information

1 – includes device type information

Please select:

Please check MAC address rule, configuration filename

0 – includes no MAC address information

1 – includes the first 2 characters in MAC address

2 – includes the first 4 characters in MAC address

3 – includes the first 6 characters in MAC address

4 – includes the first 8 characters in MAC address

5 – includes the first 10 characters in MAC address

6 – includes all characters in MAC address

Please select:

Please check ROS version rule, configuration filename

0 – includes no ROS version information

1 – includes entire ROS version information

2 – includes all except device type

3 – includes all except device type and date

4 – includes the highest 3 version number

5 – includes the highest 2 version number

6 – includes the highest version number

Please select:

[Example]

Set configure file naming rule

Raisecom(config)# **service config filename rule 81630**

[Related commands]

Commands	Description
----------	-------------

[no]service config	Enable/disable auto-update
no service config filename	Recover configuration filename.
service config tftp-server A.B.C.D	Configure server address.
no service config tftp-server	Recover server address.
service config overwrite {enable/disable}	Enable/disable local configuration file overwrite function.
service config startup {enable/disable}	Enable/disable auto-configuration and load of power on startup.
show service config	Show state and auto-configuration setting.

32.4 service config overwrite

[Function]

Configure whether local configuration file is covered by server configuration file. This command is available to ISCOM2000/2100/2800/2900/3000 series.

[Command format]

service config overwrite {enable/disable}

[Parameter]

enable: enable.

disable: disable.

[Default]

disable

[Command Modes]

Global configuration mode, Privileged user

[Executing Command Instruction]

After using this command and startup auto-configuration load, the server configuration file covers local configuration file.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Enable overwrite:

```
Raisecom(config)# service config overwrite enable
```

Disable overwrite:

```
Raisecom(config)# service config overwrite disable
```

[Related commands]

Commands	Description
service config filename <i>FILENAME</i>	Command for configuring filename.
no service config filename	Recover configuration filename.
service config tftp-server <i>A.B.C.D</i>	Configure server address.
no service config tftp-server	Recover server address.
service config startup <i>{enable/disable}</i>	Enable/disable auto-configuration and load of power on startup.
show service config	Show state and auto-configuration setting.
service config	Startup auto-configuration and load.

32.5 service config tftp-server

[Function]

Configure TFTP server address.

This command is available to ISCOM2000/2100/2800/2900/3000 series.

[Command format]

```
service config tftp-server A.B.C.D
```

[Parameter]

A.B.C.D: IP address.

[Default]

0.0.0.0

[Command Modes]

Global configuration mode, Privileged user

[Executing Command Instruction]

IP address should be type A, B and C, it should not be all 0 address, broadcast address, type D address and reserved type E address. After operating inverse command, IP address can set to all 0 address and use **show service config** to show address "--".

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

Invalid IP address

[Example]

Configure TFTP server address:

Raisecom(config)# **service config tftp-server A.B.C.D**

[Related commands]

Commands	Description
service config filename <i>FILENAME</i>	Command for configuring filename.
no service config filename	Recover configuration filename.
service config	Startup auto-configuration and load.
no service config tftp-server	Recover server address.
service config overwrite <i>{enable/disable}</i>	Enable/disable local configuration file overwrite function
service config startup <i>{enable/disable}</i>	Enable/disable auto-configuration and load of power on startup.
show service config	Show state and auto-configuration setting.

32.6 service config trap

[Function]

Configure auto-update module TRAP switch.

[Command format]

service config trap *{enable/disable}*

[Parameter]

enable: enable.

disable: disable.

[Default]

disable

[Command Modes]

Global configuration mode, Privileged user (priority 15)

[Executing Command Instruction]

When device auto-update TRAP is enabled and file update finished, file update complete TRAP will be sent.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Enable auto-update TRAP:

Raisecom(config)# **service config trap enable**

Disable overwrite:

Raisecom(config)# **service config trap disable**

[Related commands]

Commands	Description
show service config	Show state and auto-configuration setting.

32.7 service config version

[Function]

Configure auto-update file version ID

[Command format]

service config version {system-boot | bootstrap | startup-config}

VERSION

[Parameter]

System-boot: system boot file

Bootstrap: bootstrap file

Startuup-config: system boot configuration file

VERSION: version ID, format is 'year- month- day –times', like 0906031

[Default]

System software default version ID is establish data adding 0, like 0906030

[Command Modes]

Global configuration mode, Privileged user (priority 15)

[Executing Command Instruction]

The version ID will be updated no matter if the update file is download successfully. The version character string length is stable 7 bytes, which must be figures

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

Version-string length must be 7

[Example]

Configure system-boot file version number:

Raisecom(config)# **service config version system-boot 0906035**

Configure startup-config file version number:

Raisecom(config)# **service config version bootstrap 0905063**

[Related commands]

Commands	Description
show service config	Show state and auto-configuration setting.

32.8 show service config

[Function]

Show auto-configuration state and setting.

This command is available to ISCOM2000/2100/2800/2900/3000 series.

[Command format]

Show service config

[Command Modes]

Privileged EXEC mode, Privileged user

[Executing Command Instruction]

Use this command to review auto-configuration load setting and state. The showing information includes power on load, configure server IP address, configure file name, overwrite local configuration file, finish sending alarm, current running state and result state.

[Explanation of command execution echo]

Perform on startup: <enable/disable>

Config server IP address: <IP>

Config file name: <file name>

Overwrite local configuration file: <enable/disable>

Send Completion trap: <enable/disable>

Operation states: <waiting /getting/loading/writing /done>

Result:

<none/succeeded/acquireFailed/getFailed/writeFailed/notEnoughMemory/other>

[Example]

Operate showing command:

Raisecom(config)# **show service config**

[Related commands]

Commands	Description
service config filename <i>FILENAME</i>	Command for configuring filename.
no service config filename	Recover configuration filename.
service config tftp-server <i>A.B.C.D</i>	Configure server address.
no service config tftp-server	Recover server address.
service config overwrite <i>{enable/disable}</i>	Enable/disable local configuration file overwrite function
service config startup <i>{enable/disable}</i>	Enable/disable auto-configuration and load of power on startup.
service config	Startup auto-configuration and load.

32.9 show service config filename rule

[Function]

Explain configure file naming rule

[Command format]

Show service config filename rule [*<80001-89999>*]

[Command Modes]

Privileged EXEC mode, Privileged user (priority 10)

[Executing Command Instruction]

When using the command, if the rule number has been designated, the meaning will be shown; if it is not designated, then the detailed rule instruction will be shown.

[Explanation of command execution echo]

Rule number <rule number> is reserved

Configuration filename rule number <rule number> indicate rule below

Device type: *X*

MAC Address: *AaBb CcDdEeFf*

Ros Version: *ROS_h.i.j.X.k.y*

Filename: *<configuration filename>*

Filename = *(Device Type)_M(MAC Address info)_(ROS Version info)*

Device type: X

MAC address: AaBb.CcDd.EeFf

ROS version: ROS_h.i.j.X.k.Y

Rule Number 8wxyz indicate:

8 – no meaning

w – whether including device information

0 – including no device type information

1 – including device type information (X)

x – MAC address information in filename

0 – including no MAC address information

1 – including the first 2 characters in MAC address (Aa)

2 – including the first 4 characters in MAC address (AaBb)

3 – including the first 6 characters in MAC address (AaBb.Cc)

4 – including the first 8 characters in MAC address (AaBb.CcDd)

*5 – including the first 10 characters in MAC address
(AaBb.CcDd.Ee)*

6 – including all characters in MAC address (AaBb.CcDd.EeFf)

7-9 reserve

y – ROS version information in filename

0 – including no ROS version information

1 – including entire ROS version information

2 – including all except device type (ROS_h.i.j.k.Y)

3 – including all except device type and date (ROS_h.i.j.k)

4 – including the highest 3 version number (ROS_h.i.j)

5 – including the highest 2 version number (ROS_h.i)

6 – including the highest version number (ROS_h)

7-9 *reserve*

z – *Extended information*

0 – *including no extended information*

1-9 *reserve*

Example:

<i>rule number</i>	<i>filename</i>
81050	<i>X_ROS_h.i</i>
80130	<i>MAaBb_ROSh.i.j.k</i>
80010	<i>ROS_h.i.j.X.k.Y</i>
81630	<i>X_MAAaBb.CcDd.EeFf_ROS_h.i.j.k</i>

[Example]

Explain config-file naming rule:

Raisecom# **show service config filename rule**

[Related commands]

Commands	Description
no service config filename	Recover configuration filename.
no service config tftp-server	Recover server address.
No server config	Enable/disable auto-update

Chapter 33 Commands of Ethernet Ring

33.1 clear ethernet ring statistics

[Function]

Clear Ethernet ring protocol message statistics

[Command Format]

Clear Ethernet ring [*ring ID*] statistics

[Parameter]

Ringid: Ethernet ring ID, range is 1-8

[Default]

None.

[Command Modes]

Privileged EXEC mode; privileged user (priority 15)

[Executing Command Instruction]

None

[Explanation of command execution echo]

1

Set successfully

2

Set unsuccessfully

3

Ethernet ring X does not exist

[Example]

Clear ring 1 statistics

Raisecom# **clear Ethernet ring 1 statistics**

[Related commands]

Commands	Description
Show Ethernet ring [<1-8>] port	Show Ethernet ring port configuration
Show Ethernet ring [<1-8>] port statistics	Show Ethernet ring port message statistics

33.2 ethernet ring

[Function]

Enable/disable Ethernet ring

[Command Format]

Ethernet ring <RingID> {enable | disable}

[Parameter]

Ringid: Ethernet ring ID, range is 1-8

Enable: enable ring switch

Disable: disable ring switch

[Default]

Ring switch is disabled

[Command Modes]

Global configuration mode; privileged user (priority 15)

[Executing Command Instruction]

When the ring is enabled, Ethernet ring protocol will work normally

[Explanation of command execution echo]

1

Set successfully

2

Set unsuccessfully

3

Ring X is already enabled

[Example]

Enable ring switch

Raisecom(config)# **Ethernet ring 1 enable**

[Related commands]

Commands	Description
Show Ethernet ring [<1-8>]	Show Ethernet ring configuration
Show Ethernet ring [<1-8>] port	Show Ethernet ring port configuration

33.3 ethernet ring description

[Function]

Configure Ethernet ring description

[Command Format]

Ethernet ring <RingID> **description** <word>

[Parameter]

Ringid: Ethernet ring ID, range is 1-8

<word>: ring description

[Default]

By default it is configured to Ethernet Ring X, X stands for ring number

[Command Modes]

Global configuration mode; privileged user (priority 15)

[Executing Command Instruction]

None

[Explanation of command execution echo]

1

Set successfully

2

Set unsuccessfully

3

Ethernet ring X does not exist

4

Description can not exceed 32 characters

[Example]

Configure ring 1 description

Raisecom(config)# **Ethernet ring 1 description** CaiHongMansion

[Related commands]

Commands	Description
No Ethernet ring <1-8> description	Restore Ethernet ring to default description
Show Ethernet ring [<1-8>] port	Show Ethernet ring port message statistics

33.4 ethernet ring hello-time

[Function]

Configure Ethernet ring hello message interval

[Command Format]

Ethernet ring <RingID> **hello-time** <hellotime>

[Parameter]

Ringid: Ethernet ring ID, range is 1-8

Hello-time: hello message interval, value range is 1-180, unit is second

[Default]

Default hello time is 1s

[Command Modes]

Global configuration mode; privileged user (priority 15)

[Executing Command Instruction]

When the ring is enabled, Ethernet ring protocol will work normally

[Explanation of command execution echo]

1

Set successfully

2

Set unsuccessfully

3

Ring X does not exit

[Example]

Set hello time to 3s

Raisecom(config)# **Ethernet ring 1 hello-time 3**

[Related commands]

Commands	Description
No Ethernet ring <i><1-8> hello time</i>	Restore hello time to default value
Show Ethernet ring <i>[<1-8>]</i>	Show Ethernet ring configuration
Show Ethernet ring <i>[<1-8>] port</i>	Show Ethernet ring port configuration

33.5 ethernet ring holdtime

[Function]

Configure Ethernet ring port ageing time

[Command Format]

Ethernet ring <RingID> **hold-time** <holdtime>

[Parameter]

Ringid: Ethernet ring ID, range is 1-8

Holdtime: hello message interval, range is 3-360, unit is second

[Default]

Default value is 15s

[Command Modes]

Global configuration mode; privileged user (priority 15)

[Executing Command Instruction]

None.

[Explanation of command execution echo]

1

Set successfully

2

Set unsuccessfully

3

Ring X does not exist

[Example]

Set ring 1 ring-port ageing time:

Raisecom(config)# **Ethernet ring 1 holdtime 10**

[Related commands]

Commands	Description
No Ethernet ring <1-8> holdtime	Restore Ethernet ring 1 holdtime to default value
Show Ethernet ring [<1-8>]	Show Ethernet ring configuration
Show Ethernet ring [<1-8>] port	Show Ethernet ring port configuration

33.6 ethernet ring port

[Function]

Create Ethernet ring

[Command Format]

Ethernet ring <RingID>secondaryport

[Parameter]

Ringid: Ethernet ring ID, range is 1-8

Secondaryport: secondary port

[Default]

None

[Command Modes]

Port configuration mode; privileged user (priority 15)

[Executing Command Instruction]

It is requested to configure the command in first port mode

[Explanation of command execution echo]

1

Set successfully

2

Set unsuccessfully

3

Primary and Secondary port of Ethernet ring can not be the same

4

Error Configuration

5

Port X has been configured as ring port before

Ring X has already been existed

[Example]

Set ring number to 1, first port and secondary port are X and Y respectively

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

Raisecom(config-port)# **Ethernet ring 1 Y**

[Related commands]

Commands	Description
No Ethernet ring	Delete ring
Show Ethernet ring [<1-8>]	Show Ethernet ring configuration
Show Ethernet ring [<1-8>] port	Show Ethernet ring port configuration

33.7 ethernet ring priority

[Function]

Configure ring priority

[Command Format]

Ethernet ring <RingID>**priority** <priority>

[Parameter]

Ringid: Ethernet ring ID, range is 1-8

Priority: priority range is 0-255; 0 stands for the lowest priority, 255

stands for the highest priority

[Default]

Default priority is 1

[Command Modes]

Global configuration mode; privileged user (priority 15)

[Executing Command Instruction]

None

[Explanation of command execution echo]

1

Set successfully

2

Set unsuccessfully

3

Ethernet ring X does not exist

[Example]

Set bridge priority to 3

Raisecom(config)# **Ethernet ring 1 priority 3**

[Related commands]

Commands	Description
No Ethernet ring <1-8>	Restore bridge priority to default value
Show Ethernet ring [<1-8>]	Show Ethernet ring configuration
Show Ethernet ring [<1-8>] port	Show Ethernet ring port configuration

33.8 ethernet ring protocol-vlan

[Function]

Configure Ethernet ring protocol vlan

[Command Format]

Ethernet ring <RingID> **protocol-vlan** <protocolvlan>

[Parameter]

Ringid: Ethernet ring ID, range is 1-8

protocolvlan: protocol vlan range is 2-4094

[Default]

Default priority is 2

[Command Modes]

Global configuration mode; privileged user (priority 15)

[Executing Command Instruction]

None

[Explanation of command execution echo]

1

Set successfully

2

Set unsuccessfully

3

Ethernet ring X does not exist

[Example]

Set ring 1 protocol message VLAN to 5:

Raisecom(config)# **Ethernet ring 1 protocol-vlan 5**

[Related commands]

Commands	Description
No Ethernet ring <1-8> protocol-vlan	Restore Ethernet ring protocol VLAN
Show Ethernet ring [<1-8>]	Show Ethernet ring configuration
Show Ethernet ring [<1-8>] port	Show Ethernet ring port configuration

33.9 ethernet ring restore-delay

[Function]

Configure fault restore delay time

[Command Format]

Ethernet ring <RingID> **restore-delay** <RestoreRelay>

[Parameter]

Ringid: Ethernet ring ID, range is 1-8

RestoreRelay: delay time range is 3-180s

[Default]

Default Restore Delay is 5s

[Command Modes]

Global configuration mode; privileged user (priority 15)

[Executing Command Instruction]

None

[Explanation of command execution echo]

1

Set successfully

2

Set unsuccessfully

3

Ethernet ring X does not exist

[Example]

Set Restore Delay to 15s:

Raisecom(config)# **Ethernet ring 1 restore-delay 15**

[Related commands]

Commands	Description
No Ethernet ring <1-8> restore-delay	Configure restore delay time
Show Ethernet ring [<1-8>]	Show Ethernet ring configuration
Show Ethernet ring [<1-8>] port	Show Ethernet ring port configuration

33.10 show ethernet ring

[Function]

Show Ethernet ring configuration

[Command Format]

Show Ethernet ring [<RingID>]

[Parameter]

Ringid: Ethernet ring ID, range is 1-8

[Default]

None

[Command Modes]

Privileged EXEC mode; privileged user (priority 15)

[Executing Command Instruction]

None

[Explanation of command execution echo]

I

Ring Global Switch: <global switch variable>

Ethernet Ring X:

Ring Admin: <ring switch variable>

Ring State: <ring state variable>

Bridge State: <ring state variable>

Ring state duration: <ring state duration>

Bridge Priority: <bridge priority variable>

Bridge MAC: <bridge MAC>

Ring DB State: <DB state variable>

Ring DB Priority: <DB priority variable>

Ring DB: <DB MAC address>

Hello Time: <hello message sending interval, unit: second>

Restore delay: <fault restore delay time, unit: second>

Hold Time: <ring port ageing time, unit: second>

Protocol Vlan: <protocol vlan>

[Example]

Show ring 1 configuration

Raisecom# **show Ethernet ring 1**

[Related commands]

Commands	Description
Show Ethernet ring [<i><1-8></i>] port	Show Ethernet ring port configuration
Show Ethernet ring [<i><1-8></i>] port statistics	Show Ethernet ring port statistics

33.11 show ethernet ring port

[Function]

Show Ethernet ring port configuration

[Command Format]

Show Ethernet ring [*<RingID>*] port

[Parameter]

Ringid: Ethernet ring ID, range is 1-8

[Default]

None

[Command Modes]

Privileged EXEC mode; privileged user (priority 10)

[Executing Command Instruction]

None

[Explanation of command execution echo]

Primary Port: <primary port configuration>

Port Active State: <port activity state, the value can be Active/Inactive>

State: <primary port state, the value can be Block/Forward>

Peer State: <peer port state, the value is None/Discovery/Full>

Switch counts: <secondary port switch time>

Current state duration: <secondary port current state duration>

Peer Ring Node: <device list information>

Secondary Port: <secondary port configuration>

Port Active State: <port activity state, the value is Active/Inactive>

State: <primary port state, the value is Block/Forward>

Peer State: <peer port state, the value state is None/Discovery/Full>

Switch counts: <primary port state switch time>

Current state duration: <primary port current state duration>

Peer Ring Node: <device list information>

[Example]

Show ring 1 configuration

Raisecom# **show Ethernet ring 1 port**

[Related commands]

Commands	Description
----------	-------------

Show Ethernet ring [<i><1-8></i>]	Show Ethernet ring configuration
Show Ethernet ring [<i><1-8></i>] port statistic	Show Ethernet ring port message statistics

33.12 show ethernet ring port statistic

[Function]

Show Ethernet ring port message statistics

[Command Format]

Show Ethernet ring [*<RingID>*] port statistic

[Parameter]

Ringid: Ethernet ring ID, range is 1-8

[Default]

None

[Command Modes]

Privileged EXEC mode; privileged user (priority 10)

[Executing Command Instruction]

None

[Explanation of command execution echo]

Primary Port: <primary port configuration>

Port Active State: <port activity state, the value can be Active/Inactive>

State: <primary port state, the value can be Block/Forward>

Peer State: <peer port state, the value is None/Discovery/Full>

Switch counts: <secondary port switch time>

Current state duration: <secondary port current state duration>

Peer Ring Node: <device list information>

Secondary Port: <secondary port configuration>

Port Active State: <port activity state, the value is Active/Inactive>

State: <primary port state, the value is Block/Forward>

Peer State: <peer port state, the value state is None/Discovery/Full>

Switch counts: <primary port state switch time>

Current state duration: <primary port current state duration>

Peer Ring Node: <device list information>

[Example]

Show ring 1 configuration

Raisecom# **show Ethernet ring 1 port statistic**

[Related commands]

Commands	Description
Show Ethernet ring [<1-8>]	Show Ethernet ring configuration
Show Ethernet ring [<1-8>] port	Show Ethernet ring port configuration

Chapter 34 Traceroute Commands

34.1 traceroute

[Applicable Equipment]

ISCOM serious switches

[Function]

Trace the route that a message has taken

[Command Format]

Traceroute A.B.C.D [**firstTTL** *first-TTL*] [**maxTTL** *max-TTL*] [**port** *port*] [**waittime** *timeout*] [**count** *num-packet*]

[Parameter]

A. B. C. D: the traced destination IP address

firstTTL: specify the least hop number, range is 1-255

maxTTL: specify the maximum hop number, range is 1-255

port: specify the probe message destination port number, range is 1-65535, usually it is larger than 300000

waittime: specify the overtime length that traceoute waits for answering, range is 1-60, the default value is 3s

count: specify each TTL probe packets number, range is 1-10, the default value is 3s

[Default]

firstTTL default value is 1

maxTTL default value is 30

port default value is 33434

waittime default value is 3s

count default value is 3

[Command Modes]

Privilege EXEC and privilege users

[Explanation of command execution echo]

When the commands is executed successfully, the information below will be shown:

Router1#**traceroute 34.0.0.4**

Type ctrl+c to abort.

Tracing the route to 34.0.0.4

1 12.0.0.2 4 ms 4 m 4 m

2 23.0.0.3 20 ms 16 ms 16 ms

*3 34.0.0.4 16 ms * 16 ms*

Trace complete

When the configured destination IP address is invalid the information below will be shown:

Raisecom #%"<ipaddress>" Invalid IP Address.

<ipaddress> strands for the IP address got from input or mib configuration

[Example]

Trace the route to www.sina.com.cn(58.63.236.42)

Raisecom#**config**

Raisecom(config)# **int ip 0**

Raisecom(config-ip)#**ip address 10.0.0.8 1**

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

Raisecom(config)#**ip default-gateway 10.100.0.1**

Raisecom(config)#**exit**

Raisecom#Tracing the route to 58.63.236.42

Type ctrl+c to abort.

```
1  10.0.0.1    10 ms   10 ms   10 ms
      2  192.168.101.5  3 ms     3 ms   73 ms
3  192.168.101.5  10 ms   10 ms   10 ms
      4  202.96.4.81  18 ms   16 ms   19 ms
5  202.106.228.177  9 ms     5 ms   12 ms
      6  202.106.228.5  10 ms    8 ms    9 ms
7  202.96.12.25  7 ms     8 ms    5 ms
      8  219.158.11.66 24 ms    20 ms   10 ms
9  202.97.15.57  101 ms   101 ms  126 ms
10 202.97.60.185  218 ms   222 ms  205 ms
11 202.97.40.58  119 ms   112 ms  113 ms
12 219.136.246.134 118 ms   142 ms  131 ms
13 219.136.246.6  138 ms   135 ms  110 ms
14 58.63.232.46  103 ms   115 ms  105 ms
15 58.63.236.42  199 ms   205 ms  197 ms
```

Trace complete

[Related commands]

Command	Description
ip default-gateway A.B.C.D	Configure the switch default gateway
interface address A.B.C.D	Configure the switch IP address

34.2 traceroute concurrent number

[Applicable Equipment]

ISCOM serious switches

[Function]

Configure traceroute maximum concurrent number

[Command Format]

Traceroute concurrent number

[Command Mode]

Hide mode

[Executing Command Instruction]

The command is mainly used in system test, use the command to change **traceroute mib** maximum concurrent number to 1 or restore it to default value 10; when the command is used for the first time, traceroute maximum concurrent number will be changed to 1; when the command is executed for the second time, the maximum concurrent number will be restored to default value 10.

[Explanation of command execution echo]

The first time that the command is executed:

Raisecom(debug)# **traceroute concurrent number**

traceroute max concurrent instance number is 1

The second time that the command is executed:

Raisecom(debug)# **traceroute concurrent number**

traceroute max concurrent instance number is 10

[Example]

Configure traceroute maximum concurrent number to 1:

Raisecom(debug)# **traceroute concurrent number**

Chapter 35 TACACS+ Commands

35.1 enable login

[Function]

Configure authentication mode of enable login.

[Command Format]

```
enable login {local-radius / local-user / radius-local  
[server-no-response] / radius-user / tacacs-user / tacacs-local  
[server-no-response] / local-tacacs}
```

[Parameters]

local-radius: the local user has precedence over radius user;

local-user: local user;

radius-local: user on remote radius server has precedence over local user;

radius-local server-no-response Radius: user on remote radius server has precedence over local user; use local user to login when radius server doesn't respond;

radius-user: user on remote radius server;

tacacs-user: user on remote tacacs+ server;

tacacs-local: user on remote tacacs+ server has precedence over local user;

tacacs-local server-no-response: user on remote tacacs+ server has precedence over local user; use local user to login when tacacs+ server doesn't respond;

local-tacacs: the local user has precedence over tacacs+ user.

[Default]

Default enable login mode is local-user.

[Command Modes]

Privileged EXEC mode

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Configure enable login mode of switch to be tacacs-local:

Raisecom# **enable login** *tacacs-local*

[Related commands]

Commands	Description
user login { <i>local-radius</i> / <i>local-user</i> / <i>radius-local</i> [<i>server-no-response</i>] / <i>radius-user</i> / <i>tacacs-user</i> / <i>tacacs-local</i> [<i>server-no-response</i>] / <i>local-tacacs</i> }	Configure authentication mode of user login.

35.2 show tacacs-server

[Function]

Show tacacs+ server address, key and authentication packets statistics information.

[Command Format]

show tacacs-server

[Default]

Tacacs+ Server Info:

Sever Address: --

Sever Shared Key: --

Total Packet Sent: 0

Total Packet Recv: 0

Num of Error Packets: 0

[Command Modes]

Privileged EXEC mode

[Explanation of command execution echo]

Tacacs+ Server Info:

Sever Address: <IP address>

Sever Shared Key: <the key>

Total Packet Sent: <send packets>

Total Packet Recv: <received packets>

Num of Error Packets: <error packets>

[Related commands]

Commands	Description
tacacs-server <i>A.B.C.D</i>	Configure tacacs+ server address.
tacacs-server key	Configure tacacs+ server key.

35.3 tacacs-server

[Function]

Configure tacacs+ server address.

[Command Format]

[no] tacacs-server *A.B.C.D*

[Parameters]

A.B.C.D: tacacs server address, must be unicast address.

[Default]

The server address is 0.0.0.0 by default, shown as "--".

[Command Modes]

Privileged EXEC mode

[Explanation of command execution echo]

Set successfully

Show the information for succeeding in configuring server address.

Invalid IP Address

Configuration is failure if the input ip address is illegal unicast address.

[Example]

Set Tacacs+ server address to be 192.168.0.100:

Raisecom# **tacacs-server** 192.168.0.100

Delete Tacacs+ server address:

Raisecom# **no tacacs-server**

[Related commands]

Commands	Description
show tacacs-server	Show configuration of tacacs+.

35.4 tacacs-server key

[Function]

Configure tacacs+ server key.

[Command Format]

[no] tacacs-server key *WORD*

[Parameters]

WORD: string of key, in length of 200 characters.

[Default]

The key is empty by default.

[Command Modes]

Privileged EXEC mode

[Explanation of command execution echo]

Set successfully

Show the information for succeeding in configuring key.

Key can not exceed 200 characters

Show the information if input key string over 200 characters.

Set unsuccessfully

Show the information for failing to configure key.

[Example]

Configure Tacacs+ server key to be 123:

Raisecom# **tacacs-server key 123**

Delete Tacacs+ server key:

Raisecom# **no tacacs-server key**

[Related commands]

Commands	Description
show tacacs-server	Show configuration of tacacs+.

35.5 user login

[Function]

Configure user login mode.

[Command Format]

user login { *local-radius / local-user / radius-local [server-no-response]*
/ *radius-user / tacacs-user / tacacs-local [server-no-response]* /

local-tacacs}

[Parameters]

local-radius: the local user has precedence over radius user;

local-user: local user;

radius-local: user on remote radius server has precedence over local user;

radius-local server-no-response Radius: user on remote radius server has precedence over local user; use local user to login when radius server doesn't respond;

radius-user: user on remote radius server;

tacacs-user: user on remote tacacs+ server;

tacacs-local: user on remote tacacs+ server has precedence over local user;

tacacs-local server-no-response: user on remote tacacs+ server has precedence over local user; use local user to login when tacacs+ server doesn't respond;

local-tacacs: the local user has precedence over tacacs+ user.

[Default]

Default user login mode is local-user.

[Command Modes]

Privileged EXEC mode

[Explanation of command execution echo]

Set User Login Method unsuccessfully

[Example]

Configure user login mode of switch to be tacacs-local:

Raisecom# **user login** *tacacs-local*

[Related commands]

Commands	Description
----------	-------------

enable login {*local-radius* / *local-user* / *radius-local*
[server-no-response] / *radius-user* / *tacacs-user* /
tacacs-local [*server-no-response*] / *local-tacacs*}

Configure authentication
mode of enable login.

Chapter 36 SLA Commands

36.1 show sla configuration

[Function]

Show operation related configuration

[Command Format]

Sla sla {all | *oper-num*} configuration

[Parameter]

Oper-num SLA operation number, range is 1-65535

all show all the SLA operation configuration

[Default]

By default SLA operation configuration will not be shown

[Command Modes]

Privileged EXEC mode; privileged user

[Executing Command Instruction]

Only user with priority level 10 can use the command

[Explanation of command execution echo]

Set successfully

Operation XX does not exist

Operation <1>:

Type: cfm echo

StartTime : Starttime

CoS:

CoS

Vlan ID: vlanId

MD Level: mdLevel

Destination Mac Address: HHHH.HHHH.HHHH

Timeout(sec): 5

Schedule Status: status

Schedule Life(sec): life

Schedule Period(sec):
period-----

Operation <I>:

Type: cfm echo

StartTime : Starttime

CoS: CoS

Vlan ID: vlanId

MD Level: mdLevel

Destination Mac Address: HHHH.HHHH.HHHH

Timeout(seconds): 5

Packet Interval(millionseconds) : interval

Number of Packets: packetNum

Schedule Status: status

Schedule Life(seconds): life

Schedule Period(seconds): period

Operation <I>:

Type: icmp echo

StartTime : Starttime

Destination IP Address: *A.B.C.D*

Timeout(sec): *5*

Schedule Status: *status*

Schedule Life(sec): *life*

Schedule Period(sec): *period*

Operation <I>:

Type: icmp jitter

StartTime : Starttime

Destination IP Address: *A.B.C.D*

Timeout(sec): *5*

Packet Interval(millionseconds) : *interval*

Number of Packets: *packetNum*

Schedule Status: *status*

Schedule Life(sec): *life*

Schedule Period(sec): *period*

The total number of operation configured is <0>

[Example]

Show SLA operation 2 configuration

Raisecom(config)#**show sla 2 configuration**

Show all SLA operation configuration

Raisecom(config)#**show sla all configuration**

[Executing Command notice]

None

[Related commands]

Command	Description
sla <i>oper-num</i> cfm-echo <i>mac-address</i> level <i>level-id</i> vlan <i>vlan-id</i> [cos <i>cos-id</i>]	sla cfm-echo operation basic configuration
sla <i>oper-num</i> cfm-jitter <i>mac-address</i> level <i>level-id</i> vlan <i>vlan-id</i> [interval <i>interval-time</i>] [packets <i>packets-num</i>] [cos <i>cos-id</i>]	sla cfm-jitter operation basic configuration
sla <i>oper-num</i> icmp-echo <i>ip-address</i>	sla icmp-echo operation basic configuration
sla <i>oper-num</i> icmp-jitter <i>ip-address</i> [interval <i>interval-time</i>] [packets <i>packets-nums</i>]	sla icmp-jitter operation basic configuration
sla schedule <i>oper-num</i> [life { forever <i>life-time</i> }] [period <i>period-time</i>]	Configure SLA schedule information, enable SLA operation schedule

36.2 show sla result

[Function]

Show the operation latest test information

[Command Format]

Show sla {all | *oper-num*} result

[Parameter]

Oper-num SLA operation number, range is 1-65535

all show all the SLA operation configuration

[Default]

By default the latest SLA operation test information will not be shown

[Command Modes]

Privileged EXEC mode; privileged user

[Executing Command Instruction]

Only user with priority level 10 can use the command

[Explanation of command execution echo]

Operation XX does not exist

Operation <I>: Success/Failure

<i>Info of Latest Test</i>	<i>TWO-WAY</i>	<i>ONE-WAY(SD)</i>
<i>ONE-WAY(DS)</i>		

<i>Delay (msec)</i>
...		

Operation <I>:

Schedule Status: *(active\complete\intial)*

Number of Send Test: *XX*

Number of Successful Test: *XX*

Percent of Drop Pkts: *XX.XXX%*

<i>Info of Latest Test</i>	<i>TWO-WAY</i>	<i>ONE-WAY(SD)</i>	<i>ONE-WAY(DS)</i>
----------------------------	----------------	--------------------	--------------------

<i>Delay Min(msec)</i>
<i>Delay Max(msec)</i>
<i>Delay Sum(msec)</i>
<i>Delay Sum2(msec)</i>
<i>Jitter Sum(msec)</i>			

The total number of active operations is XX!

Operation <1>:

Type: echo/jitter

[Example]

Show SLA operation 2 latest operation test information

Raisecom(config)#**show sla 2 result**

Show all SLA operation latest operation test information

Raisecom(config)#**show sla all result**

[Executing Command notice]

None

[Related commands]

Command	Description
sla oper-num cfm-echo mac-address level <i>level-id</i> vlan <i>vlan-id</i> [cos <i>cos-id</i>]	sla cfm-echo operation basic configuration
sla oper-num cfm-jitter mac-address level <i>level-id</i> vlan <i>vlan-id</i> [interval <i>interval-time</i>] [packets <i>packets-num</i>] [cos <i>cos-id</i>]	sla cfm-jitter operation basic configuration
sla oper-num icmp-echo ip-address	sla icmp-echo operation basic configuration
sla oper-num icmp-jitter ip-address [interval <i>interval-time</i>] [packets <i>packets-nums</i>]	sla icmp-jitter operation basic confiuration
sla schedule oper-num [life {forever <i>life-time</i> }] [period <i>period-time</i>]	Configure SLA schedule information, enable SLA operation schedule

36.3 sla cfm-echo configuration

[Function]

Configure SLA cfm-echo operation basic information

[Command Format]

Sla *oper-num* **cfm-echo** *mac-address* **level** *level-address* **level**
level-id **vlan** *vlan-id* [**cos** *cos-id*]

[Parameter]

Oper-num SLA operation number, range is 1-65535

Mac-address destination MAC address, format is *HHHH.HHHH.HHHH*

Level-id MD domain level, range is 0-7

Vlan-id VLAN ID, range is 1-4094

Cos-id service level, range is 0-7, default value is 0

[Default]

By default there is no SLA operation basic configuration

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Only user with priority level 15 can use the command

[Explanation of command execution echo]

Set successfully

Set unsuccessfully. Operation XX has been set! Please delete the operation XX first!

Set unsuccessfully. The total amount of operations which can be configured cannot exceed 100!

[Example]

Configure CFM-echo operation, operation number is 2, destination MAC address is 000e.5e03.45d0, maintaining domain level is 3, VLAN ID is 4, service level is 1

```
Raisecom(config)# sla 2 cfm-echo dest-mac 000e.5e03.45d0 level 3  
vlan 4 cos 1
```

Delete SLA operation basic configuration:

Raisecom(config)#**no sla 2**

[Related commands]

Commands	Description
Show sla {all <i>oper-num</i> } configuration	Show operation related configuration

36.4 sla cfm-jitter configuration

[Function]

Configure SLA cfm-jitter operation basic information

[Command Format]

Sla *oper-num* **cfm-jitter** *mac-address* **level** *level-id* **vlan** *vlan-id*
[interval *interval-time***] [packets** *packets-num***] [cos** *cos-id***]**

[Parameter]

Oper-num SLA operation number, range is 1-65535

Mac-address destination MAC address, format is *HHHH.HHHH.HHHH*

Level-id MD domain level, range is 0-7

Vlan-id VLAN ID, range is 1-4094

Interval-time detection interval, range is 1- 6000ms, default value is 20ms

Packes-num detection message number, range is 1-100, default value is 10

Cos-id service level, range is 0-7, default value is 0

[Default]

By default there is no SLA operation basic configuration

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Only user with priority level 15 can use the command

[Explanation of command execution echo]

Set successfully

Set unsuccessfully. MAC Address is illegal! Please check the input MAC address first!

Set unsuccessfully. Operation XX has been set! Please delete the operation XX first!

Set unsuccessfully. The total amount of operations which can be configured cannot exceed 100!

[Example]

Configure CFM-echo operation, operation number is 2, destination MAC address is 000e.5e03.45d0, maintaining domain level is 3, VLAN ID is 4, detection interval is 10ms, detection message number is 10, service level is 1

```
Raisecom(config)# sla 2 cfm-jitter dest-mac 000e.5e03.45d0 level 3  
vlan 4 interval 10 packets 5 cos 1
```

Delete SLA operation basic configuration:

```
Raisecom(config)#no sla 2
```

[Related commands]

Commands	Description
Show sla {all <i>oper-num</i> } configuration	Show operation related configuration

36.5 sla icmp-echo configuration

[Function]

Configure ICMP-echo operation basic information

[Command Format]

Sla *oper-num* icmp-echo *ip-address*

[Parameter]

Oper-num SLA operation number, range is 1-65535

Ip-address destination IP address, format is:XXX.XXX.XXX.XXX

[Default]

By default there is no SLA operation basic configuration

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Only user with priority level 15 can use the command

[Explanation of command execution echo]

Set successfully

Set unsuccessfully. MAC Address is illegal! Please check the input MAC address first!

Set unsuccessfully. Operation XX has been set! Please delete the operation XX first!

Set unsuccessfully. The total amount of operations which can be configured cannot exceed 100!

[Example]

Configure ICMP-echo operation, operation number is 2, destination IP address is 20.0.0.20

Raisecom(config)#**sla 2 icmp-echo dest-ipaddr 20.0.0.20**

Delete SLA operation basic configuration

Raisecom(config)#**no sla 2**

[Related commands]

Commands	Description
Show sla {all <i>oper-num</i> } configuration	Show operation related configuration

36.6 sla icmp-jitter configuration

[Function]

Configure ICMP-jitter operation basic information

[Command Format]

Sla *oper-num icmp-jitter ip-address*

[Parameter]

Oper-num SLA operation number, range is 1-65535

Ip-address destination IP address, format is:XXX.XXX.XXX.XXX

Interval-time detection interval, range is 1-60000ms, default value is 20ms

Packet-num detection message number, range is 1-100, default value is 10

[Default]

By default there is no SLA operation basic configuration

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Only user with priority level 15 can use the command

[Explanation of command execution echo]

Set successfully

Set unsuccessfully. MAC Address is illegal! Please check the input MAC address first!

Set unsuccessfully. Operation XX has been set! Please delete the operation XX first!

Set unsuccessfully. The total amount of operations which can be configured cannot exceed 100!

[Example]

Configure ICMP-jitter operation, operation number is 2, destination IP address is 20.0.0.20, detection interval is 10ms, detection message number is 10

Raisecom(config)#**sla 2 icmp-jitter dest-ipaddr 20.0.0.20 interval 10**

packets 5

Delete SLA operation basic configuration

Raisecom(config)#**no sla 2**

[Related commands]

Commands	Description
Show sla {all oper-num} configuration	Show operation related configuration

36.7 sla schedule

[Function]

Configure SLA operation; configure schedule and detection period according to operation number

[Command Format]

Sla schedule *oper-num* [**life**{**forever** | *life-time*}] [**period** *period-time*]
ip-address

[Parameter]

Oper-num SLA operation number, range is 1-65535

Forever always in schedule state

Life--time schedule period, range is forever or 1-604800s, default value is forever

Period-time detection period, range is 1-604800s, by default it is 20s

[Default]

By default SLA operation schedule is disabled.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

Only user with priority level 15 can use the command

[Explanation of command execution echo]

Set successfully

*Set unsuccessfully, period = XX < YY = PP*II + timeout(5);*

*The configuration must meet: Period > packets*interval + timeout(5)!*

Set unsuccessfully. Operation XX has been set! Please delete the operation XX first!

Set unsuccessfully. The total amount of operations which can be configured cannot exceed 100!

[Example]

Configure SLA operation 2 schedule information, schedule period is 20s, test interval is 10s, enable schedule

Raisecom(config)#**sla schedule 2 life 20 period 10**

Delete SLA operation basic configuration

Raisecom(config)#**no sla schedule all**

[Executing Command notice]

1. before schedule, you need to make sure that the SLA operation of the same operation number has been configured
2. several operation can be configured at the same time, the maximum operation number is 10
3. only when one schedule has been ended up can another one start

[Related commands]

Commands	Description
Show sla {all <i>oper-num</i> } configuration	Show operation related configuration

Chapter 37 Physical Interface Commands

37.1 show cable-diagnostics

[Function]

Show line diagnostics information

[Command Format]

Show cable-diagnostics port-list *port-list*

Show cable-diagnostics line *port-list*

Show cable-diagnostics client *port-list*

[Parameter]

Port-list physical interface list

Line-list line port list

Client-list client port number

[Default]

None

[Command Modes]

Privileged user

[Executing Command Instruction]

Use the command show device virtual line detection result

[Explanation of command execution echo]

<port-id> <value> <time> <status> <value> <status> <value>

(E)

Port Attribute Time RX Stat RX Len(m) TX Stat TX Len(m)

<port-id> <value> <time> <status> <value> <status> <value>

[Example]

Raisecom# **show cable-diagnostics port-list 1**

[Related commands]

Commands	Description
Test cable-diagnostics	Execute line diagnostics

37.2 test cable-diagnostics

[Function]

Remote device virtual line detection.

[Command Format]

Test cable-diagnostics port-list *line-list*

Test cable-diagnostics line *line-list*

Test cable-diagnostics client *client-list*

[Parameter]

Port-list physical interface list

Line-list line port list

Client-list client port number

[Default]

None

[Command Modes]

Privileged user

[Executing Command Instruction]

Use the command execute virtual line detection based on port

[Explanation of command execution echo]

Set successfully

Test on port port-id will affect link state and traffic

Test will take a few seconds to run on these ports.

Use 'show cable-diagnostics' to read the test results.

Test is running on port port-id ! Please wait for few seconds to test again.

Port port-id dose not support cable diagnosis !

[Example]

Raisecom# **test cable-diagnostics port-list 1**

[Related commands]

Commands	Description
Show cable-diagnostics port-list <i>port-list</i>	Show line diagnostics information



Chapter 38 NTP Configuration

Commands

38.1 debug ntp

[Function]

Enable NTP debug function.

[Command format]

[no] debug ntp {*adjustment* / *packet* / *synchronization* / *error* / *all*}

[Parameter]

adjustment: clock adjustment debugging information;

packet: packet debugging information;

synchronization: synchronization status;

error: error debugging information;

all: all debugging information.

[Default]

Disable NTP debug function

[Command Modes]

Privileged EXEC mode, Privileged user

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

[Example]

Raisecom# **debug ntp all**

[Related commands]

Commands	Description
[no] ntp refclock <i>[A.B.C.D]</i> [<i>stratum</i>]	Setting device as NTP reference clock or delete NTP reference clock device.
[no] ntp peer <i>ip-address</i> [version (<i>v1/v2/v3</i>)]	Configure/delete NTP peer.
[no] ntp server <i>ip-address</i> [version (<i>v1/v2/v3</i>)]	Configure/delete NTP server.
show ntp associations [detail]	Show NTP connection information.
show ntp status	Show device NTP status.

38.2 ntp peer

[Function]

Configure NTP peer address in global configuration mode.

[Command format]

[no] ntp peer *ip-address* [**version** *v1/ v2/ v3*]

[Parameter]

ip-address: IP address of server;

version: version.

[Default]

If users operate this command without configuring version and NTP peer IP for RC551, the version is 3 by default.

[Command Modes]

Port configuration mode, Privileged user

[Executing Command Instruction]

If haven't configure device as NTP reference clock source, configuration of NTP peer conforms to RFC1166 criterion will be successful. The device takes NTP peer as its peer and configuring NTP peer will fail if the device is reference clock source.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

Set unsuccessfully, device is the reference clock.

[Example]

Setting NTP peer in global configuration mode:

Raisecom(config)# **ntp peer 10.0.0.169 version v3**

Deleting NTP peer in global configuration mode:

Raisecom(config)# **no ntp peer 10.0.0.169**

[Related commands]

Commands	Description
[no] ntp refclock A.B.C.D [stratum]	Setting NTP reference clock device or deleting device.
show ntp associations [detail]	Show NTP connection information.
show ntp status	Show device NTP status.

38.3 ntp refclock-master

[Function]

Set device as NTP reference clock source in global configuration mode.

[Command format]

[no] ntp refclock-master [A.B.C.D] [stratum]

[Parameter]

A.B.C.D: reference clock source identifier;

stratum: system stratum level.

[Default]

Native clock source is not NTP reference clock source by default. By configuring this command, the reference clock is 127.127.1.0 and stratum is 8 by default.

[Command Modes]

Global configuration mode; privileged user

[Executing Command Instruction]

In global configuration mode, if users haven't configured server or peer, and the reference clock source is configured correctly, this command will be executed successfully; and this command will fail to execute if have been configured server or peer.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

Se unsuccessfully. please delete the peer or server.

[Example]

Set reference clock 127.127.1.1 and stratum 7 for device:

Raisecom(config)# **ntp refclock-master 127.127.1.0 7**

[Related commands]

Commands	Description
[no] ntp peer ip-address [version (v1/v2/v3)]	Configure/delete NTP peer.
[no] ntp server ip-address [version (v1/v2/v3)]	Configure/delete NTP server.
show ntp associations [detail]	Show NTP connection information.
show ntp status	Show device NTP status.

38.4 ntp server

[Function]

Configure NTP server address in global configuration mode.

[Command format]

[no] ntp server *ip-address* [**version** *v1* / *v2* / *v3*]

[Parameters]

ip-address: server IP;

version: version.

[Default]

If users operate this command without configuring version and NTP server IP for media converter, the version is 3 by default.

[Command Modes]

Global configuration mode, Privileged user

[Executing Command Instruction]

If haven't configure device as NTP reference clock source, configuration of NTP server conforms to RFC1166 criterion will be successful. The device takes NTP server as its server and configuring NTP server will fail if the device is reference clock source.

[Explanation of command execution echo]

Set successfully.

Set unsuccessfully.

Set unsuccessfully, device is the reference clock.

[Example]

Setting NTP server in global configuration mode:

Raisecom(config)# **ntp server** *10.0.0.169* **version** *v3*

Deleting NTP server in global configuration mode:

Raisecom(config)# **no ntp server** 10.0.0.169

[Related commands]

Commands	Description
[no] ntp refclock A.B.C.D [STATUS]	Setting NTP reference clock device or deleting device.
show ntp associations [detail]	Show NTP connection information.
show ntp status	Show device NTP status.

38.5 show ntp associations

[Function]

Show NTP connection information.

[Command format]

show ntp associations [detail]

[Command Modes]

Privileged EXEC mode, Privileged user

[Explanation of command execution echo]

Show connection information:

```
Server(ip)    refid    stratum  poll  when    delay    offset    dispersion
mode reach
```

```
(s)20.6.6.9  127.127.1.0    4      9    58927    -1.065525    0.005769    0.000000
1 255
```

```
Peer(ip)      refid      stratum  poll  when    delay    offset    dispersion
mode reach
```

```
(u)20.6.6.8    0.0.0.0        16      10    58522     0.000000     0.000000
16.000000    0 0
```

Show detailed connection information:

```

Server(ip)    refid    stratum  poll  when    delay    offset
dispersion    mode  reach

(s)20.6.6.9   127.127.1.0    4      9    59216   -1.065525   0.005769
0.000000      1    255

filtoffset = 0.000741  0.001415  0.002088  0.002758  0.003422  0.003780
0.004427  0.005769

filtdelay = -1.065526  -1.065525  -1.065525  -1.065526  -1.065525
-1.065525  -1.065525  -1.065525

filtdispersion= 16.000000  16.000000  16.000000  16.000000  16.000000
16.000000  16.000000  0.000000

Peer(ip)    refid    stratum  poll  when    delay    offset
dispersion    mode  reach

(u)20.6.6.8   0.0.0.0      16      10    58811   0.000000   0.000000
16.000000      0    0

filtoffset = 0.000000  0.000000  0.000000  0.000000  0.000000  0.000000
0.000000  0.000000

filtdelay = 0.000000  0.000000  0.000000  0.000000  0.000000
0.000000  0.000000  0.000000

filtdispersion =16.000000  16.000000  16.000000  16.000000  16.000000
16.000000  16.000000  16.000000

```

[Example]

Raisecom#**show ntp associations**

[Related commands]

Commands	Description
[no] ntp refclock <i>[A.B.C.D]</i> <i>[stratum]</i>	Setting device as NTP reference clock or delete NTP reference clock device.
[no] ntp peer <i>ip-address</i> [version (<i>v1/v2/v3</i>)]	Configure/delete NTP peer.
[no] ntp server <i>ip-address</i> [version (<i>v1/v2/v3</i>)]	Configure/delete NTP server.

38.6 show ntp status

[Function]

Show NTP status information.

[Command format]

show ntp status

[Command Modes]

Privileged EXEC mode, Privileged user

[Explanation of command execution echo]

Show NTP status information:

```
Clock status :      synchronized
NTP peer :          20.6.6.9
NTP version :       3
NTP mode :          ntpSlave
Leap :              0
Poll :              8
Stratum :           5
Precision :         2**4
Reference clock :    20.6.6.9
Reference time :     cd6c8915.0c0d3480(Thu Mar 19 09:04:21.047 UTC 2009)
Current clock :      cd6d6ee4.0c0d3480(Fri Mar 20 01:24:52.047 UTC 2009)
Root delay :         -1.000009
Root dispersion :    0.001380
```

[Example]

Raisecom#**show ntp status**

[Related commands]

Commands	Description
[no] ntp refclock [A.B.C.D] [stratum]	Setting device as NTP reference clock or delete NTP reference clock device.

[no] ntp peer ip-address [version (v1/v2/v3)]	Configure/delete NTP peer.
[no] ntp server ip-address [version (v1/v2/v3)]	Configure/delete NTP server.

Chapter 39 Telnet Commands

39.1 show telnet-server

[Function]

Show **telnet server** configuration

[Command format]

Show telnet-server

[Parameter]

None

[Command Modes]

Privileged EXEC mode; privileged user

[Executing Command Instruction]

Use show telnet-server to show current telnet server configuration

[Example]

Raisecom#**show telnet-server**

Max session: 5

Accept port-list: 1-26

[Related commands]

Commands	Description
telnet-server accept port-list { <i>all</i> <i>portList</i> }	Set telnet ports on the switch.
telnet-server max-session <i>max-session-num</i>	Set maximal telnet connected number on the switch.
telnet-server close terminal-telnet <i>terminal-number</i>	Disable telnet connects to the switch.
telnet <i>ip-address</i> [port <i>port-number</i>]	telnet other switch or PC

39.2 telnet

[Function]

telnet to remote device

[Command format]

telnet *ip-address* [**port** *port-number*]

[Parameter]

ip-address: ip address for remote device;

port-number: telnet port number.

[Command Modes]

Privileged EXEC; user diagnostic mode (for RC5xx series)

[Executing Command Instruction]

Only privileged users with priority higher than or equal 5 can use this command. Configure gateway first when the telnet switch is not in the same network segment with this switch.

[Explanation of command execution echo]

Connect failed!

Connection to host lost

[Example]

Logon telnet IP 10.1.2.3, the device provide telnet server port 555:

raisecom#**telnet 10.1.2.3 port 555**

[Related commands]

Commands	Description
telnet-server accept port-list { <i>all</i> <i>portList</i> }	Set telnet ports on the switch.
telnet-server max-session	Set maximal telnet connected number

<i>max-session-num</i>	on the switch.
telnet-server close terminal-telnet <i>terminal-number</i>	Disable telnet connects to the switch.
show telnet-server	Show telnet server configuration.

39.3 telnet-server

[Function]

Configure telnet connection

[Command format]

telnet-server {close terminal-telnet *terminal-number* / max-session *max-session-num* / accept port-list *portlist*}

[Parameter]

Terminal-number the connected terminal number

Max-seesion-num maximum connection number

Portlist port list

[Default]

At most 5 telnet connection

[Command Modes]

Global configuration mode

[Executing Command Instruction]

telnet-server close terminal-telnet *terminal-number* close a certain end telnet connection

telnet-server max-session *max-session-num* set telnet connection maximum number

telnet-server accept port-list {all | *portlist*} (ISCOM20/21/28/29/30/22 serious devices)

telnet-server accept {line *portlist* | client *portlist*} (5x1 serious devices) configure the port so that it can be telnet

[Explanation of command execution echo]

Connect failed!

Connection to host lost

[Example]

Close terminal 1 telnet connection

Raisecom#**telnet-server close terminal-telnet 1**

[Related commands]

Commands	Description
telnet-server accept port-list { <i>all</i> <i>portList</i> }	Set telnet ports on the switch.
telnet-server max-session <i>max-session-num</i>	Set maximal telnet connected number on the switch.
telnet-server close terminal-telnet <i>terminal-number</i>	Disable telnet connects to the switch.
show telnet-server	Show telnet server configuration.

Chapter 40 PPPoE Commands

40.1 pppoeagent

[Function]

To start or shutdown PPPoE function of specified port

[Command Format]

pppoeagent {enable | disable}

[Parameter]

enable To start PPPoE function of specified port

disable To shutdown PPPoE function of specified port

[Default]

PPPoE function on the port is shutdown by default

[Command Modes]

port / batch mode, privileged user (permissions 15)

[Executing Command Instruction]

The command. is used to to configure attach string of Circuit ID by default
command can be configure the state of the switch of PPPoE + function on
the specified port. When one port configure pppoeagent trust port, enable
PPPoE + function.

[Explanation of command execution echo]

Set successfully

Set ports portlist unsuccessfully

[Example]

To enter global configuration mode

Raisecom#**config**

To enter port / batch mode

Raisecom(config)#**interface range 1-5**

To start corresponding port PPPoE + function

Raisecom(config-range)#**pppoeagent enable**

Set successfully

Raisecom(config-range)#

[Related commands]

Commands	Description
show pppoeagent	To display PPPoE + configurable information

40.2 pppoeagent circuit-id

[Function]

To configure port Circuit ID for user defined string

[Command Format]

pppoeagent circuit-id *INFO*

[Parameter]

content of *INFO* Circuit ID (not more than the length of 63 character string)

[Default]

Port Circuit ID is the default format: vlan ID\ portID\ additional string.

[Command Modes]

privileged user on port mode (permissions 15)

[Executing Command Instruction]

The command. Is used to To configure port Circuit ID for user defined string

[Explanation of command execution echo]

Set successfully

Circuit-ID must not longer than 63 bytes

[Example]

To enter global configuration mode

```
Raisecom#config
```

To enter port mode

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

To configure port Circuit ID (If Circuit ID contains spaces, you need to include them in double quotes)

```
Raisecom(config-port)#pppoeagent circuit-id hello
```

Set successfully

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

[Related commands]

Commands	Description
show pppoeagent	To display PPPoE + configurable information
no pppoeagent circuit-id	To restore port Circuit ID by default

40.3 pppoeagent circuit-id attach-string

[Function]

To configure attach string of switch Circuit ID as user defined string

[Command Format]

pppoeagent circuit-id attach-string *STRING*

[Parameter]

The attach string of ***STRING*** Circuit ID(no more than 55 bytes)

[Default]

The attach string of Circuit ID is the hostname of the switch by default

[Command Modes]

privileged user on port mode (permissions 15)

[Executing Command Instruction]

The command. is used to to configure attach string of Circuit ID by default

[Explanation of command execution echo]

Set successfully

Attach string must not longer than 55 bytes

[Example]

To enter global configuration mode

Raisecom#**config**

Raisecom(config)# **pppoeagent circuit-id attach-string hello**

Set successfully

Raisecom(config)#

[Related commands]

Commands	Description
show pppoeagent	To display PPPoE + configurable information
no pppoeagent circuit-id attach-string	To restoreattach-string of Circuit ID by default

40.4 pppoeagent remote-id

[Function]

To configure Remote ID of specified port

[Command Format]

pppoeagent remote-id {switch-mac | client-mac}

[Parameter]

switch-mac To use MAC address of switch as Remote ID

client-mac To use MAC address of client end as Remote ID

[Default]

To use MAC address of switch as Remote ID by default

[Command Modes]

port / batch mode, privileged user (permissions 15)

[Executing Command Instruction]

The command. is used to to configure Remote ID of the specified port

[Explanation of command execution echo]

Set successfully

[Example]

To enter global configuration mode

```
Raisecom#config
```

To enter port mode

```
Raisecom(config)#interface range 1-5
```

```
Raisecom(config-range)#pppoeagent remote-id client-mac
```

Set successfully

```
Raisecom(config-range)#
```

[Related commands]

Commands	Description
show pppoeagent	To display PPPoE + configurable information

40.5 pppoeagent remote-id format

[Function]

To configure formatting approach of the Remote ID on specified port

[Command Format]

```
pppoeagent remote-id format {binary | ascii}
```

[Parameter]

binary: To format Remote ID with binary

ascii: To format Remote ID with ASCII

[Default]

Formatting approach of the Remote ID is binary by default

[Command Modes]

port / batch mode, privileged user (permissions 15)

[Executing Command Instruction]

The command. is used to to configure formatting approach of the Remote ID

[Explanation of command execution echo]

Set successfully

[Example]

To enter global configuration mode

Raisecom#**config**

To enter port / batch mode

Raisecom(config)#**interface range 1-5**

To start corresponding port PPPoE + function

Raisecom(config-range)#**pppoeagent remote-id format ascii**

Set successfully

Raisecom(config-range)#

[Related commands]

Commands	Description
show pppoeagent	To display PPPoE + configurable information

40.6 pppoeagent trust

[Function]

To configure port as trust port

[Command Format]

pppoeagent trust

[Default]

The port is non-trust.port by default

[Command Modes]

port / batch mode, privileged user (permissions 15)

[Executing Command Instruction]

The command. is used to to configure specified port as trust port. no pppoeagent trust command is used to to configure no-trust port. PPPoE + enable, it can not be configured to trust port.

[Explanation of command execution echo]

Set successfully

Set ports portlist unsuccessfully

[Example]

To enter global configuration mode

```
Raisecom#config
```

To enter port mode

```
Raisecom(config)#interface range 1-5
```

```
Raisecom(config-range)# pppoeagent trust
```

Set successfully

```
Raisecom(config-range)#
```

[Related commands]

Commands	Description
show pppoeagent	To display PPPoE + configurable information

40.7 pppoeagent vendor-specific-tag overwrite

[Function]

To start /shutdown PPOE + TAG cover features of specified port

[Command Format]

pppoeagent vendor-specific-tag overwrite {enable | disable}

[Parameter]

enable To start PPoE + TAG cover features of specified port

disable To shutdown PPoE + TAG cover features of specified port

[Default]

PPoE + TAG cover features on port is off

by default

[Command Modes]

port / batch mode, privileged user (permissions 15)

[Executing Command Instruction]

The command. is used to to configure the switch state.of PPPoE + TAG cover features on the specified port

[Explanation of command execution echo]

Set successfully

[Example]

To enter global configuration mode

Raisecom#**config**

To enter port mode

Raisecom(config)#**interface range 1-5**

Raisecom(config-range)#**pppoeagent vendor-specific-tag
overwrite enable**

Set successfully

Raisecom(config-range)#

[Related commands]

Commands	Description
show pppoeagent	To display PPoE + configurable information

40.8 show pppoeagent

[Function]

To display PPPoE + configurable information

[Command Format]

show pppoeagent [**port-list** *portlist*]

show pppoeagent line *linelist* [**client** *clientlist*]

show pppoeagent client *clientlist*

[Parameter]

portlist list of port

linelist list of line end

clientlist list of client

[Command Modes]

Other mode except **view**, privileged user (permissions 15)

[Executing Command Instruction]

The command. is used to to view: attatch stringconfiguration, port state enabled, PPPoE + TAG cover enabled, Remote ID, formatting approach of Remote ID and content of Circuit ID

[Explanation of command execution echo]

See [Example]

[Example]

User need to view relative PPPoE+ information on port 1-5

Raisecom#**show pppoeagent port-list 1-5**

Attatch string: %defaulted format %

*port port enabled cover enabled Remote-ID formatting approaching
Circuit-ID*

```
-----  
1    disable    enable    client-mac  ASCII  %defaulted format %  
2    disable    enable    client-mac  ASCII  %defaulted format %  
3    disable    enable    client-mac  ASCII  %defaulted format %  
4    disable    enable    client-mac  ASCII  %defaulted format %  
5    disable    enable    client-mac  ASCII  %defaulted format %*
```

*defaulted format of Circuit-ID:port ID \VLANID \attach string

**defaulted string is HOST NAME

40.9 show pppoeagent statistic

[Function]

To display PPPoE + statistical information

[Command Format]

show pppoeagent statistic [**port-list** *portlist*]

show pppoeagent statistic line *linelist* [**client** *clientlist*]

show pppoeagent statistic client *clientlist*

[Parameter]

portlist

linelist

clientlist [Default]

[Command Modes]

Other mode except **view**, privileged user (permissions 15)

[Executing Command Instruction]

The command. Is used to view following information: numbers of received PADI message, numbers of successful-Send PADI Message, numbers of received PADR message, and numbers of successful-Send PADI Message

[Explanation of command execution echo]

See [Example]

[Example]

User need to view statistic on port 1-5

Raisecom#**show pppoeagent statistic port-list 1-5**

<i>port</i>	<i>receiced PADI</i>	<i>sent PADI</i>	<i>received PADR</i>	<i>sent PADR</i>
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0

[Related commands]

Commands	Description
clear pppoeagent statistic	To clear PPPoE+ statistic

Chapter 41 Y.1731 Commands

41.1 clear ethernet cfm errors

[Function]

Clear information of cfm errors database

[Command Format]

clear ethernet cfm errors [**level** *level*]

[Parameters]

level: level of domain, range in 0-7.

[Command Mode]

Global configuration mode

[Explanation of Command Executing Echo]

Set successfully

[Example]

Clear information of errors database with MD level 3:

Raisecom(config)# **clear ethernet cfm errors level 3**

[Related Commands]

Commands	Description
show ethernet cfm errors	Show information of errors database.

41.2 clear ethernet cfm remote

[Function]

Clear remote MEP

[Command Format]

clear ethernet cfm remote-mep [**level** *level* [**service** *CSIID* [**mpid** *mepid*]]]

[Parameters]

level: level of domain, range in 0-7;

CSIID: name of service instance;

mepid: MEP ID, range in 1-8191.

[Command Mode]

Global configuration mode

[Explanation of Command Executing Echo]

Set successfully

[Example]

Clear MD level 3, service instance ma3-1-4, remote MEPid 4:

Raisecom(config)# **clear ethernet cfm remote-mep level 3 service ma3-1-4 mpid 4**

[Related Commands]

Commands	Description
show ethernet cfm mep	Show MEP under service instance.
show ethernet cfm remote-mep	Show remote MEP.

41.3 clear ethernet cfm traceroute cache

[Function]

Clear traceroute cache database

[Command Format]

clear ethernet cfm traceroute-cache

[Command Mode]

Global configuration mode

[Explanation of Command Executing Echo]

Set successfully

[Example]

Clear linktrace database:

Raisecom(config)# **clear ethernet cfm traceroute-cache**

[Related Commands]

Commands			Description
show	ethernet	cfm	Show traceroute cache.
traceroute-cache			

41.4 clear performance-monitor statistics

[Function]

Configure history statistic information of performance monitor pair.

[Command Format]

clear ethernet cfm performance-monitor {all | frame-loss-ratio | delay | delay-variation}

[Parameters]

all: clear all information, including frame loss ratio, frame delay and delay variation;

frame-loss-ratio: clear frame loss ratio;

delay: clear frame delay;

delay-variation: clear frame delay variation.

[Command Mode]

Service instance mode

[Explanation of Command Executing Echo]

Set successfully

[Example]

Clear frame delay information of performance monitor in service instance ma3-1-4:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **clear ethernet cfm performance-monitor delay**

[Related Commands]

Commands	Description
show ethernet cfm performance-monitor	Show configuration information of performance monitor.

41.5 ethernet cfm

[Function]

Set the global y.1731 function switch.

[Command Format]

ethernet cfm {*enable / disable*}

[Parameter]

enable: enable global y.1731 function switch;

disable: disable global y.1731 function switch;

[Default]

disable

[Command Modes]

Global configuration mode

[Executing Command Instruction]

Enable this function

[Explanation of command execution echo]

Set successfully

[Example]

Enable global y.1731 function switch:

Raisecom(config)# **ethernet cfm enable**

Disable global y.1731 function switch:

Raisecom(config)# **ethernet cfm disable**

[Related commands]

Commands	Description
show ethernet cfm	Show current configuration information.

41.6 ethernet cfm domain

[Function]

Create domain

[Command Format]

ethernet cfm domain [md-name *DOMAIN-NAME*] level *level*

no ethernet cfm domain level *level*

[Parameter]

DOMAIN-NAME: name of domain, 1-16 character;

level: level of domain, 8 levels in all: level 0-7.

[Command Mode]

Global configuration mode

[Executing Command Instruction]

The function cfm asks for confirming a domain and level of the domain at first, that is to say, to confirm network range for connection fault detection.

[Explanation of command execution echo]

Set successfully.

Creating cfm domain successfully.

Set unsuccessfully. The length of Maintenance Domain name can't be longer than 16.

Creating cfm domain unsuccessfully for the input MD name is more than

16 characters.

Set unsuccessfully. There has been a MD at level level-id.

Creating cfm domain unsuccessfully for the MD level has existed already.

Set unsuccessfully. There has been this domain name.

Creating cfm domain unsuccessfully for the MD name has existed already.

[Example]

Creating domain named as md3-1, and level at level 3:

Raisecom(config)# **ethernet cfm domain md3-1 level 3**

Creating domain level at level 4 and without domain name:

Raisecom(config)# **ethernet cfm level 4**

[Related commands]

Commands	Description
show ethernet cfm domain	Show current maintain domain and configuration information of service application.

41.7 ethernet cfm errors archive-hold-time

[Function]

Configure holding time for error ccm database.

[Command Format]

ethernet cfm errors archive-hold-time minutes

no ethernet cfm errors archive-hold-time

[Parameter]

minutes: holding time for errors, range in 1-65535, unit: minute

[Default]

100

[Command Modes]

Global configuration mode

[Executing Command Instruction]

This command can set error items holding time in error CCM database.

[Explanation of command execution echo]

Set successfully

[Example]

Configure error CCM database holding time for error items to be 180:

Raisecom(config)# **ethernet cfm errors archive-hold-time 180**

Restore error CCM database holding time for error items to default:

Raisecom(config)# **no ethernet cfm errors archive-hold-time**

[Related commands]

Commands	Description
show ethernet cfm errors	Show error CCM database information.

41.8 ethernet cfm mip level

[Function]

Configure static remote MEP

[Command Format]

ethernet cfm mip level *level*

no ethernet cfm mip level *level*

[Parameters]

level: configure domain level for MIP, range in 0-7.

[Command Mode]

Interface configuration mode

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. The MD with Level level-id isn't configured.

[Example]

Configure MEP with MP ID 1 under service instance ma3-1-4 at port 2:

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

Raisecom(config-port)#**ethernet cfm mip level 5**

[Related Commands]

Commands	Description
show ethernet cfm local-mp	Show local MP configuration information.

41.9 ethernet cfm port

[Function]

Configure port y.1731 function switch.

[Command Format]

ethernet cfm {enable / disable}

[Parameter]

enable: enable port y.1731 function switch;

disable: disable port y.1731 function switch;

[Default]

disable

[Command Modes]

Interface configuration mode; Interface port batch configuration mode

[Executing Command Instruction]

Enable the function

[Explanation of command execution echo]

Set successfully

[Example]

Enable port y.1731 function switch:

Raisecom(config-port)# **ethernet cfm enable**

Disable port y.1731 function switch:

Raisecom(config-port)# **ethernet cfm disable**

[Related commands]

Commands	Description
show ethernet cfm	Show current configuration information.

41.10 ethernet cfm remote mep age-time

[Function]

Configure aging time of remote MEP

[Command Format]

ethernet cfm remote mep age-time *minutes*

[Parameters]

minutes: aging time, range in 1-65535, unite: minute

[Default]

100

[Command Mode]

Global configuration mode

[Explanation of Command Executing Echo]

Set successfully

[Example]

Configure aging time of remote MEP to be 10 minutes:

Raisecom(config)# **ethernet cfm remote mep age-time 10**

[Related Commands]

Commands	Description
show ethernet cfm	Show current configuration information.

41.11 ethernet cfm traceroute cache

[Function]

Configure database switch of traceroute cache

[Command Format]

ethernet cfm traceroute cache {enable | disable}

[Parameters]

enable: LinkTrace database function enable;

disable: LinkTrace database function disable.

[Default]

disable

[Command Mode]

Global configuration mode

[Explanation of Command Executing Echo]

Set successfully

[Example]

Enable LinkTrace database function:

Raisecom(config)# **ethernet cfm traceroute cache enable**

[Related Commands]

Commands	Description
show ethernet cfm traceroute-cache	Show traceroute cache.

41.12 ethernet cfm traceroute cache hold-time

[Function]

Configure holding time of traceroute cache database item

[Command Format]

ethernet cfm traceroute cache hold-time *minutes*
no ethernet cfm traceroute cache hold-time

[Parameters]

minutes: LinkTrace database items holding time, range in 1-65535.

[Default]

100 minutes

[Command Mode]

Global configuration mode

[Explanation of Command Executing Echo]

Set successfully

[Example]

Configure holding time of LinkTrace database items to be 500 minutes:

Raisecom(config)# **ethernet cfm traceroute cache hold-time 500**

[Related Commands]

Commands			Description
show	ethernet	cfm	Show traceroute cache.
traceroute-cache			

41.13 ethernet cfm traceroute cache size

[Function]

Configure traceroute cache database item

[Command Format]

ethernet cfm traceroute cache size *entrys*

no ethernet cfm traceroute cache size

[Parameters]

entrys: item number of LinkTrace database, range in 1-512.

[Default]

100

[Command Mode]

Global configuration mode

[Explanation of Command Executing Echo]

Set successfully

[Example]

Configure to hold 500 items in linktrace database:

Raisecom(config)# **ethernet cfm traceroute cache size 500**

[Related Commands]

Commands			Description
show	ethernet	cfm	Show traceroute cache.
	traceroute-cache		

41. 14 ping

[Function]

Executing ping function of layer-2

[Command Format]

ping {*MAC-ADDRESS* | **mep** *mepid*} [**count** *number*] [**size** *length*][**source** *mepid*]

[Parameters]

MAC-ADDRESS: mac address to ping;

mepid: MEP ID, range in 1-8191;

number: ping packets number at layer-2, range in 1-1024;

length: number of ping packets bytes at layer-2, range in 1-1484;

[Command Mode]

Service instance mode

[Explanation of Command Executing Echo]

Sending 5 Ethernet CFM loopback messages to 000e.5e03.688d, timeout is 2.5 seconds:

Success rate is 100 percent (5/5).

Ping statistics from 000e.5e03.688d:

Received loopback replys: <5 /0 /0 > (In order/Out of order/Error)

Failed to issue ping command! You must use command to enable ethernet cfm

Failed to issue ping command!mep does not find remote mep

Failed to issue ping command ! source mep does not exist

Failed to issue ping command ! source mep port disable

Failed to issue ping command!There aren't any MEPs

[Example]

Ping remote MEP 5 under service instance ma3-1-4:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **ping mep 5**

41.15 service

[Function]

Create service application.

[Command Format]

service *CSIID level level*

no service *CSIID level level*

[Parameter]

CSIID: ID of the created service, buildup by 1-13 characters string;

level: domain level of service, in range of 0-7.

[Command Modes]

Global configuration mode

[Executing Command Instruction]

This command can reduce cfm detecting range into a smaller range under domain. Fault detection for different service applications in one domain has noninterference each other.

[Explanation of command execution echo]

Set successfully.

This command was executed successfully.

Set unsuccessfully. The length of service name can't be longer than 13.

The command was executed unsuccessfully because there are should be not more than 13 characters for length of service name.

Set unsuccessfully. There isn't maintenance domain at level level-id.

Set unsuccessfully. There isn't maintenance domain at level level-id.

The command was executed unsuccessfully because the input MD level does not exist at level level-id.

Set unsuccessfully. The total amount of service instances exceed maximum.

The command was executed unsuccessfully because the total amount of service instances exceed up limit.

Set unsuccessfully. The MAID(MD name+MA name) is the same

The command was executed unsuccessfully because there MAID is

identical.

Set unsuccessfully. There has been the same service name in this MD

The command was executed unsuccessfully because there is identical service instance existing.

[Example]

Creating service instance ID ma3-1-4, and level is 3:

```
Raisecom(config)#service ma3-1-4 level 3
```

```
Raisecom(config-service)
```

Deleting service instance ID ma3-1-4 with level 3:

```
Raisecom(config-port)# no service ma3-1-4 level 3
```

[Related commands]

Commands	Description
show ethernet cfm domain	Show current domain and its service instance configuration information.

41.16 service cc enable

[Function]

Configure CCM transmission switch for MEP.

[Command Format]

```
service cc {enable | disable} mep {mepid-list | all}
```

[Parameters]

enable: CCM switch enable;

disable: CCM switch disable;

mepid-list: MEP ID list, range in 1-8191, including “,” and “-”;

all: all MEP.

[Command Mode]

Service instance mode

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. mep mpid does not exist.

[Example]

Enable all MEP cc switch under service instance ma3-1-4:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **service cc enable mep all**

[Related Commands]

Commands	Description
show ethernet cfm domain	Show current domain and its service instance configuration information.

41.17 service cc interval

[Function]

Configure CCM message transmitting interval.

[Command Format]

service cc interval {1 | 10 | 60 | 600}

[Parameters]

7: 1s

10: 10s

60: 60s

600: 600s

[Default]

10s

[Command Mode]

Service instance mode

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. The function of CC has enabled for some a MEP in this service instance, please disabled it first.

[Example]

Configure CCM transmitting interval under service instance ma3-1-4 to be 1 minute:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **service cc interval 60**

[Related Commands]

Commands	Description
show ethernet cfm domain	Show current domain and its service instance configuration information.

41.18 service cvlan

[Function]

Configure customer vlan for service instance.

[Command Format]

service cvlan *vlan*

no service cvlan

[Parameters]

vlan: vlan ID, range in 1-4094.

[Command Mode]

Service instance mode

[Explanation of Command Executing Echo]

Set successfully

[Example]

Configure cvlan to be 4000 in service instance ma3-1-4:

```
Raisecom(config)# service ma3-1-4 level 3
Raisecom(config-service)# service cvlan 4000
```

[Related Commands]

Commands	Description
show ethernet cfm domain	Show current domain and its service instance configuration information.

41.19 service mep

[Function]

Configure local MEP

[Command Format]

service mep [up] mpid *mepid* **port** *port-list*

service mep [up] mpid *mepid* **line** *line-list*

service mep [up] mpid *mepid* **client** *client-list*

no service mep mpid *mepid*

[Parameters]

mepid: configure ID for local MEP, range in 1-8191;

port-list: port list;

line-list: line port list;

client-list: client port list.

[Command Mode]

Service instance mode

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. The MEPID is duplicate in this service instance.

Set unsuccessfully. MEP <MEPID> is remote MEP at this service instance.

Set unsuccessfully. A MEP exists on this port with the same level and the same VLAN.

Set unsuccessfully. no vlan in this service instance.

Set unsuccessfully. The total amount of MEPs exceed maximum.

[Example]

Configure MEP under service instance ma3-1-4 at port 2, with MP ID 1:

Raisecom(config)#**service ma3-1-4 level 3**

Raisecom(config-service)#**service vlan-list 100**

Raisecom(config-service)#**service mep up mpid 1 port 2**

[Related Commands]

Commands	Description
show ethernet cfm mep	Show MEP information in service instance.
show ethernet cfm local-mp	Show local MP configuration information.

41.20 service performance-monitor delay object

[Function]

Configure time delay object for performance monitor pair

[Command Format]

service performance-monitor delay object *milliseconds*

[Parameters]

milliseconds: time delay object value, range in 1-1000, unit: ms.

[Default]

1000

[Command Mode]

Service instance mode

[Executing Command Instructions]

The performance monitor switch must be disabled before configuration.

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. Performance-monitor has been enabled

[Example]

Configure time delay object of performance monitor to be 300ms in service instance ma3-1-4:

Raisecom(config)# service ma3-1-4 level 3

Raisecom(config-service)# service performance-monitor delay object
300

[Related Commands]

Commands			Description
show	ethernet	cfm	Show configuration information of performance-monitor information

41.21 service performance-monitor delay threshold

[Function]

Configure frame delay alarm threshold for performance monitor pair.

[Command Format]

service performance-monitor delay {rising-threshold |
falling-threshold} threshold

[Parameters]

rising-threshold: upper threshold value;

falling-threshold: lower threshold value;

threshold: level of threshold, range in 0-7, indicating 0%, 0.1%, 0.2%, 0.5%, 1%, 2%, 5% and 100% respectively.

[Default]

rising-threshold: 7

falling-threshold: 0

[Command Mode]

Service instance mode

[Executing Command Instructions]

The performance monitor switch must be disabled before configuration.

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. Performance-monitor has been enabled

Set unsuccessfully. The falling threshold of delay is larger than raising threshold of delay

[Example]

Configure upper threshold of performance monitor frame delay level at 3 in service instance ma3-1-4:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **service performance-monitor delay rising-threshold 3**

[Related Commands]

Commands	Description
----------	-------------

show	ethernet	cfm	Show configuration information of performance-monitor information
			performance monitor.

41.22 service performance-monitor delay-variation object

[Function]

Configure time delay variation object for performance monitor pair

[Command Format]

service performance-monitor delay-variation object *milliseconds*

[Parameters]

milliseconds: time delay variation object value, range in 1-1000, unit: ms.

[Default]

1000

[Command Mode]

Service instance mode

[Executing Command Instructions]

The performance monitor switch must be disabled before configuration.

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. Performance-monitor has been enabled

[Example]

Configure time delay variation object of performance monitor to be 300ms in service instance ma3-1-4:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **service performance-monitor delay-variation object 300**

[Related Commands]

Commands			Description
show	ethernet	cfm	Show configuration information of performance-monitor information

41.23 service performance-monitor delay-variation threshold

[Function]

Configure frame delay variation alarm threshold for performance monitor pair.

[Command Format]

service performance-monitor delay-variation {rising-threshold | falling-threshold} *threshold*

[Parameters]

rising-threshold: upper threshold value;

falling-threshold: lower threshold value;

threshold: level of threshold, range in 0-7, indicating 0%, 0.1%, 0.2%, 0.5%, 1%, 2%, 5% and 100% respectively.

[Default]

rising-threshold: 7

falling-threshold: 0

[Command Mode]

Service instance mode

[Executing Command Instructions]

The performance monitor switch must be disabled before configuration.

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. Performance-monitor has been enabled

Set unsuccessfully. The falling threshold of dv is larger than raising threshold of dv

[Example]

Configure upper threshold of performance monitor delay variation level at 3 in service instance ma3-1-4:

```
Raisecom(config)# service ma3-1-4 level 3
```

```
Raisecom(config-service)# service performance-monitor delay  
variation rising-threshold 3
```

[Related Commands]

Commands			Description
show	ethernet	cfm	Show configuration information of performance monitor.
performance-monitor information			

41.24 service performance-monitor enable

[Function]

Configure performance monitor switch

[Command Format]

```
service performance-monitor {enable | disable}
```

[Parameters]

enable: enable performance monitor function;

disable: disable performance monitor function.

[Default]

disable

[Command Mode]

Service instance mode

[Executing Command Instructions]

The performance monitor switch can not be configured until the

performance monitor pair has been configured.

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. There isn't PM peers in this service instance.

[Example]

Enable performance monitor function switch in service instance ma3-1-4:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **service performance-monitor enable**

[Related Commands]

Commands			Description
show	ethernet	cfm	Show configuration information of performance monitor.
performance-monitor information			

41.25 service performance-monitor frame-loss-ratio threshold

[Function]

Configure frame loss ratio alarm threshold for performance monitor pair.

[Command Format]

service performance-monitor frame-loss-ratio {rising-threshold | falling-threshold} threshold

[Parameters]

rising-threshold: upper threshold value;

falling-threshold: lower threshold value;

threshold: level of threshold, range in 0-7, indicating 0%, 0.1%, 0.2%, 0.5%, 1%, 2%, 5% and 100% respectively.

[Default]

rising-threshold: 7

falling-threshold: 0

[Command Mode]

Service instance mode

[Executing Command Instructions]

The performance monitor switch must be disabled before configuration.

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. Performance-monitor has been enabled

Set unsuccessfully. The falling threshold of FLR is larger than raising threshod of FLR

[Example]

Configure upper threshold of performance monitor frame loss ratio level at 3 in service instance ma3-1-4:

Raisecom(config)# service ma3-1-4 level 3

Raisecom(config-service)# service performance-monitor frame-loss-ratio rising-threshold 3

[Related Commands]

Commands			Description
show	ethernet	cfm	Show configuration information of performance-monitor information
			performance monitor.

41.26 service performance-monitor peer

[Function]

Configure performance monitor pair

[Command Format]

service performance-monitor remote *mepid* source *mepid*

no service performance-monitor

[Parameters]

remote: remote MEP;

source: local MEP;

mepid: MEP ID, range in 1-8191.

[Command Mode]

Service instance mode

[Executing Command Instructions]

The performance monitor switch must be disabled before configuration.

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. source id is equal to remote id

Set unsuccessfully. source mep does not exist

Set unsuccessfully. Performance-monitor peer has existed

Set unsuccessfully. Performance-monitor has been enabled

[Example]

Configure performance monitor pair in service instance ma3-1-4 with remote MEP 1 and source MEP 2:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **service performance-monitor remote 1 source 2**

[Related Commands]

Commands			Description
show	ethernet	cfm	Show configuration information of performance-monitor information
			performance monitor.

41.27 service priority

[Function]

Configure message priority

[Command Format]

service priority *priority*

[Parameters]

priority: 802.1p priority, range in 0-7.

[Default]

6

[Command Mode]

Service instance mode

[Explanation of Command Executing Echo]

Set successfully

[Example]

Configure message priority to be 1 under service instance ma3-1-4:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **service priority 1**

[Related Commands]

Commands	Description
show ethernet cfm domain	Show current domain and its service instance configuration information.

41.28 service remote mep

[Function]

Configure static remote MEP

[Command Format]

service remote mep *mepid*

no service remote mep *mepid*

[Parameters]

mepid: configure ID for static remote MEP, range in 1-8191.

[Command Mode]

Service instance mode

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. This MEP has existed in the service instance.

[Example]

Configure static remote MEP ID to be 3 under service instance ma3-1-4:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **service remote mep 3**

[Related Commands]

Commands	Description
show ethernet cfm mep	Show MEP information.

41.29 service remote mep learning

[Function]

Configure remote MEP learning switch of service instance

[Command Format]

service remote mep learning {enable | disable}

[Parameters]

enable: CCM switch enable;

disable: CCM switch disable.

[Default]

disable

[Command Mode]

Service instance mode

[Explanation of Command Executing Echo]

Set successfully

[Example]

Enable remote MEP learning function switch under service instance
ma3-1-4:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **service remote mep learning**

[Related Commands]

Commands	Description
show ethernet cfm remote-mep	Show remote MEP information.

41.30 service remote mep mac

[Function]

Configure static remote MEP

[Command Format]

service remote mep *mepid* **mac** *ABCD.ABCD.ABCD*

no service remote mep *mepid*

[Parameters]

mepid: configure ID for static remote MEP, range in 1-8191.

ABCD.ABCD.ABCD: configure MAC address for remote MEP.

[Command Mode]

Service instance mode

[Explanation of Command Executing Echo]

Set successfully

Set unsuccessfully. This MEP has existed in the service instance

Set unsuccessfully. The static remote MEP has reached maximum

Set unsuccessfully. The mac is not unicast address

Set unsuccessfully. The mac is the same as local bridge mac

[Example]

Configure static remote MEP ID to be 3 under service instance ma3-1-4,
mac address is 1234.1234.1234:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **service remote mep 3 mac 1234.1234.1234**

[Related Commands]

Commands	Description
show ethernet cfm mep	Show MEP information.

41.31 service vlan-list

[Function]

Configure service instance vlan mapping

[Command Format]

service vlan-list *vlan-list*

no service vlan-list

[Parameters]

vlan-list: the vlan list of mapping, range in 1-4094, including “,” and “-”.

[Default]

Doesn't mapping any vlan by default.

[Command Mode]

Service instance mode

[Executing Command Instructions]

Vlan mapping must be configured after creating service instance to make cfm message being processed in the configured master vlan.

[Explanation of Command Executing Echo]

Set successfully

The command is successfully executed.

Set unsuccessfully. Some a MEP is in the service instance, please delete MEP first

The command failed to execute for there is MEP in the service instance.

Set unsuccessfully. vlan vlan-id already map to other primary vlan

The command failed to execute for there is vlan in vlan list being mapped to other master vlan.

Set unsuccessfully. The count of vlan has reached 32

The command failed to execute for the configured vlan reaches maximum.

Set unsuccessfully. This service has been mapped to other vlan,please delete it first

The command failed to execute for service instance has been correlated to other vlan.

Set unsuccessfully. The primary vlan has been mapped to other service instance

The command failed to execute for the master vlan has already being mapped to other service instance.

[Example]

Configure vlan mapping list vlan1-5 with service instance ID ma3-1-4:

```
Raisecom(config)# service ma3-1-4 level 3
```

```
Raisecom(config-service)# service vlan-list 1-5
```

Deleting vlan map with service instance ID ma3-1-4:

```
Raisecom(config)# service ma3-1-4 level 3
```

```
Raisecom(config-service)# no service vlan
```

[Related Commands]

Commands	Description
show ethernet cfm domain	Show current domain and its service instance configuration information.

41.32 show ethernet cfm

[Function]

Show cfm information

[Command Format]

show ethernet cfm

[Command Mode]

Privileged EXEC mode

[Explanation of Command Executing Echo]

Global CFM Admin Status: enable
Port CFM Enabled Portlist:1-9
Archive hold time of error CCMs: 100
The trap status: macRemErrXcon

[Example]

Show cfm information:
Raisecom(config)# **show ethernet cfm**

41.33 show ethernet cfm domain

[Function]

Show domain information

[Command Format]

show ethernet cfm domain [*level level*]

[Parameters]

level: level of domain, range in 0-7.

[Command Mode]

Privileged EXEC mode

[Explanation of Command Executing Echo]

Level: 3
Total services:1

<i>Service</i>	<i>Vlan</i>	<i>Vlan Number</i>	<i>CcmInterval</i>	<i>Remote Learn</i>
Ma3-1-4	4	1	10	enable

[Example]

Show error information of MD level 3:
Raisecom(config)# **show ethernet cfm errors level 3**

41.34 show ethernet cfm errors

[Function]

Show information of errors database.

[Command Format]

show ethernet cfm errors [**level** *level*]

[Parameters]

level: level of domain, range in 0-7.

[Command Mode]

Privileged EXEC mode

[Explanation of Command Executing Echo]

AffectedService	Level	VLAN	MPID	RemoteMep	Mac	ErrorType

[Example]

Show error information of MD level 3:

Raisecom(config)# **show ethernet cfm errors level 3**

41.35 show ethernet cfm local-mp

[Function]

Show MEP under service instance

[Command Format]

show ethernet cfm local level *level* **service** *CSIID*

[Parameters]

level: level of domain, range in 0-7;

CSIID: service instance ID.

[Command Mode]

Privileged EXEC mode

[Explanation of Command Executing Echo]

MepId	Type	Mac Address

1	dynamic remote	000e.5e03.688d
4	local	---

[Example]

Show MEP information of level 3, service instance ma3-1-4:

Raisecom(config)# **show ethernet cfm mep level 3 service ma3-1-4**

41.36 show ethernet cfm mep

[Function]

Show MEP under service instance

[Command Format]

show ethernet cfm mep level *level* service *CSIID*

[Parameters]

level: level of domain, range in 0-7;

CSIID: service instance ID.

[Command Mode]

Privileged EXEC mode

[Explanation of Command Executing Echo]

MepId	Type	Mac Address

1	dynamic remote	000e.5e03.688d
4	local	---

[Example]

Show MEP information of level 3, service instance ma3-1-4:

Raisecom(config)# **show ethernet cfm mep level 3 service ma3-1-4**

41.37 show ethernet cfm performance-monitor

[Function]

Show remote MEP under service instance.

[Command Format]

show ethernet cfm performance-monitor {*previous intervals* **quarter** | **current-quarter** | **last-24-hour** | **current-24-hour**} {**frame-loss-ratio** | **frame-delay** | **frame-delay-variation**} **level** *level* [*service CSIID*]

[Parameters]

previous: history 15 minutes;

intervals: the former 15 minutes from the 1st to 96th, range in 1-96;

quarter: 15 minutes;

current-quarter: current 15 minutes;

last-24-hour: history 24 hours;

current-24-hour: current 24 hours;

frame-loss-ratio: frame loss ratio;

frame-delay: frame time delay;

frame-delay-variation: frame time delay variation;

level: level of domain, range in 0-7;

CSIID: service instance ID.

[Command Mode]

Privileged EXEC mode

[Explanation of Command Executing Echo]

Show frame loss ratio information in current 24 hours:

Level:3 service:ma3-1-4

current 24 hour Far-end FLR statistic

<i>Tx</i>	<i>loss</i>	<i>ratio</i>	<i>Elapsed-time</i>
-----------	-------------	--------------	---------------------

476	7	14	4735
-----	---	----	------

current 24 hour Near-end FLR statistic

<i>Tx</i>	<i>loss</i>	<i>ratio</i>	<i>Elapsed-time</i>
-----------	-------------	--------------	---------------------

535	68	127	4735
-----	----	-----	------

Show frame time delay information in current 24 hours:

Level:3 service:ma3-1-4

Delay Object:1000 Rising threshold:7 Failing threshold:0

current 24 hours Far-end delay statistic

Min delay	Avg delay	Max delay	Above obj	Below obj
-----------	-----------	-----------	-----------	-----------

8	8	8	0	556
---	---	---	---	-----

current 24 hours Near-end delay statistic

Min delay	Avg delay	Max delay	Above obj	Below obj
-----------	-----------	-----------	-----------	-----------

4	4	4	0	556
---	---	---	---	-----

current 24 hours Round-trip delay statistic

Min delay	Avg delay	Max delay	Above obj	Below obj
-----------	-----------	-----------	-----------	-----------

0	2	3	0	556
---	---	---	---	-----

Show frame time delay information in current 24 hours:

Level:3 service:ma3-1-4

Delay Object:1000 Rising threshold:7 Failing threshold:0

current 24 hours Far-end delay statistic

Min delay	Avg delay	Max delay	Above obj	Below obj
-----------	-----------	-----------	-----------	-----------

8	8	8	0	556
---	---	---	---	-----

current 24 hours Near-end delay statistic

Min delay	Avg delay	Max delay	Above obj	Below obj
-----------	-----------	-----------	-----------	-----------

4	4	4	0	556
---	---	---	---	-----

current 24 hours Round-trip delay statistic

Min delay	Avg delay	Max delay	Above obj	Below obj
-----------	-----------	-----------	-----------	-----------

0	2	3	0	556
---	---	---	---	-----

Show frame time delay variation information in current 24 hours:

Level:3 service:ma3-1-4

current 24 hours Far-end delay-variation statistic

Avg variation	Max variation	Above obj	Below obj
---------------	---------------	-----------	-----------

0	0	0	563
---	---	---	-----

current 24 hours Near-end delay-variation statistic

<i>Avg variation</i>	<i>Max variation</i>	<i>Above obj</i>	<i>Below obj</i>
0	0	0	563

current 24 hours Round-trip delay-variation statistic

<i>Avg variation</i>	<i>Max variation</i>	<i>Above obj</i>	<i>Below obj</i>
0	3	0	563

Show frame loss ratio information in current 15 minutes:

Level:3 service:ma3-1-4

current 15 minute Far-end FLR statistic

<i>Tx</i>	<i>loss</i>	<i>ratio</i>	<i>Elapsed-time</i>
61	0	0	601

current 15 minute Near-end FLR statistic

<i>Tx</i>	<i>loss</i>	<i>ratio</i>	<i>Elapsed-time</i>
60	0	0	601

Show frame time delay information in current 15 minutes:

Level:3 service:ma3-1-4

Delay Object:1000 Rising threshold:7 Failing threshold:0

current 15 minute Far-end delay statistic

<i>Min delay</i>	<i>Avg delay</i>	<i>Max delay</i>	<i>Above obj</i>	<i>Below obj</i>
8	8	8	0	68

current 15 minute Near-end delay statistic

<i>Min delay</i>	<i>Avg delay</i>	<i>Max delay</i>	<i>Above obj</i>	<i>Below obj</i>
4	4	4	0	68

current 15 minute Round-trip delay statistic

<i>Min delay</i>	<i>Avg delay</i>	<i>Max delay</i>	<i>Above obj</i>	<i>Below obj</i>
3	3	3	0	68

Show frame time delay variation information in current 15 minutes:

Level:3 service:ma3-1-4

current 15 minute Far-end delay-variation statistic

Avg variation	Max variation	Above obj	Below obj
---------------	---------------	-----------	-----------

0	0	0	73
---	---	---	----

current 15 minute Near-end delay-variation statistic

Avg variation	Max variation	Above obj	Below obj
---------------	---------------	-----------	-----------

0	0	0	73
---	---	---	----

current 15 minute Round-trip delay-variation statistic

Avg variation	Max variation	Above obj	Below obj
---------------	---------------	-----------	-----------

0	0	0	73
---	---	---	----

Show frame loss ratio information in period of 15 minutes beforetime:

Level:3 service:ma3-1-4

BeginTime:1Hours 43Minutes 12Sec 650MilliSec

history 15 minutes Far-end FLR statistic

Peer Mepid	Tx	loss	ratio
------------	----	------	-------

1	92	7	76
---	----	---	----

history 15 minutes Near-end FLR statistic

Peer Mepid	Tx	loss	ratio
------------	----	------	-------

1	152	68	447
---	-----	----	-----

Show frame time delay information in period of 15 minutes beforetime:

Level:3 service:ma3-1-4

Delay Object:1000 Rising threshold:7 Failing threshold:0

BeginTime:0Hours 0Minutes 6Sec 378MilliSec

Previous 15 minute Far-end delay statistic

Peer MEPid	Min delay	Avg delay	Max delay	Above obj	Below obj
------------	-----------	-----------	-----------	-----------	-----------

1	8	8	8	0	83
---	---	---	---	---	----

Previous 15 minute Near-end delay statistic

Peer MEPid	Min delay	Avg delay	Max delay	Above obj	Below obj
------------	-----------	-----------	-----------	-----------	-----------

1	4	4	4	0	83
<i>Previous 15 minute Round-trip delay statistic</i>					
<i>Peer MEPid</i>	<i>Min delay</i>	<i>Avg delay</i>	<i>Max delay</i>	<i>Above obj</i>	<i>Below obj</i>

1	0	2	3	0	83

Show frame time delay variation information in period of 15 minutes beforetime:

Level:3 service:ma3-1-4
BeginTime:0Hours 0Minutes 6Sec 423MilliSec

<i>Previous 15 minute Far-end delay-variation statistic</i>			
<i>Avg variation</i>	<i>Max variation</i>	<i>Above obj</i>	<i>Below obj</i>

0	0	0	82
<i>current 15 minute Near-end delay-variation statistic</i>			
<i>Avg variation</i>	<i>Max variation</i>	<i>Above obj</i>	<i>Below obj</i>

0	0	0	82
<i>current 15 minute Round-trip delay-variation statistic</i>			
<i>Avg variation</i>	<i>Max variation</i>	<i>Above obj</i>	<i>Below obj</i>

0	3	0	82

Show frame time delay variation information in period of 15 minutes beforetime:

Level:3 service:ma3-1-4			
BeginTime:0Hours 0Minutes 6Sec 423MilliSec			
<i>Previous 15 minute Far-end delay-variation statistic</i>			
<i>Avg variation</i>	<i>Max variation</i>	<i>Above obj</i>	<i>Below obj</i>

	0	0	0
<i>current 15 minute Near-end delay-variation statistic</i>			
<i>Avg variation</i>	<i>Max variation</i>	<i>Above obj</i>	<i>Below obj</i>

0	0	0	82
---	---	---	----

current 15 minute Round-trip delay-variation statistic

<i>Avg variation</i>	<i>Max variation</i>	<i>Above obj</i>	<i>Below obj</i>
----------------------	----------------------	------------------	------------------

0	3	0	82
---	---	---	----

Show frame loss ratio information in last 24 hours:

Level:3 service:ma3-1-4

BeginTime:NULL

history 24 hours Far-end FLR statistic

<i>Peer Mepid</i>	<i>Tx</i>	<i>loss</i>	<i>ratio</i>
-------------------	-----------	-------------	--------------

2	200	2	10
---	-----	---	----

history 24 hours Near-end FLR statistic

<i>Peer Mepid</i>	<i>Tx</i>	<i>loss</i>	<i>ratio</i>
-------------------	-----------	-------------	--------------

2	200	2	10
---	-----	---	----

Show frame time delay information in last 24 hours:

Level:3 service:ma3-1-4

Delay Object:1000 Rising threshold:7 Failing threshold:0

BeginTime:NULL

Previous 15 minute Far-end delay statistic

<i>Peer MEPid</i>	<i>Min delay</i>	<i>Avg delay</i>	<i>Max delay</i>	<i>Above obj</i>	<i>Below obj</i>
-------------------	------------------	------------------	------------------	------------------	------------------

2	<0	2	8	10	86
---	----	---	---	----	----

Previous 15 minute Near-end delay statistic

<i>Peer MEPid</i>	<i>Min delay</i>	<i>Avg delay</i>	<i>Max delay</i>	<i>Above obj</i>	<i>Below obj</i>
-------------------	------------------	------------------	------------------	------------------	------------------

2	<0	2	8	10	86
---	----	---	---	----	----

Previous 15 minute Round-trip delay statistic

<i>Peer MEPid</i>	<i>Min delay</i>	<i>Avg delay</i>	<i>Max delay</i>	<i>Above obj</i>	<i>Below obj</i>
-------------------	------------------	------------------	------------------	------------------	------------------

2	<0	2	8	10	86
---	----	---	---	----	----

Show frame delay variation information in last 24 hours:

Level:3 service:ma3-1-4

BeginTime:NULL

Previous 24h Far-end delay-variation statistic

Avg variation	Max variation	Above obj	Below obj
---------------	---------------	-----------	-----------

2	4	10	86
---	---	----	----

current 24 hours Near-end delay-variation statistic

Avg variation	Max variation	Above obj	Below obj
---------------	---------------	-----------	-----------

2	4	10	86
---	---	----	----

current 24 hours Round-trip delay-variation statistic

Avg variation	Max variation	Above obj	Below obj
---------------	---------------	-----------	-----------

2	4	10	86
---	---	----	----

[Example]

Show level 3 service instance ma3-1-4 frame loss ratio information in current 15 minutes:

```
Raisecom(config)# show ethernet cfm performance-monitor  
current-quarter frame-loss-ratio level 3 service ma3-1-4
```

41.38 show ethernet cfm performance-monitor information

[Function]

Show configuration information of performance monitor.

[Command Format]

```
show ethernet cfm performance-monitor information level level  
service CSIID
```

[Parameters]

level: level of domain, range in 0-7;

CSIID: service instance ID.

[Command Mode]

Privileged EXEC mode

[Explanation of Command Executing Echo]

Show configuration information of performance monitor:

Level:3
service:ma3-1-4
Performance-Monitor:enabled
Performance-Monitor: trap:disabled
Frame-Loss-Ratio raising threshold:7
Frame-Loss-Ratio failing threshold:0
Delay raising threshold:7
Delay failing threshold:0
Delay-Viriation raising threshold:7
Delay-Viriation failing threshold:0

S-MEPID: Source MEP ID
D-MEPID: Destination MEP ID
DV : Delay Variation
Obj : Objective
S-MEPID D-MEPID Delay Obj DV Obj

4 1 1000 1000

[Example]

Show total frame loss ratio of level 3 service instance ma3-1-4:

Raisecom(config)# **show ethernet cfm total frame-loss-ratio level 3**
service ma3-1-4

41.39 show ethernet cfm performance-monitor total frame-loss-ratio

[Function]

Show total frame loss ratio of performance monitor.

[Command Format]

show ethernet cfm performance-monitor total frame-loss-ratio **level**
level service CSIID

[Parameters]

total: total statistic information from performance monitor to current;

frame-loss-ratio: frame loss ratio;

level: level of domain, range in 0-7;

CSIID: service instance ID.

[Command Mode]

Privileged EXEC mode

[Explanation of Command Executing Echo]

Show total frame loss ratio:

Level:3 service:ma3-1-4

FLR:frame loss ratio

Total Far-end FLR statistic

<i>Tx</i>	<i>loss</i>	<i>ratio</i>	<i>Elapsed-time</i>	<i>Unavialable-time</i>
670	7	10	6683	69

FLR:frame loss ratio

Total Near-end FLR statistic

<i>Tx</i>	<i>loss</i>	<i>ratio</i>	<i>Elapsed-time</i>	<i>Unavialable-time</i>
730	68	93	6683	622

[Example]

Show total frame loss ratio of level 3 service instance ma3-1-4:

```
Raisecom(config)# show ethernet cfm total frame-loss-ratio level 3  
service ma3-1-4
```

41.40 show ethernet cfm remote

[Function]

Show remote MEP under service instance

[Command Format]

```
show ethernet cfm remote-mep [level level [service CSIID [mpid  
mepid]]]
```

[Parameters]

level: level of domain, range in 0-7;

CSIID: service instance ID;

mepid: MEP id, range in 1-8191.

[Command Mode]

Privileged EXEC mode

[Explanation of Command Executing Echo]

Mpid	MdName	MaName	Level	Vlan	PortState	Mac	Address
Ingress Port	Age						

1	md3-1	ma3-1-4	3	4	Down	000E.5E03.688D	
8	3						

[Example]

Show remote mep information of level 3 service instance ma3-1-4:

```
Raisecom(config)# show ethernet cfm remote-mep level 3 service  
ma3-1-4
```

41.41 show ethernet cfm traceroute

[Function]

Show traceroute cache information

[Command Format]

show ethernet cfm traceroute-cache

[Command Mode]

Privileged EXEC mode

[Explanation of Command Executing Echo]

The size of the linktrace database: 100 hold-time: 100
Tracing the route to 000e.5e03.688d on domain md3-1, level 3, VLAN 4.
Traceroute send via port 8.

<i>Hops</i>	<i>HostMac</i>	<i>Ingress/EgressPort</i>	<i>IsForwarded</i>	<i>RelayAction</i>
<i>NextHop</i>				

<i>1</i>	<i>000e.5e03.84c1</i>	<i>8/-</i>	<i>Yes</i>	<i>rlyFdb</i>
<i>000e.5e03.84c1</i>				
	<i>!2</i>	<i>000e.5e03.84c1</i>	<i>-/8</i>	<i>No</i>
				<i>rlyHit</i>

The linktrace database doesn't exist. You must use command to enable the linktrace database storing data

[Example]

Show traceroute-cache information:

Raisecom(config)# **show ethernet cfm traceroute-cache**

41.42 snmp-server trap cfm

[Function]

Set alarm type for service instance cfm.

[Command Format]

snmp-server trap cfm {all | macremerr | remerr | ccmerr | xcon | none} mep {mepid-list | all}
no snmp-server trap cfm mep {mepid-list |all}

[Parameters]

all: all alarm types or all MEP;

macremerr: send alarms in type of Macstatus, RemoteCCM, ErrorCCM and XconCCM;

remerr: send alarms in type of RemoteCCM, ErrorCCM and XconCCM;

ccmerr: send alarms in type of ErrorCCM and XconCCM;

xcon: only send alarms in type of XconCCM;

none: don't send any alarm;

mepid-list: MEP ID list, range in 1-8191, including “,” or “-”.

[Default]

macremerr

[Command Mode]

Service instance mode

[Executing Command Instructions]

There will be trap transmitted when relevant network type event appears.

[Explanation of Command Executing Echo]

Set successfully

[Example]

Set cfm trap type of all mep to be remerr:

```
Raisecom(config)# snmp-server cfm-trap remerr mep all
```

Restore cfm trap:

```
Raisecom(config)#no snmp-server cfm-trap mep all
```

[Related Commands]

Commands	Description
show ethernet cfm domain	Show current domain and its service instance configuration information.

41.43 snmp-server trap performance-monitor

[Function]

Configure monitor trap switch for performance monitor pair

[Command Format]

```
snmp-server trap performance-monitor {enable | disable}
```

[Parameters]

enable: enable performance monitor trap switch;

disable: disable performance monitor trap switch.

[Default]

disable

[Command Mode]

Service instance mode

[Explanation of Command Executing Echo]

Set successfully

[Example]

Enable performance monitor trap switch in service instance ma3-1-4:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **snmp-server trap performance-monitor enable**

[Related Commands]

Commands			Description
show	ethernet	cfm	Show configuration information of performance monitor.
performance-monitor information			

41. 44 traceroute

[Function]

Executing traceroute function of layer-2

[Command Format]

traceroute {*MAC-ADDRESS* | **mep** *mepid*} [**tth** *tth*] [**source** *mepid*]

[Parameters]

MAC-ADDRESS: destination mac address that executes traceroute;

mepid: MEP ID, range in: 1-8191;

tth: starting tth value, range in: 1-255.

[Command Mode]

Service instance mode

[Explanation of Command Executing Echo]

Set successfully

TTL: <64>

Tracing the route to 000e.5e03.688d on domain md3-1, level 3, VLAN 4.

Traceroute send via port 8.

Hops NextHop	HostMac	Ingress/EgressPort	IsForwarded	RelayAction
1 000e.5e03.84c1	000e.5e03.84c1	8/-	Yes	rlyFdb
	!2 000e.5e03.84c1 000e.5e03.688d	-/8	No	rlyHit

Set successfully

Failed to issue traceroute command! You must use command to enable ethernet cfm

Set successfully

Failed to issue traceroute command!Source MEP equeal with target MEP

Set successfully

Failed to issue traceroute command!mep does not find remote mep

Set successfully

Failed to issue traceroute command ! source mep does not exsit

Set successfully

Failed to issue traceroute command ! source mep port disable

Set successfully

Failed to issue traceroute command!There aren't any MEPs

[Example]

Destination mac of traceroute under service instance ma3-1-4 is 1235.1234.1234:

Raisecom(config)# **service ma3-1-4 level 3**

Raisecom(config-service)# **traceroute 1235.1234.1234**

Chapter 42 Commands of Storm-control

42.1 generate ssh-key

[Function]

The command is used to generate ssh2 authenticated key

[Command Format]

Geberate ss -key

[Command Modes]

Global configuration mode; privileges of the users

[Executing Command Instruction]

The command is used to generate the SSH V2 authenticated key

Note: For different system generated key time is different, please be patient.

[Explanation of command execution echo]

Generating RSA Key...Done!

Saving key ...Done!

[Example]

To generate SSH V2 authenticatedkey

Raisecom# **generate ssh-key**

Generating RSA Key...Done!

Saving key ...Done!

[Related commands]

Commands	Description
Show ssh2 public-key	Show SSHV2 server public-key
show ssh server	Show the operation of SSHV2 server

42.2 show ssh2 public-key authentication

[Function]

The command is used to show ssh2 authenticated public-key

[Command Format]

show ssh2 public-key authentication

[Command Modes]

Global configuration mode; privileges of the users

[Executing Command Instruction]

The command is used to show SSH V2 **publickey** authenticated public-key

[Explanation of command execution echo]

[Example]

To show SSH V2 authenticated public-key
Raisecom#sh ssh2 public-key authentication
Authentication public key:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key"
AAAAB3NzaC1yc2EAAAABJQAAAIBvsM1AUbgB29+uTXji2+4ovmudtqQkuV+p
U6m/oaZ5TQWgtH5U4cBdhwOdJSm/cYmoTuKaWMB0JRgMuheKjvdY1mAu352u
nhLUS7+Jc8tggqMvyg8wHV+RPKCtHJZhccKCROky70sx39NSoHjBQLLQ8hjr
FQ/fD+K/ItcYaNgdhw==
---- END SSH2 PUBLIC KEY ----

[Related commands]

Commands	Description
ssh2 server authentication public-key	Input ssh2 server authentication RSA public-key

42.3 show ssh2 session

[Function]

The command is used to show Client Information of SSH V2 server

[Command Format]

show ssh2 session

[Command Modes]

Global configuration mode; privileges of the users

[Executing Command Instruction]

The command is used to show SSH V2 server Client Information

[Explanation of command execution echo]

[Example]

SSH V2 serve Client Information

Raisecom# show ssh2 session

<i>ID</i>	<i>Ver</i>	<i>Cipher(IN/OUT)</i>	<i>Con-Time</i>	<i>State</i>	<i>UserId</i>	<i>Ip</i>

<i>0</i>	<i>2.0</i>	<i>aes/aes</i>		<i>0h:0m:13s</i>	<i>OK(1channels)</i>	<i>raisecom</i>
<i>10.169.0.9</i>						
<i>1</i>	<i>2.0</i>	<i>--/--</i>	<i>--</i>	<i>Closed</i>	<i>--</i>	<i>--</i>
<i>2</i>	<i>2.0</i>	<i>--/--</i>	<i>--</i>	<i>Closed</i>	<i>--</i>	<i>--</i>
<i>3</i>	<i>2.0</i>	<i>--/--</i>	<i>--</i>	<i>Closed</i>	<i>--</i>	<i>--</i>
<i>4</i>	<i>2.0</i>	<i>--/--</i>	<i>--</i>	<i>Closed</i>	<i>--</i>	<i>--</i>

42.4 ssh2 server

[Function]

To start or shut down the functions of the server SSH V2

[Command Format]

[no] ssh2 server

[Default]

SSH V2 server does not start

[Command Modes]

Global configuration mode; privileges of the users

[Executing Command Instruction]

The command is used to start the SSH V2 server.

no form of the command is used to shut down the SSH server launched

[Explanation of command execution echo]

Set successfully!

Set unsuccessfully!

Please first generate SSH Key!

[Example]

To start the SSH V2 server.

Raisecom> **ssh server**

[Related commands]

Commands	Description
show ssh server	Show the operation of SSHV2 server

42.5 ssh2 server authentication public-key

[Function]

The command is used to input ssh2 server authentication public-key

[Command Format]

ssh2 server authentication public-key

[Command Modes]

Global configuration mode; privileges of the users

[Executing Command Instruction]

The command is used to input ssh2 server authentication RSA public-key. Text-editing software can be used to open generated RSA public key file in customer terminal, and then by running the command

line will copy the key file to the console, type **ctrl + s** to save your input.

[Explanation of command execution echo]

Discard Input!

It indicates that your input is ignored

Input Key Error!

It indicates that your input is wrong

[Example]

To input SSH V2 server authentication RSA public-key

Raisecom# **ssh2 server authentication public-key**

(Ctrl+s) for save input and return

(Ctrl+z) for discard input and return.

-----.

---- BEGIN SSH2 PUBLIC KEY ----

Comment: "rsa-key-20090408"

AAAAB3NzaC1yc2EAAAABJQAAAIBvsMIAUbgB29+uTXji2+4ovmudtqQkuV+p

U6m/

oaZ5TQWgtH5U4cBdhwOdJSm/cYmoTuKaWMB0JRgMuheKjvdYlmAu352unhLU

S7+J

c8tggqMvyg8wHV+RPKCtHJZhccKCROky70sx39NSoHjBQLLQ8hjrFQ/fD+K/It

cY

aNgdhw==

---- END SSH2 PUBLIC KEY ----

[Related commands]

Commands	Description
show ssh2 public-key	Show public-key of SSHV2 server

42.6 ssh2 server authentication {password | rsa-key }

[Function]

The command is used to set up ssh2 server authentication

[Command Format]

ssh2 server authentication {password | rsa-key }

[Parameter]

password: The use of local username password authentication

rsa-key: The use of **RSA** public key authentication method
[Default]

Default: The use of local username password authentication

[Command Modes]

Global configuration mode; privileges of the users

[Executing Command Instruction]

The command is used to set up ssh2 server authentication

[Explanation of command execution echo]

Set successfully!

Set unsuccessfully!

Please first input authentication public Key

It indicates that if you want to set up RSA public key authentication method, please enter the public key in advance

[Example]

SSH V2 server frame authentication is set at RSA-key

Raisecom# **ssh2 server authentication rsa-key**

[Related commands]

Commands	Description
show ssh server	Show the operation of SSHV2 server

42.7 ssh2 server authentication-retries

[Function]

The command is used to set up the frequency of authentication-retries of SSH V2 server

[Command Format]

ssh2 server authentication-retries *retry*
no ssh2 server authentication-retries

[Parameter]

retry units of the frequency, range of 1-100

[Default]

The frequency of default authentication-retries of SSH V2 server: 20 times

[Command Modes]

Global configuration mode; privileges of the users

[Executing Command Instruction]

The command is used to set up the frequency of authentication-retries of SSH V2 server

no form of the command is used to restore the default settings of the SSH server

[Explanation of command execution echo]

Set successfully!

Set unsuccessfully!

Error input time out value.

It indicates that time parameter input is illegal.

[Example]

To set up the frequency of authentication-retries of SSH V2 server: three times

Raisecom# **ssh2 server authentication- retries 3**

[Related commands]

Commands	Description
show ssh server	Show the operation of SSHV2 server

42.8 ssh2 server authentication-timeout

[Function]

The command is used to set up SSH V2 authentication server timeout

[Command Format]

ssh2 server authentication-timeout *time*

no ssh2 server authentication-timeout

[Parameter]

time units of seconds, range 100-65535

[Default]

Default authentication timeout: 600 seconds

[Command Modes]

Global configuration mode; privileges of the users

[Executing Command Instruction]

Use the command to set up SSH V2 authentication server timeout
no form of the command to restore the default settings.

[Explanation of command execution echo]

Set successfully

Set unsuccessfully

Error input time out value.

It indicates that time parameter input is unlawful

[Example]

To set up SSH V2 authentication server timeout: 300 seconds
Raisecom# **ssh2 server authentication-timeout 300**

[Related commands]

Commands	Description
show ssh server	shows the operation of the server SSHV2

42.9 ssh2 server port**[Function]**

The command is used to set up SSH V2 server listening port

[Command Format]

ssh2 server port *port*
no ssh2 server port

[Parameter]

port TCP port, range 1-65535

[Default]

default listening port: 22

[Command Modes]

Global configuration mode; privileges of the users

[Executing Command Instruction]

The command is used to set up SSH V2 server listening port
no form of the command is used to restore the default settings

[Explanation of command execution echo]

Set successfully!

Set unsuccessfully!

Current SSH Server is running(port:xx), Restart server to active setting.

It indicates that parameters input can not enter into force immediately

[Example]

To set up SSH V2 server listening port: 2000
Raisecom# **ssh2 server port 2000**

[Related commands]

Commands	Description
show ssh server	Show the operation of SSHV2 server

42.10 ssh2 server session**[Function]**

Enable or disable SSH V2 customer terminal

[Command Format]

ssh2 server session {*sessionlist*} {enable |disable}

[Parameter]

- *sessionlist* customer terminal list, in support of multi-input, range 0-4

- **enable**
- **disable** prohibited

[Default]

Default:enable

[Command Modes]

Global configuration mode; privileges of the users

[Executing Command Instruction]

Enable or disable SSH V2 customer terminal

[Explanation of command execution echo]

Set successfully!

Set unsuccessfully!

The input session ids list is wrong

It indicates that the list input is illegal

[Example]

To disable SSH V2 server 1,3,4 customer terminal

Raisecom# **ssh2 server port 2000**

[Related commands]

Commands	Description
Show ssh session	Show the condition of SSHV2 server customer terminal
show ssh server	Show the operation of SSHV2 server

A

access-list-map, 382

arp, 253

C

class-map(config), 411

class-map(config-pmap), 412

clear, 13

clear arp, 254

clear device statistics, 13

clear dot1x statistics, 552

clear double-tagging-vlan statistics, 66

clear ethernet cfm errors, 666

clear ethernet cfm remote, 666

clear ethernet cfm traceroute cache, 667

clear ethernet ring statistics, 590

clear extended-oam statistics, 485

clear filter statistics, 383

clear mac-address-table, 79

clear mvr port statistics, 191

clear oam event, 467

clear oam statistics, 467

clear performance-monitor statistics, 668

clear rate-limit statistics vlan, 67

clear relay statistics, 109

clear rmon, 236

clear service-policy statistics, 414

clock set, 322

clock summer-time, 323

clock summer-time recurring, 324

clock timezone, 325

cluster, 288

cluster-autoactive, 289

cluster-autoactive commander-mac, 290

cmd-str schedule-list, 338

console-cli, 14

creat vlan, 352

D

debug, 15

debug dai, 445

debug ntp, 638

description, 94, 121, 486

dir, 17

dot1x auth-control, 553

dot1x reauthentication, 554

- dot1x timer quiet-period, 555
- dot1x timer reauth-period, 557
- dot1x timer server-timeout, 558
- dot1x timer supp-timeout, 560
- dot1x timer tx-period, 561
- download, 18, 487
- download remote, 489
- driver, 20, 345
- duplex, 95, 494
- dynamic statistics time, 96
- E**
- enable, 21
- enable login, 22, 612
- enable password, 23
- erase, 24, 495
- ethernet cfm, 669
- ethernet cfm domain, 670
- ethernet cfm errors archive-hold-time, 671
- ethernet cfm mip level, 672
- ethernet cfm port, 673
- ethernet cfm remote mep age-time, 674
- ethernet cfm traceroute cache, 675
- ethernet cfm traceroute cache hold-time, 676
- ethernet cfm traceroute cache size, 676
- ethernet ring, 591
- ethernet ring description, 592
- ethernet ring hello-time, 593
- ethernet ring holdtime, 595
- ethernet ring port, 596
- ethernet ring priority, 597
- ethernet ring protocol-vlan, 598
- ethernet ring restore-delay, 600
- exit, 25
- extended-oam notification, 496

F

- fault-pass, 497
- filter, 384
- filter {enable|disable}, 386
- flowcontrol, 499
- flowcontrol {receive|send}, 97

G

- generate ssh-key, 718

H

- help, 26

history, 27

hostname, 500

I

inside-loopback, 501

instance vlan, 137

interface client, 502

interface ip, 122

interface port, 28

interface range, 29

ip address, 122, 503

ip address dhcp vlanid, 166

ip arp-inspection, 446

ip arp-inspection trust, 448

ip default-gateway, 456, 505

ip dhcp client, 168

ip dhcp client renew, 170

ip dhcp information option attach-string, 172

ip dhcp information option circuit-id, 173

ip dhcp information option remote-id, 175

ip dhcp snooping, 176

ip dhcp snooping information option, 178

ip dhcp snooping port-list, 179

ip dhcp snooping trust, 180

ip igmp filter vlan, 192

ip igmp max-groups, 193

ip igmp max-groups action, 194

ip igmp querier, 196

ip igmp querier query-interval, 197

ip igmp snooping immediate-leave, 198

ip igmp snooping mrouter, 199

ip igmp snooping timeout, 201

ip igmp snooping vlan-list, 202

ip route, 457

ip route aging-time, 458

ip routing, 460

ip source binding, 568

ip verify source, 569

ip verify source trust, 571

ip-access-list, 387

L

line-speed auto, 506

list, 29

logging console, 311

logging file, 312

- logging host, 314
- logging on, 315
- logging time-stamp, 316
- logout, 31
- loopback-detection destination-address, 331
- loopback-detection down-time, 332
- loopback-detection hello-time, 333

M

- mac-access-list, 388
- mac-address-table aging-time, 80
- mac-address-table learning, 81
- mac-address-table static multicast, 82
- mac-address-table static unicast, 84
- mac-address-table threshold, 85
- match, 415
- match arp, 390
- match ip, 391
- match ip icmp, 395
- match ip igmp, 396
- match ip tcp, 398
- match ip udp, 400
- match user-define, 402
- match(ACLMAP layer 2), 404
- member, 291
- member auto-build, 294
- mirror, 54
- mirror block-non-mirror, 55
- mirror divider, 56
- mirror filter, 57
- mirror monitor-port, 59
- mirror source-port-list, 60
- mirror source-port-list ingress egress, 61
- mls double-tagging tpid, 371
- mls qos {aggregate-policer | class-policer | single-policer }, 423
- mls qos mapping cos, 416
- mls qos mapping dscp, 417
- mls qos port-priority, 418
- mls qos queue scheduler sp, 419
- mls qos queue scheduler wrr, 420
- mls qos queue wrr, 421
- mls qos trust port-priority, 422
- mvr immediate, 203
- mvr mode, 205
- mvr proxy, 206

mvr proxy last-member-query, 208
mvr proxy query-max-response-time, 209
mvr proxy source-ip, 211
mvr proxy suppression, 212
mvr timeout, 214
mvr type, 215
mvr vlan, 217
mvr vlan group, 218

N

name, 138, 353
no relay shutdown, 110
ntp peer, 639
ntp refclock-master, 640
ntp server, 642

O

oam enable, 468
oam peer event trap, 469
oam remote-loopback, 470

P

password, 31
permit | deny, 220
ping, 32, 677
police, 425
policy-map, 426
pppoeagent, 653
pppoeagent circuit-id, 654
pppoeagent circuit-id attach-string, 655
pppoeagent remote-id, 656
pppoeagent remote-id format, 657
pppoeagent trust, 658
pppoeagent vendor-specific-tag overwrite, 659

Q

quit, 34

R

radius accounting-server, 35
radius accounting-server key, 36
range, 221
rate-limit, 507
rate-limit double-tagging-vlan, 68
rate-limit egress, 70
rate-limit flow-control, 71
rate-limit ingress, 72
rate-limit vlan, 74
rcommand, 297

- reboot, 37, 509
- redirect-to port, 427
- relay, 110
- relay cos, 112
- relay destination-address, 113
- relay drop-threshold, 114
- relay port, 115
- relay shutdown-threshold, 116
- remote-device, 510
- rmon alarm, 236
- rmon event, 238
- rmon history, 240
- rmon statistic, 242
- rndp, 298
- rtdp, 299
- rtdp max-hop, 301
- S**
- schedule-list, 341
- search mac-address, 86
- service, 678
- service cc enable, 680
- service cc interval, 681
- service config, 575
- service config filename, 576
- service config filename rule, 578
- service config overwrite, 580
- service config tftp-server, 581
- service config trap, 582
- service config version, 583
- service cvlan, 682
- service mep, 683
- service performance-monitor delay object, 684
- service performance-monitor delay threshold, 685
- service performance-monitor delay-variation object, 687
- service performance-monitor delay-variation threshold, 688
- service performance-monitor enable, 689
- service performance-monitor frame-loss-ratio threshold, 690
- service performance-monitor peer, 691
- service priority, 693
- service remote mep, 693
- service remote mep learning, 694
- service remote mep mac, 695
- service vlan-list, 696
- service-policy, 428

- set, 429
- show access-list, 406
- show access-list-map, 407
- show arp, 255
- show buffer, 347
- show cable-diagnostics, 511, 634
- show class-map, 430
- show clock, 326
- show cluster member, 302
- show device statistics, 38
- show diags, 348
- show dot1x, 563
- show dot1x statistics, 564
- show ethernet cfm, 698
- show ethernet cfm domain, 699
- show ethernet cfm errors, 699
- show ethernet cfm local-mp, 700
- show ethernet cfm mep, 701
- show ethernet cfm performance-monitor, 701
- show ethernet cfm performance-monitor information, 708
- show ethernet cfm performance-monitor total frame-loss-ratio, 709
- show ethernet cfm remote, 710
- show ethernet cfm traceroute, 711
- show ethernet ring, 601
- show ethernet ring port, 602
- show ethernet ring port statistic, 604
- show extended-oam statistics, 511
- show extended-oam status, 513
- show filter, 407
- show inside-loopback, 514
- show interface ip, 124
- show interface ip description, 125
- show interface ip statistics, 126
- show interface port, 99, 515
- show interface port detail, 516
- show interface port statistics, 519
- show interface port switchport, 353
- show interface port transceiver, 547
- show interface vlan-mapping add-outer, 372
- show interface vlan-mapping translate, 373
- show ip arp-inspection, 449
- show ip dhcp client, 182
- show ip dhcp information option, 185
- show ip dhcp snooping, 186

show ip dhcp snooping binding, 187
show ip igmp filter, 223
show ip igmp filter port, 224
show ip igmp filter vlan, 225
show ip igmp profile, 227
show ip igmp snooping, 228
show ip protocol, 460
show ip route, 462
show ip verify source, 572
show keepalive, 451
show logging, 318
show loopback-detection, 334
show mac aging-time, 87
show mac-address-table multicast, 88
show mac-address-table static, 90
show mac-address-table threshold, 91
show memory, 348
show mirror, 63
show mls qos, 431
show mls qos mapping cos, 432
show mls qos mapping dscp, 433
show mls qos mapping localpriority, 433
show mls qos policer, 434
show mls qos port, 435
show mls qos queue, 436
show mvr, 230
show mvr member, 231
show mvr port, 232
show ntp associations, 643
show ntp status, 645
show oam, 471
show oam capability, 521
show oam loopback, 473
show oam peer, 474
show oam peer event, 476
show oam statistics, 478
show oam trap, 480
show policy-map, 438
show pppoeagent, 661
show pppoeagent statistic, 662
show radius-server, 40, 565
show rate-limit, 75
show rate-limit vlan, 76
show relay, 117

- show relay statistics, 118
- show remote-device information, 522
- show rmon, 243
- show rmdp, 304
- show rmdp neighbor, 305
- show rtdp, 306
- show rtdp device-list, 307
- show running-config, 41
- show schedule-list, 343
- show service config, 585
- show service config filename rule, 586
- show service-policy statistics, 440
- show sfp, 524
- show sla configuration, 620
- show sla result, 623
- show snmp access, 258
- show snmp community, 259
- show snmp config, 260
- show snmp group, 261
- show snmp host, 263
- show snmp statistics, 263
- show snmp trap remote, 265, 525
- show snmp user, 266
- show snmp view, 268
- show sntp, 328
- show spanning tree, 139
- show spanning-tree port-list/line/client, 143
- show spanning-tree region-operation, 145
- show ssh2 public-key authentication, 719
- show ssh2 session, 719
- show startup-config, 42
- show storm-control, 106
- show switchport qinq, 375
- show system mtu, 100
- show tacacs-server, 613
- show tech-support, 350
- show telnet-server, 648
- show trunk, 129
- show user, 44
- show version, 45
- show vlan, 355
- shutdown, 101, 526
- sla cfm-echo configuration, 625
- sla cfm-jitter configuration, 627

- sla icmp-echo configuration, 628
- sla icmp-jitter configuration, 629
- sla schedule, 631
- snmp trap remote, 269, 527
- snmp trap transceiver, 550
- snmp-server access, 270
- snmp-server community, 273, 528
- snmp-server contact, 275
- snmp-server enable traps, 276
- snmp-server group, 277
- snmp-server host, 279
- snmp-server keepalive-trap, 452
- snmp-server keepalive-trap interval, 453
- snmp-server location, 281
- snmp-server trap cfm, 712
- snmp-server trap performance-monitor, 713
- snmp-server user, 282
- snmp-server view, 284
- sntp server, 329
- spanning-tree, 147
 - spanning-tree clear statistics, 148
 - spanning-tree edged-port, 149
 - spanning-tree extern-path-cost, 150
 - spanning-tree forward-delay, 151
 - spanning-tree hello-time, 153
 - spanning-tree inter-path-cost, 154
 - spanning-tree link-type, 155
 - spanning-tree max-age, 156
 - spanning-tree mcheck, 158
 - spanning-tree mode, 159
 - spanning-tree region-configuration, 160
 - spanning-tree rootguard, 161
- speed, 102, 529
- ssh2 server, 720
 - ssh2 server authentication {password | rsa-key }, 722
 - ssh2 server authentication public-key, 721
 - ssh2 server authentication-retries, 723
 - ssh2 server authentication-timeout, 724
 - ssh2 server port, 725
 - ssh2 server session, 726
- state, 357
- storm-control, 107
- switch-mode double-tagged-vlan, 530
- switch-mode transparent, 532

switchport access egress-allowed vlan, 358

switchport access vlan, 360

switchport mode, 361

switchport qinq dot1q-tunnel, 376

switchport trunk allowed vlan, 363

switchport trunk native vlan, 365

switchport trunk untagged vlan, 366

switchport vlan-mapping add-outer, 377

switchport vlan-mapping translate, 379

system mtu, 103, 533

T

tacacs-server, 614

tacacs-server key, 615

telnet, 649

telnet-server, 650

terminal history, 46

terminal time-out, 47

test cable-diagnostics, 534, 635

traceroute, 607, 714

traceroute concurrent number, 609

trunk, 130

trunk group, 131

trunk loading-sharing mode, 132

trunk loading-sharing ticket-generation-algorithm, 134

trust cos, 441

trust dscp, 442

U

upload, 535

upload remote, 539

user, 48

user login, 49, 616

user name privilege, 51

V

vlan, 368

W

write, 52, 544